CYBERCRIME

# UNDERSTANDING CYBERCRIME:
## PHENOMENA, CHALLENGES AND LEGAL RESPONSE




SEPTEMBER 2012

Telecommunication Development Sector

# Understanding cybercrime: Phenomena, challenges and legal response

***September 2012***



The ITU publication *Understanding cybercrime: phenomena, challenges and legal response* has been prepared by Prof. Dr. Marco Gercke and is a new edition of a report previously entitled *Understanding Cybercrime: A Guide for Developing Countries*. The author wishes to thank the Infrastructure Enabling Environment and E-Application Department, ITU Telecommunication Development Bureau.

This publication is available online at: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

© ITU 2012

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

# Table of contents


Page

**Purpose** ..... **iii**

**1. Introduction** ..... **1**
- 1.1 Infrastructure and services ..... 1
- 1.2 Advantages and risks ..... 2
- 1.3 Cybersecurity and cybercrime ..... 2
- 1.4 International dimensions of cybercrime ..... 3
- 1.5 Consequences for developing countries ..... 4

**2. The phenomena of cybercrime** ..... **11**
- 2.1 Definitions ..... 11
- 2.2 Typology of cybercrime ..... 12
- 2.3 Development of computer crime and cybercrime ..... 12
- 2.4 Extent and impact of cybercrime offences ..... 14
- 2.5 Offences against the confidentiality, integrity and availability of computer data and systems ..... 16
- 2.6 Content-related offences ..... 21
- 2.7 Copyright and trademark related offences ..... 27
- 2.8 Computer-related offences ..... 29
- 2.9 Combination offences ..... 33

**3. The challenges of fighting cybercrime** ..... **74**
- 3.1 Opportunities ..... 74
- 3.2 General challenges ..... 75
- 3.3 Legal challenges ..... 82

**4. Anti-cybercrime strategies** ..... **97**
- 4.1 Cybercrime legislation as an integral part of a cybersecurity strategy ..... 97
- 4.2 A cybercrime policy as starting point ..... 98
- 4.3 The role of regulators in fighting cybercrime ..... 101

**5. Overview of activities of regional and international organizations** ..... **114**
- 5.1 International approaches ..... 114
- 5.2 Regional approaches ..... 123
- 5.3 Scientific and independent approaches ..... 144
- 5.4 The relationship between regional and international legislative approaches ..... 144
- 5.5 The relationship between international and national legislative approaches ..... 145

**6. Legal response** ..... **169**
- 6.1 Definitions ..... 169
- 6.2 Substantive criminal law ..... 177
- 6.3 Digital evidence ..... 225
- 6.4 Justisdiction ..... 234
- 6.5 Procedural law ..... 238
- 6.6 International cooperation ..... 266
- 6.7 Liability of Internet providers ..... 280

**7. [Keyword Index]** ..... Error! Bookmark not de

## Purpose

The purpose of the ITU report *Understanding Cybercrime: Phenomena, Challenges and Legal Response* is to assist countries in understanding the legal aspects of cybersecurity and to help harmonize legal frameworks. As such, the report aims to help developing countries better understand the national and international implications of growing cyberthreats, to assess the requirements of existing national, regional and international instruments, and to assist countries in establishing a sound legal foundation.

This report provides a comprehensive overview of the most relevant topics linked to the legal aspects of cybercrime and focuses on the demands of developing countries. Due to the transnational dimension of cybercrime, the legal instruments are the same for developing and developed countries. However, the references used were selected for the benefit of developing countries, in addition to a broad selection of resources provided for a more in-depth study of the different topics. Whenever possible, publicly available sources were used, including many free-of-charge editions of online law journals.

The report contains six main chapters. After an introduction (*Chapter 1*), it provides an overview of the phenomena of cybercrime (*Chapter 2*). This includes descriptions of how crimes are committed and explanations of the most widespread cybercrime offences such as hacking, identity theft and denial-of-service attacks. An overview of the challenges is also provided, as they relate to the investigation and prosecution of cybercrime (*Chapters 3* and *4*). After a summary of some of the activities undertaken by international and regional organizations in the fight against cybercrime (*Chapter 5*), it continues with an analysis of different legal approaches with regard to substantive criminal law, procedural law, digital evidence, international cooperation and the responsibility of Internet service providers (*Chapter 6*), including examples of international approaches as well as good-practice examples from national solutions.

This publication addresses the first of the seven strategic goals of the ITU Global Cybersecurity Agenda (GCA), which calls for the elaboration of strategies for the development of cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures, as well as addressing the approach to organizing national cybersecurity efforts under ITU-D Study Group 1 Question 22/1. Establishing the appropriate legal infrastructure is an integral component of a national cybersecurity strategy. The related mandate of ITU with regard to capacity building was emphasized by Resolution 130 (Rev. Guadalajara, 2010) of the ITU Plenipotentiary Conference, on Strengthening the role of ITU in building confidence and security in the use of information and communication technologies. The adoption by all countries of appropriate legislation against the misuse of ICTs for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cybersecurity. Since threats can originate anywhere around the globe, the challenges are inherently international in scope and require international cooperation, investigative assistance, and common substantive and procedural provisions. Thus, it is important that countries harmonize their legal frameworks to combat cybercrime and facilitate international cooperation.

### Disclaimer regarding hyperlinks

The document contains several hundred links to publically available documents. All references were checked at the time the links were added to the footnotes. However, no guarantee can be provided that the up-to-date content of the pages to which the links relate are still the same. Therefore the reference – wherever possible – also includes information about the author or publishing institution, title and if possible year of the publication to enable the reader to search for the document if the linked document is not available anymore.

# 1. Introduction

**Bibliography (selected):** *Barney*, Prometheus Wired: The Hope for Democracy in the Age of Network Technology, 2001; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture, 2006; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe, 2006; *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141 *et seq.*; *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3; *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2; *Masuda*, The Information Society as Post-Industrial Society, 1980; *Sieber*, The Threat of Cybercrime, Organised crime in Europe: the threat of Cybercrime, 2005; *Tanebaum*, Computer Networks, 2002; *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1; *Yang, Miao*, ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th International Conference on Electronic Commerce, page 52-56; *Zittrain*, History of Online Gatekeeping, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2.

## 1.1 Infrastructure and services

The Internet is one of the fastest-growing areas of technical infrastructure development.[1] Today, information and communication technologies (ICTs) are omnipresent and the trend towards digitization is growing. The demand for Internet and computer connectivity has led to the integration of computer technology into products that have usually functioned without it, such as cars and buildings.[2] Electricity supply, transportation infrastructure, military services and logistics – virtually all modern services depend on the use of ICTs.[3]

Although the development of new technologies is focused mainly on meeting consumer demands in western countries, developing countries can also benefit from new technologies.[4] With the availability of long-distance wireless communication technologies such as WiMAX[5] and computer systems that are now available for less than USD 200[6], many more people in developing countries should have easier access to the Internet and related products and services.[7]

The influence of ICTs on society goes far beyond establishing basic information infrastructure. The availability of ICTs is a foundation for development in the creation, availability and use of network-based services.[8] E-mails have displaced traditional letters[9]; online web representation is nowadays more important for businesses than printed publicity materials;[10] and Internet-based communication and phone services are growing faster than landline communications.[11]

The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for developing countries.

ICT applications, such as e-government, e-commerce, e-education, e-health and e-environment, are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas. ICT applications can facilitate the achievement of millennium development targets, reducing poverty and improving health and environmental conditions in developing countries. Given the right approach, context and implementation processes, investments in ICT applications and tools can result in productivity and quality improvements. In turn, ICT applications may release technical and human capacity and enable greater access to basic services. In this regard, online identity theft and the act of capturing another person's credentials and/or personal information via the Internet with the intent to fraudulently reuse it for criminal purposes is now one of the main threats to further deployment of e-government and e-business services.[12]

The costs of Internet services are often also much lower than comparable services outside the network.[13] E-mail services are often available free of charge or cost very little compared to traditional postal services.[14] The online encyclopaedia Wikipedia[15] can be used free of charge, as can hundreds of online hosting services.[16] Lower costs are important, as they enable services to be used by many more users, including people with only limited income. Given the limited financial resources of many people in developing countries, the Internet enables them to use services they may not otherwise have access to outside the network.

## 1.2 Advantages and risks

The introduction of ICTs into many aspects of everyday life has led to the development of the modern concept of the information society.[17] This development of the information society offers great opportunities.[18] Unhindered access to information can support democracy, as the flow of information is taken out of the control of state authorities (as has happened, for example, in Eastern Europe and North Africa).[19] Technical developments have improved daily life – for example, online banking and shopping, the use of mobile data services and voice over Internet protocol (VoIP) telephony are just some examples of how far the integration of ICTs into our daily lives has advanced.[20]

However, the growth of the information society is accompanied by new and serious threats.[21] Essential services such as water and electricity supply now rely on ICTs.[22] Cars, traffic control, elevators, air conditioning and telephones also depend on the smooth functioning of ICTs.[23] Attacks against information infrastructure and Internet services now have the potential to harm society in new and critical ways.[24]

Attacks against information infrastructure and Internet services have already taken place.[25] Online fraud and hacking attacks are just some examples of computer-related crimes that are committed on a large scale every day.[26] The financial damage caused by cybercrime is reported to be enormous.[27] In 2003 alone, malicious software caused damages of up to USD 17 billion.[28] By some estimates, revenues from cybercrime exceeded USD 100 billion in 2007, outstripping the illegal trade in drugs for the first time.[29] Nearly 60 per cent of businesses in the United States believe that cybercrime is more costly to them than physical crime.[30] These estimates clearly demonstrate the importance of protecting information infrastructures.[31]

Most of the above-mentioned attacks against computer infrastructure are not necessarily targeting critical infrastructure. However, the malicious software "Stuxnet" that was discovered in 2010 underlines the threat of attacks focusing on critical infrastructure.[32] The software, with more than 4 000 functions[33], focused on computer systems running software that is typically used to control critical infrastructure.[34]

## 1.3 Cybersecurity and cybercrime

Cybercrime and cybersecurity are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on cybersecurity[35] addresses cybercrime as one major challenge underlines this.

Cybersecurity[36] plays an important role in the ongoing development of information technology, as well as Internet services.[37] Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy.[38] Deterring cybercrime is an integral component of a national cybersecurity and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework and strategy for cybersecurity thus requires a comprehensive approach.[39] Cybersecurity strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime.[40] The development and support of cybersecurity strategies are a vital element in the fight against cybercrime.[41]

The legal, technical and institutional challenges posed by the issue of cybersecurity are global and far-reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation.[42] In this regard, the World Summit on the Information Society (WSIS)[43] recognized the real and significant risks posed by inadequate cybersecurity and the proliferation of cybercrime. The provisions of §§ 108-110 of the *WSIS Tunis Agenda for the Information Society*[44], including the Annex, set out a plan for multistakeholder

implementation at the international level of the *WSIS Geneva Plan of Action*,[45] describing the multistakeholder implementation process according to eleven action lines and allocating responsibilities for facilitating implementation of the different action lines. At WSIS, world leaders and governments designated ITU to facilitate the implementation of WSIS Action Line C5, dedicated to building confidence and security in the use of ICTs.[46]

In this regard, the ITU Secretary-General launched the Global Cybersecurity Agenda (GCA)[47] on 17 May 2007, alongside partners from governments, industry, regional and international organizations, academic and research institutions. The GCA is a global framework for dialogue and international cooperation to coordinate the international response to the growing challenges to cybersecurity and to enhance confidence and security in the information society. It builds on existing work, initiatives and partnerships with the objective of proposing global strategies to address today's challenges related to building confidence and security in the use of ICTs. Within ITU, the GCA complements existing ITU work programmes by facilitating the implementation of the three ITU Sectors' cybersecurity activities, within a framework of international cooperation.

The Global Cybersecurity Agenda has seven main strategic goals, built on five work areas: 1) Legal measures; 2) Technical and procedural measures; 3) Organizational structures; 4) Capacity building; and 5) International cooperation.[48]

The fight against cybercrime needs a comprehensive approach. Given that technical measures alone cannot prevent any crime, it is critical that law-enforcement agencies are allowed to investigate and prosecute cybercrime effectively.[49] Among the GCA work areas, "Legal measures" focuses on how to address the legislative challenges posed by criminal activities committed over ICT networks in an internationally compatible manner. "Technical and procedural measures" focuses on key measures to promote adoption of enhanced approaches to improve security and risk management in cyberspace, including accreditation schemes, protocols and standards. "Organizational structures" focuses on the prevention, detection, response to and crisis management of cyberattacks, including the protection of critical information infrastructure systems. "Capacity building" focuses on elaborating strategies for capacity-building mechanisms to raise awareness, transfer know-how and boost cybersecurity on the national policy agenda. Finally, "International cooperation" focuses on international cooperation, dialogue and coordination in dealing with cyberthreats.

The development of adequate legislation and within this approach the development of a cybercrime-related legal framework is an essential part of a cybersecurity strategy. This requires first of all the necessary substantive criminal law provisions to criminalize acts such as computer fraud, illegal access, data interference, copyright violations and child pornography.[50] The fact that provisions exist in the criminal code that are applicable to similar acts committed outside the network does not mean that they can be applied to acts committed over the Internet as well.[51] Therefore, a thorough analysis of current national laws is vital to identify any possible gaps.[52] Apart from substantive criminal law provisions[53], the law-enforcement agencies need the necessary tools and instruments to investigate cybercrime.[54] Such investigations themselves present a number of challenges.[55] Perpetrators can act from nearly any location in the world and take measures to mask their identity.[56] The tools and instruments needed to investigate cybercrime can be quite different from those used to investigate ordinary crimes.[57]

## 1.4 International dimensions of cybercrime

Cybercrime often has an international dimension.[58] E-mails with illegal content often pass through a number of countries during the transfer from sender to recipient, or illegal content is stored outside the country.[59] Within cybercrime investigations, close cooperation between the countries involved is very important.[60] The existing mutual legal assistance agreements are based on formal, complex and often time-consuming procedures, and in addition often do not cover computer-specific investigations.[61] Setting up procedures for quick response to incidents, as well as requests for international cooperation, is therefore vital.[62]

A number of countries base their mutual legal assistance regime on the principle of "dual criminality".[63] Investigations on a global level are generally limited to those crimes that are criminalized in all participating countries. Although there are a number of offences – such as the distribution of child pornography – that can be prosecuted in most jurisdictions, regional differences play an important role.[64] One example is other types of illegal content, such as hate speech. The criminalization of illegal content differs in various countries.[65] Material that can lawfully be distributed in one country can easily be illegal in another country.[66]

The computer technology currently in use is basically the same around the world.[67] Apart from language issues and power adapters, there is very little difference between the computer systems and cell phones sold in Asia and those sold in Europe. An analogous situation arises in relation to the Internet. Due to standardization, the network protocols used in countries on the African continent are the same as those used in the United States.[68] Standardization enables users around the world to access the same services over the Internet.[69]

The question is what effect the harmonization of global technical standards has on the development of the national criminal law. In terms of illegal content, Internet users can access information from around the world, enabling them to access information available legally abroad that could be illegal in their own country.

Theoretically, developments arising from technical standardization go far beyond the globalization of technology and services and could lead to the harmonization of national laws. However, as shown by the negotiations over the First Protocol to the Council of Europe Convention on Cybercrime (the "Convention on Cybercrime"),[70] the principles of national law change much more slowly than technical developments.[71]

Although the Internet may not recognize border controls, there are means to restrict access to certain information.[72] The access provider can generally block certain websites and the service provider that stores a website can prevent access to information for those users on the basis of IP-addresses linked to a certain country ("IP-targeting").[73] Both measures can be circumvented, but are nevertheless instruments that can be used to retain territorial differences in a global network.[74] The OpenNet Initiative[75] reports that this kind of censorship is practised by about two dozen countries.[76]

## 1.5 Consequences for developing countries

Finding response strategies and solutions to the threat of cybercrime is a major challenge, especially for developing countries. A comprehensive anti-cybercrime strategy generally contains technical protection measures, as well as legal instruments.[77] The development and implementation of these instruments need time. Technical protection measures are especially cost-intensive.[78] Developing countries need to integrate protection measures into the roll-out of the Internet from the beginning, as although this might initially raise the cost of Internet services, the long-term gains in avoiding the costs and damage inflicted by cybercrime are large and far outweigh any initial outlays on technical protection measures and network safeguards.[79]

The risks associated with weak protection measures could in fact affect developing countries more intensely, due to their less strict safeguards and protection.[80] The ability to protect customers, as well as firms, is a fundamental requirement not only for regular businesses, but also for online or Internet-based businesses. In the absence of Internet security, developing countries could encounter significant difficulties promoting e-business and participating in online service industries.

The development of technical measures to promote cybersecurity and proper cybercrime legislation is vital for both developed countries and developing countries. Compared with the costs of grafting safeguards and protection measures onto computer networks at a later date, it is likely that initial measures taken right from the outset will be less expensive. Developing countries need to bring their anti-cybercrime strategies into line with international standards from the outset.[81]

[1] On the development of the Internet, see: *Yang, Miao*, ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th International Conference on Electronic Commerce, page 52 – 56; The World Information Society Report 2007, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/. According to ITU, there were over 2 billion Internet users by the end of 2010, of which 1.2 billion in developing countries. For more information, see: ITU ICT Facts and Figures 2010, page 3, available at: www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

[2] Regarding the threat of attacks against computer systems integrated in cars, see: BBC News, Cars safe from computer viruses, 11.05.2005, available at: http://news.bbc.co.uk/1/hi/technology/4536307.stm.

[3] See *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1. *Bohn/Coroama/Langheinrich/Mattern/Rohs,* "Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications", Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 *et seq.*, available at: www.vs.inf.ethz.ch/res/papers/hera.pdf. A demonstration of the impact of even short interruptions to Internet and computer services was the harm caused by the computer worm "Sasser". In 2004, the worm affected computers running versions of Microsoft's Windows operating system. As a result of the worm, a number of services were interrupted. Among them were the US airline "Delta Airlines" that had to cancel several trans-Atlantic flights because its computer systems had been swamped by the worm, whilst the electronic mapping services of the British Coastguard were disabled for a few hours. See Heise News, 04.01.2005, available at: www.heise.de/newsticker/meldung/54746; BBC News, "Sasser net worm affects millions", 04.05.2004, available at: http://news.bbc.co.uk/1/hi/technology/3682537.stm.

[4] Regarding the possibilities and technology available to access the Internet in developing countries, see: *Esteve/Machin*, Devices to access Internet in Developing countries, available at: www2007.org/workshops/paper_106.pdf.

[5] WiMAX (Worldwide Interoperability for Microwave Access) is a technology that provides wireless data services (such as access to the Internet) over long distances. For more information, see: The WiMAX Forum, available at www.wimaxforum.org; *Andrews, Ghosh, Rias*, Fundamentals of WiMAX: Understanding Broadband Wireless Networking; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

[6] Under the "One Laptop per Child" initiative, inexpensive laptop computers should be distributed to children, especially those in developing countries. The project is organized by the United States-based non-profit organization OLPC. For more information, see the official OLPC website at www.laptop.org. Regarding the technology of the laptop, see Heise News, Test of the 100 dollar laptop, 09.05.2007, available at: www.heise.de/english/newsticker/news/89512.

[7] Current reports highlight that around 11 per cent of the African population has access to the Internet. See www.internetworldstats.com/stats1.htm.

[8] Regarding the impact of ICT on society, see the report Sharpening Europe's Future Through ICT – Report from the information society technologies advisory group, 2006, available at: ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-shaping-europe-future-ict-march-2006-en.pdf.

[9] Regarding the related risks of attacks against e-mail systems, see the report that United States Department of Defense had to shut down their e-mail system after a hacking attack. See: www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

[10] Regarding the ability to block Internet-based information services by denial-of-service attacks, see below: § 2.5.5.

[11] Regarding the related difficulties of lawful interception of Voice over IP communication, see: *Bellovin and others*, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP", available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, "Voice over IP: Forensic Computing Implications", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[12] *ITU*, ICT Applications and Cybersecurity Background Note to the 2009 Pacific ICT Ministerial Forum held in Tonga 17-20 February 2009, 2009, available at: www.itu.int/ITU-D/asp/CMS/Events/2009/PacMinForum/doc/Background%20Note-Theme-4-ICT%20Apps%20&%20Cybersecurity.pdf.

[13] Regarding the possibilities of low-cost access the Internet in developing countries, see: *Esteve/Machin*, Devices to access Internet in developing countries, available at: www2007.org/workshops/paper_106.pdf.

[14] Regarding the number of users of free-or-charge e-mail services, see: *Graham*, Email carriers deliver gifts of ninety features to lure, keep users, USA Today, 16.04.2008, available at: www.usatoday.com/tech/products/2008-04-15-google-gmail-webmail_N.htm. The article mentions that the four biggest webmail providers have several hundred million users – Microsoft (256 million), Yahoo (254 million), Google (91 million) and AOL (48 million). For an overview on

e-mail statistics, see: *Brownlow*, e-mail and web statistics, April 2008, available at: www.email-marketing-reports.com/metrics/email-statistics.htm.

[15] www.wikipedia.org

[16] Regarding the use of free-of-charge services in criminal activities, see for example: Symantec Press Release, Symantec Reports Malicious Web Attacks Are on the Rise, 13.05.2008, available at: www.symantec.com/business/resources/articles/article.jsp?aid=20080513_symantec_reports_malicious_web_attacks_are_on_the_rise.

[17] Unlike in the industrial society, members of the information society are no longer connected by their participation in industrialization, but through their access to and the use of ICTs. For more information on the information society, see: *Masuda*, The Information Society as Post-Industrial Society; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; *Hornby/Clarke*, Challenge and Change in the Information Society.

[18] See for example: Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions, Challenges for the European Information Society beyond 2005, page 3, available at: http://ec.europa.eu/information_society/eeurope/i2010/docs/communications/new_chall_en_adopted.pdf.

[19] Regarding the impact of ICT on the development of the society, see: *Barney*, Prometheus Wired: The Hope for Democracy in the Age of Network Technology, 2001; *Yang*, Between Democracy and Development: The impact of new information technologies on civil societies in China, available at: http://programs.ssrc.org/itic/publications/civsocandgov/yangpolicyrevised.pdf; *White*, Citizen Electronic: Marx and Gilder on Information Technology and Democracy, Journal of Information Technology impact, 1999, Vol. 1, page 20, available at: www.jiti.com/v1n1/white.pdf.

[20] Regarding the extent of integration of ICTs into the daily lives and the related threats, see: § 3.2.1 below, as well as *Goodman*, The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 69, available at: http://media.hoover.org/documents/0817999825_69.pdf.

[21] See UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211, page 1; *Sieber*, The Threat of Cybercrime, Organised crime in Europe: the threat of Cybercrime, page 212; ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 14, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[22] See *Suter*, A Generic National Framework For Critical Information Infrastructure Protection, 2007, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/background-paper-suter-C5-meeting-14-may-2007.pdf.

[23] *Bohn/Coroama/Langheinrich/Mattern/Rohs,* Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications, Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 *et seq.*, available at: www.vs.inf.ethz.ch/res/papers/hera.pdf.

[24] See *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1, page 1; *Wilshusen*, Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan, Testimony before the Subcommittee on Information Policy, 2007, GAO Document GAO-08-212T, available at: www.gao.gov/new.items/d08212t.pdf.

[25] Regarding the attack against online service in Estonia, see: *Toth*, Estonia under cyberattack, available at: www.cert.hu/dmdocuments/Estonia_attack2.pdf. Regarding the attacks against major online companies in the United States in 2000, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 14, available at: http://media.hoover.org/documents/0817999825_1.pdf. The attacks took place between 07.02.2000 and 09.02.2000. For a full list of attacked companies and the dates of the attacks, see: *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf.

[26] The Online-Community HackerWatch publishes reports on hacking attacks. Based on their sources, more than 219 million incidents were reported in one month (November 2010). Source: www.hackerwatch.org. Regarding the necessary differentiation between port scans and possible attempts to break into a computer system, see: *Panjwani/Tan/Jarrin/Cukier*, An Experimental Evaluation to Determine if Port Scans are Precursors to an Attacks, available at: www.enre.umd.edu/faculty/cukier/81_cukier_m.pdf.

[27] See *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3.

[28] CRS Report for Congress on the Economic Impact of Cyber-Attacks, April 2004, page 10, available at: www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

[29] See: *O'Connell*, Cyber-Crime hits $ 100 Billion in 2007, ITU News related to ITU Corporate Strategy, 17.10.2007, available at: www.ibls.com/internet_law_news_portal_view_prn.aspx?s=latestnews&id=1882.

[30] IBM survey, published 14.05.2006, available at: www-03.ibm.com/industries/consumerproducts/doc/content/news/pressrelease/1540939123.html.

[31] *Wilshuse*n, Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan, Testimony before the Subcommittee on Information Policy, 2007, GAO Document GAO-08-212T, available at: www.gao.gov/new.items/d08212t.pdf. For more information on the economic impact of cybercrime, see below: § 2.4.

[32] Regarding the discovery and functions of the computer virus, see: *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Under the Microscope, Rev. 1.2, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[33] Cyber Security Communique, American Gas Association, 2010, available at: www.aga.org/membercenter/gotocommitteepages/NGS/Documents/1011StuxnetMalware.pdf.

[34] *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Under the Microscope, Rev. 1.2, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

[35] UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

[36] The term "Cybersecurity" is used to summarize various activities and ITU-T Recommendation X.1205 "Overview of cybersecurity" provides a definition, description of technologies, and network protection principles: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted and/or stored information in the cyberenvironment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyberenvironment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality." Also see: *ITU*, List of Security-Related Terms and Definitions, available at: www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc.

[37] With regard to development related to developing countries, see: ITU Cybersecurity Work Programme to Assist Developing Countries 2007-2009, 2007, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

[38] See for example: ITU WTSA Resolution 50 (Rev. Johannesburg, 2008), on Cybersecurity, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52 (Rev. Johannesburg, 2008), on Countering and combating spam, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45 (Doha, 2006), on Mechanism for enhancing cooperation on cybersecurity, including combating spam, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf; European Union Communication: Towards a General Policy on the Fight Against Cyber Crime, 2007, available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf; Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, 2005, available at: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

[39] For more information, references and links, see: the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009), 2007, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

[40] For more information, see: *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1.

[41] See: *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, available at: www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf; see also: Pillar One of the ITU Global Cybersecurity Agenda, available at:

www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html. With regard to the elements of an anti-cybercrime strategy, see below: §4.

[42] See in this context: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 14, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[43] For more information on the World Summit on the Information Society (WSIS), see: www.itu.int/wsis/

[44] The WSIS Tunis Agenda for the Information Society, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0

[45] The WSIS Geneva Plan of Action, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0

[46] For more information on WSIS Action Line C5: Building confidence and security in the use of ICTs, see: www.itu.int/wsis/c5/

[47] For more information on the Global Cybersecurity Agenda (GCA), see: www.itu.int/cybersecurity/gca/

[48] For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[49] For an overview of the most important instruments in the fight against cybercrime, see below: § 6.5.

[50] *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141. For an overview of the most important substantive criminal law provisions, see below: § 6.2.

[51] See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, 245 *et seq.*

[52] For an overview of cybercrime-related legislation and its compliance with the best practices defined by the Convention on Cybercrime, see the country profiles provided on the Council of Europe website, available at: www.coe.int/cybercrime/. See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

[53] See below: § 6.2.

[54] See below: § 6.5.

[55] For an overview of the most relevant challenges in the fight against cybercrime, see below: § 3.2.

[56] One possibility to mask the identity is the use of anonymous communication services. See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999. Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf. Regarding anonymous file-sharing systems see: *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Design, 2005.

[57] Regarding legal responses to the challenges of anonymous communication, see below: § 6.5.12 and § 6.5.13.

[58] Regarding the transnational dimension of cybercrime, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[59] Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management, 2005.

[60] Regarding the need for international cooperation in the fight against cybercrime, see: Putnam/Elliott, International Responses to Cyber Crime, in *Sofaer/Goodman*, Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 *et seq.*, available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[61] See below: § 6.5.

[62] *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141.

[63] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf; *Plachta*, International Cooperation in the Draft United Nations Convention against Transnational Crimes, UNAFEI Resource Material Series No. 57, 114th International Training Course, page 87 *et seq.*, available at: www.unafei.or.jp/english/pdf/PDF_rms/no57/57-08.pdf.

[64] See below: § 5.5. See for example the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide, 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

[65] The different legal traditions with regard to illegal content was one reason why certain aspects of illegal content are not included in the Council of Europe Convention on Cybercrime, but addressed in an additional protocol. See below: § 5.2.1.

[66] With regard to the different national approaches towards the criminalization of child pornography, see for example: *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet, 1999.

[67] Regarding network protocols, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

[68] The most important communication protocols are TCP (Transmission Control Protocol) and IP (Internet Protocol). For further information, see: *Tanebaum*, Computer Networks, 2002; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture, 2006.

[69] Regarding technical standardization, see: OECD, Internet Address Space, Economic Consideration in the Management of IPv4 and in the Development of IPv6, 2007, DSTI/ICCP(2007)20/FINAL, available at: www.itu.int/dms_pub/itu-t/oth/06/15/T061500000A0015PDFE.pdf. Regarding the importance of single technical as well as single legal standards, see: *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 *et seq.*

[70] Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (CETS No. 189), available at: www.conventions.coe.int.

[71] Since parties participating in the negotiation could not agree on a common position on the criminalization of the dissemination of xenophobic material, provisions related to this topic were integrated into a First Protocol to the Council of Europe Convention on Cybercrime.

[72] See: *Zittrain*, History of Online Gatekeeping, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.,* available at: http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech253.pdf.

[73] This was discussed for example within the famous Yahoo-decision. See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: www.juriscom.net/en/uni/doc/yahoo/poullet.htm; *Goldsmith/Wu*, Who Controls the Internet?: Illusions of a Borderless World, 2006, page 2 *et seq.*

[74] A possibility to circumvent geo-targeting strategies is the use of proxy servers that are located abroad.

[75] The OpenNet Initiative is a transatlantic group of academic institutions that reports about Internet filtering and surveillance. Among others, the Harvard Law School and the University of Oxford participate in the network. For more information, see: www.opennet.net.

[76] *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[77] See below:§ 4.

[78] See, with regard to the costs of technical protection measures required to fight against spam: *OECD*, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4, available at www.oecd.org/dataoecd/5/47/34935342.pdf.

[79] Regarding cybersecurity in developing countries, see: World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

[80] One example is spam. The term "spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: "ITU Survey on Anti-Spam Legislation Worldwide 2005", page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. Due to their limited resources, spam may pose a more serious issue for developing countries than for industrialized countries. See: OECD, Spam Issue in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[81] For more details about the elements of an anti-cybercrime strategy, see below:§ 4.

# 2. The phenomena of cybercrime

## 2.1 Definitions

**Bibliography (selected):** Carter, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf; Charney, Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41, Issue 7, page 489 et seq., Chawki, Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview/; Forst, Cybercrime: Appellate Court Interpretations, 1999, page 1; Goodman, Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469; Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, International Journal of Law and Information Technology, 2002, Vol. 10, No.2, page 144; Gordon/Ford, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; Hale, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37; Hayden, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3; Sieber in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004; Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf.

Most reports, guides or publications on cybercrime begin by defining the terms[82] "computer crime" and "cybercrime".[83] In this context, various approaches have been adopted in recent decades to develop a precise definition for both terms.[84] Before providing an overview of the debate and evaluating the approaches, it is useful to determine the relationship between "cybercrime" and "computer-related crimes".[85] Without going into detail at this stage, the term "cybercrime" is narrower than computer-related crimes as it has to involve a computer network. Computer-related crimes cover even those offences that bear no relation to a network, but only affect stand-alone computer systems.

During the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, two definitions were developed within a related workshop:[86] Cybercrime in a narrow sense (computer crime) covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them. Cybercrime in a broader sense (computer-related crimes) covers any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.[87]

One common definition describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity.[88] There are several difficulties with this broad definition. It would, for example, cover traditional crimes such as murder, if perchance the offender used a keyboard to hit and kill the victim. Another broader definition is provided in Article 1.1 of the Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (the "Stanford Draft"),[89] which points out that cybercrime refers to acts in respect to cybersystems.[90]

Some definitions try to take objectives or intentions into account and define cybercrime more precisely[91], such as "computer-mediated activities which are either *illegal or considered illicit* by certain parties and which can be conducted *through global electronic networks*".[92] These more refined descriptions exclude cases where physical hardware is used to commit regular crimes, but they risk excluding crimes that are considered as cybercrime in international agreements such as the Commonwealth Model Law on Computer and Computer-related Crime or the Council of Europe Convention on Cybercrime.[93] For example, a person who produces USB[94] devices containing malicious software that destroys data on computers when the device is connected commits a crime as defined by Article 4 of the Convention on Cybercrime.[95] However, since the act of deleting data using a physical device to copy malicious code has

not been committed through global electronic networks, it would not qualify as cybercrime under the narrow definition above. Such acts would only qualify as cybercrime under a definition based on a broader description, including acts such as illegal data interference.

The variety of approaches, as well as the related problems, demonstrates that there are considerable difficulties in defining the terms "computer crime" and "cybercrime".[96] The term "cybercrime" is used to describe a range of offences including traditional computer crimes, as well as network crimes. As these crimes differ in many ways, there is no single criterion that could include all acts mentioned in the different regional and international legal approaches to address the issue, whilst excluding traditional crimes that are just facilitated by using hardware. The fact that there is no single definition of "cybercrime" need not be important, as long as the term is not used as a legal term.[97] Instead of referring to a definition, the following chapters will be based on a typology-related approach.

## 2.2 Typology of cybercrime

Bibliography: *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview; *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2003, available at: www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf; *Sieber* in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004.

The term "cybercrime" is used to cover a wide variety of criminal conduct.[98] As recognized crimes include a broad range of different offences, it is difficult to develop a typology or classification system for cybercrime.[99] One approach can be found in the Convention on Cybercrime,[100] which distinguishes between four different types of offences[101]:

1. offences against the confidentiality, integrity and availability of computer data and systems;[102]
2. computer-related offences;[103]
3. content-related offences;[104] and
4. copyright-related offences.[105]

This typology is not wholly consistent, as it is not based on a sole criterion to differentiate between categories. Three categories focus on the object of legal protection: "offences against the confidentiality, integrity and availability of computer data and systems"[106]; content-related offences[107]; and copyright-related offences[108]. The fourth category of "computer-related offences"[109] does not focus on the object of legal protection, but on the method used to commit the crime. This inconsistency leads to some overlap between categories.

In addition, some terms that are used to describe criminal acts (such as "cyberterrorism"[110] or "phishing"[111]) cover acts that fall within several categories. Nonetheless, the four categories can serve as a useful basis for discussing the phenomena of cybercrime.

## 2.3 Development of computer crime and cybercrime

The criminal abuse of information technology and the necessary legal response are issues that have been discussed ever since the technology was introduced. Over the last 50 years, various solutions have been implemented at the national and regional levels. One of the reasons why the topic remains challenging is the constant technical development, as well as the changing methods and ways in which the offences are committed.

### *2.3.1 The 1960s*

In the 1960s, the introduction of transistor-based computer systems, which were smaller and less expensive than vacuum-tube based machines, led to an increase in the use of computer technology.[112] At this early stage, offences focused on physical damage to computer systems and stored data.[113] Such

incidents were reported, for example, in Canada, where in 1969 a student riot caused a fire that destroyed computer data hosted at the university.[114] In the mid 1960s, the United States started a debate on the creation of a central data-storage authority for all ministries.[115] Within this context, possible criminal abuse of databases[116] and the related risks to privacy[117] were discussed.[118]

### 2.3.2 The 1970s

In the 1970s, the use of computer systems and computer data increased further.[119] At the end of the decade, an estimated number of 100 000 mainframe computers were operating in the United States.[120] With falling prices, computer technology was more widely used within administration and business, and by the public. The 1970s were characterized by a shift from the traditional property crimes against computer systems[121] that had dominated the 1960s, to new forms of crime.[122] While physical damage continued to be a relevant form of criminal abuse against computer systems,[123] new forms of computer crime were recognized. They included the illegal use of computer systems[124] and the manipulation[125] of electronic data.[126] The shift from manual to computer-operated transactions led to another new form of crime – computer-related fraud.[127] Already at this time, multimillion dollar losses were caused by computer-related fraud.[128] Computer-related fraud, in particular, was a real challenge, and law-enforcement agencies were investigating more and more cases.[129] As the application of existing legislation in computer-crime cases led to difficulties,[130] a debate about legal solutions started in different parts of the world.[131] The United States discussed a draft bill designed specifically to address cybercrime.[132] Interpol discussed the phenomena and possibilities for legal response.[133]

### 2.3.3 The 1980s

In the 1980s, personal computers became more and more popular. With this development, the number of computer systems and hence the number of potential targets for criminals again increased. For the first time, the targets included a broad range of critical infrastructure.[134] One of the side effects of the spread of computer systems was an increasing interest in software, resulting in the emergence of the first forms of software piracy and crimes related to patents.[135] The interconnection of computer systems brought about new types of offence.[136] Networks enabled offenders to enter a computer system without being present at the crime scene.[137] In addition, the possibility of distributing software through networks enabled offenders to spread malicious software, and more and more computer viruses were discovered.[138] Countries started the process of updating their legislation so as to meet the requirements of a changing criminal environment.[139] International organizations also got involved in the process. OECD[140] and the Council of Europe[141] set up study groups to analyse the phenomena and evaluate possibilities for legal response.

### 2.3.4 The 1990s

The introduction of the graphical interface ("WWW") in the 1990s that was followed by a rapid growth in the number of Internet users led to new challenges. Information legally made available in one country was available globally – even in countries where the publication of such information was criminalized.[142] Another concern associated with online services that turned out to be especially challenging in the investigation of transnational crime was the speed of information exchange.[143] Finally, the distribution of child pornography moved from physical exchange of books and tapes to online distribution through websites and Internet services.[144] While computer crimes were in general local crimes, the Internet turned electronic crimes into transnational crime. As a result, the international community tackled the issue more intensively. UN General Assembly Resolution 45/121 adopted in 1990[145] and the manual for the prevention and control of computer-related crimes issued in 1994 are just two examples.[146]

### 2.3.5 The 21st Century

As in each preceding decade, new trends in computer crime and cybercrime continued to be discovered in the 21st century. The first decade of the new millennium was dominated by new, highly sophisticated methods of committing crimes, such as "phishing",[147] and "botnet attacks",[148] and the emerging use of technology that is more difficult for law enforcement to handle and investigate, such as "voice-over-IP

(VoIP) communication"[149] and "cloud computing".[150] It is not only the methods that changed, but also the impact. As offenders became able to automate attacks, the number of offences increased. Countries and regional and international organizations have responded to the growing challenges and given response to cybercrime high priority.

## 2.4 Extent and impact of cybercrime offences

**Bibliography (selected):** Alvazzi del Frate, Crime and criminal justice statistics challenges in Harrendorf/Heiskanen/Malby, International Statistics on Crime and Justice, 2010, page 168, available at: www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf; Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 308, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf; Hyde-Bales/Morris/Charlton, The police recording of computer crime, UK Home Office Development and Practice Report, 2004; Maguire in Maguire/Morgan/Reiner, The Oxford Handbook of Criminology, 2007, page 241 et seq., available at: www.oup.com/uk/orc/bin/9780199205431/maguire_chap10.pdf; Mitchison/Urry, Crime and Abuse in e-Business, IPTS Report, available at: www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm; Osborne/Wernicke, Introduction to Crime Analysis, 2003, page 1 et seq. available at: www.crim.umontreal.ca/cours/cri3013/osborne.pdf; Walden, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

Crime statistics can be used by academia and policy-makers as a basis for discussion and for the ensuing decision-making process.[151] Furthermore, access to precise information on the true extent of cybercrime would enable law-enforcement agencies to improve anti-cybercrime strategies, deter potential attacks and enact more appropriate and effective legislation. However, it is difficult to quantify the impact of cybercrime on society on the basis of the number of offences carried out in a given time-frame.[152] Such data can in general be taken from crime statistics and surveys,[153] but both these sources come with challenges when it comes to using them for formulating policy recommendations.

### *2.4.1 Crime statistics*

The following numbers have been extracted from national crime statistics. As further discussed below, they are not intended to be representative of either the global development of cybercrime or of the true extent of cybercrime at the national level, and are thus presented only to provide an insight into country information.

- The US Internet Complaint Center reports a 22.3 per cent increase in complaints submitted relating to cybercrime compared with 2008.[154]
- German Crime Statistics indicate that the overall number of Internet-related crimes increased in 2009 by 23.6 per cent compared with 2008.[155]

It is unclear how representative the statistics are and whether they provide reliable information on the extent of crime.[156] There are several difficulties associated with determining the global threat of cybercrime on the basis of crime statistics.[157]

First of all, crime statistics are generally created at the national level and do not reflect the international scope of the issue. Even though it would theoretically be possible to combine the available data, such an approach would not yield reliable information because of variations in legislation and recording practices.[158] Combining and comparing national crime statistics requires a certain degree of compatibility[159] that is missing when it comes to cybercrime. Even if cybercrime data are recorded, they are not necessarily listed as a separate figure.[160] Furthermore, statistics only list crimes that are detected and reported.[161] Especially with regard to cybercrime, there are concerns that the number of unreported cases is significant.[162] Businesses may fear that negative publicity could damage their reputation.[163] If a company announces that hackers have accessed their server, customers may lose faith. The full costs and consequences could be greater than the losses caused by the hacking attack. On the other hand, if offenders are not reported and prosecuted, they may go on to re-offend. Victims may not believe that

law-enforcement agencies will be able to identify offenders.[164] Comparing the large number of cybercrimes with the few successful investigations, they may see little point in reporting offences.[165] As automation of attacks enables cybercriminals to pursue a strategy of reaping large profits from many attacks targeting small amounts (e.g. as is the case with advance fee fraud[166]), the possible impact of unreported crimes could be significant. For only small amounts, victims may prefer not to go through time-consuming reporting procedures. Reported cases are often the ones that involve very large amounts.[167]

In summary, statistical information is useful to draw attention to the continuing and growing importance of the issue, and it is necessary to point out that one of the major challenges related to cybercrime is the lack of reliable information on the extent of the problem, as well as on arrests, prosecutions and convictions. As already stated, crime statistics often do not list offences separately, and available statistics on the impact of cybercrime are in general unable to provide reliable information about the scale or extent of offences at a level sufficient for policy-makers.[168] Without such data, it is difficult to quantify the impact of cybercrime on society and to develop strategies to address the issue.[169] Nevertheless, the statistics can serve as a basis for determining trends, which can be found by comparing results over several years, and serve as guidance with regard to the process of reporting cybercrime.[170]

### 2.4.2 Surveys

The following numbers have been extracted from different surveys. As further discussed below, they are not necessarily representative, and are thus presented only to give an insight into the results of such surveys.

- Credit card and bank account information are among the most popular information advertised on underground economy services. The prices range between USD 0.85-USD 30 (single credit card information) and USD 15-USD 850 (single bank account information).[171]
- In 2007, auction fraud was among the top Internet scams in the US, with an average loss of more than USD 1 000 per case.[172]
- In 2005, losses as a result of identity-related offences in the US totalled USD 56.6 billion.[173]
- The financial and personal cost of cybercrime varies significantly among single incidents in Ireland, generating aggregate costs of over EUR 250 000.[174]
- A single computer security company created more than 450 000 new malicious code signatures in a single quarter.[175]
- A quarter of all companies responding to a questionnaire in 2010 reported operational losses as a result of cybercrime.[176]
- Decreasing number of denial-of-service and computer-virus attacks reported by security professionals between 2004 and 2008.[177]
- In 2009, the United States, China, Brazil, Germany and India were among the countries reporting most malicious activities.[178]

There are several concerns related to the use of such surveys in determining the extent and impact of cybercrime.

It is very difficult to provide reliable estimations of financial losses. Some sources estimate losses to businesses and institutions in the United States[179] due to cybercrime to be as high as USD 67 billion in a single year; however, it is uncertain whether the extrapolation of sample survey results is justifiable.[180] This methodological criticism applies not only to losses, but also to the number of recognized offences.

Another difficulty related to statistical information is the fact that very often either unreliable or non-verifiable information is repeatedly quoted. One example of this relates to statistical information on the commercial aspects of Internet child pornography. Several analyses quote, for example, that TopTenReviews estimated that Internet child pornography generates USD 2.5 billion annually

worldwide.[181] Yet TopTenReviews does not provide any background information on how the research was undertaken. Bearing in mind that TopTenReview claims on its website that the company "*gives you the information you need to make a smart purchase. We make a recommendation for the best product in each category. Through our side-by-side comparison charts, news, articles, and videos we simplify the buying process for consumers*", there may be serious concerns as to the use of such data. Another example of figures quoted without verifiable reference was discovered by the Wall Street Journal in 2006.[182] While investigating a quotation that child pornography is a multi-billion dollar business (USD 20 billion a year), the journalist reported that two main documents containing information about revenues from USD 3 billion to 20 billion – a publication from NCMEC and one from the Council of Europe – referred to institutions that did not confirm the numbers.

As surveys often only count incidents without providing further information or details, it is difficult to draw conclusions with regard to trends. One example is the United States CSI[183] Computer Crime and Security Survey 2007 that analyses the number of computer-related offences committed, among other trends.[184] It is based on the responses of 494 computer security practitioners from US corporations, government agencies and financial institutions in the US.[185] The survey documents the number of offences reported by respondents between 2000 and 2007. It shows that, since 2001, the proportion of respondents who experienced and acknowledged virus attacks or unauthorized access to information (or system penetration) decreased. The survey does not explain why this decrease has occurred.

The surveys on cybercrime are unable to provide reliable information about the scale or extent of offences.[186] The uncertainty about the extent to which offences are reported by targets[187], as well as the fact that no explanation for the reducing numbers of cybercrimes can be found, render these statistics open to interpretation. At present, there is insufficient evidence for predictions on future trends and developments.

## 2.5 Offences against the confidentiality, integrity and availability of computer data and systems

**Bibliography (selected):** Chawki/Abdel Wahab, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; Ealy, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf; Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; Hackworth, Spyware, Cybercrime & Security, IIA-4; Kabay, A Brief History of Computer Crime: An Introduction for Students, 2008; Ollmann, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf; Paxson, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; Sieber, Council of Europe Organised Crime Report 2004; Szor, The Art of Computer Virus Research and Defence, 2005; Urbas/Krone, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: www.aic.gov.au/publications/tandi2/tandi329t.html; Walden, Computer Crimes and Digital Investigations, 2006, Chapter 3.250; Yee, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 et seq.

All offences in this category are directed against (at least) one of the three legal principles of confidentiality, integrity and availability. Unlike crimes that have been covered by criminal law for centuries (such as theft or murder), the computerization of offences is relatively recent, as computer systems and computer data were only developed around 60 years ago.[188] The effective prosecution of these acts requires that existing criminal law provisions not only protect tangible items and physical documents from manipulation, but also extend to include these new legal principles.[189] This section gives an overview of the most commonly occurring offences included in this category.

### 2.5.1 Illegal access (hacking, cracking)[190]

The offence described as "hacking" refers to unlawful access to a computer system[191], one of oldest computer-related crimes.[192] Following the development of computer networks (especially the Internet), this crime has become a mass phenomenon.[193] Famous targets of hacking attacks include the US National Aeronautics and Space Administration (NASA), the US Air Force, the Pentagon, Yahoo, Google, eBay and the German Government.[194]

Examples of hacking offences include breaking the password of password-protected websites[195] and circumventing password protection on a computer system. But acts related to the term "hacking" also include preparatory acts such as the use of faulty hardware or software implementation to illegally obtain a password to enter a computer system[196], setting up "spoofing" websites to make users disclose their passwords[197] and installing hardware and software-based keylogging methods (e.g. "keyloggers") that record every keystroke – and consequently any passwords used on the computer and/or device.[198]

The motivation of offenders varies. Some offenders limit their activities to circumventing security measures only in order to prove their abilities.[199] Others act through political motivation (known as "hacktivism"[200]) – one example is a recent incident involving the main United Nations website.[201] In most cases, though, the motivation of the offender is not limited to illicit access to a computer system. Offenders use this access to commit further crimes, such as data espionage, data manipulation or denial-of-service (DoS) attacks.[202] In most cases, illegal access to the computer system is only a vital first step.[203]

Many analysts recognize a rising number of attempts to illegally access computer systems, with over 250 million incidents recorded worldwide during the month of August 2007 alone.[204] Three main factors have supported the increasing number of hacking attacks: inadequate and incomplete protection of computer systems, development of software tools that automate the attacks, and the growing role of private computers as a target of hacking attacks.

#### Inadequate and incomplete protection of computer systems

Hundreds of millions of computers are connected to the Internet, and many computer systems are without adequate protection in place to prevent illegal access.[205] Analysis carried out by the University of Maryland suggests that an unprotected computer system that is connected to the Internet is likely to experience attack within less than a minute.[206] The installation of protective measures can lower the risk, but successful attacks against well-protected computer systems prove that technical protection measures can never completely stop attacks.[207]

#### Development of software tools that automate the attacks

Recently, software tools are being used to automate attacks.[208] With the help of software and pre-installed attacks, a single offender can attack thousands of computer systems in a single day using one computer.[209] If the offender has access to more computers – e.g. through a botnet[210] – he/she can increase the scale still further. Since most of these software tools use preset methods of attacks, not all attacks prove successful. Users that update their operating systems and software applications on a regular basis reduce their risk of falling victim to these broad-based attacks, as the companies developing protection software analyse attack tools and prepare for the standardized hacking attacks.

High-profile attacks are often based on individually-designed attacks. The success of those attacks is often not the result of highly sophisticated methods, but the number of attacked computer systems. Tools enabling these standardized attacks are widely available over the Internet[211] – some for free, but efficient tools can easily cost several thousand US dollars.[212] One example is a hacking tool that allows the offender to define a range of IP-addresses (e.g. from 111.2.0.0 to 111.9.253.253). The software allows for the scanning for unprotected ports of all computers using one of the defined IP-addresses.[213]

#### The growing role of private computers as a target of hacking attacks

Access to a computer system is often not the primary motivation of an attack.[214] Since business computers are generally better protected than private computers, attacks on business computers are more difficult

to carry out using pre-configured software tools.[215] Over the past few years, offenders have focused their attacks increasingly on private computers, since many private computers are inadequately protected. Further, private computers often contain sensitive information (e.g. credit card and bank account details). Offenders are also targeting private computers because, after a successful attack, offenders can include the computer in their botnet and use the computer for further criminal activities.[216]

Illegal access to a computer system may be viewed as analogous to illegal access to a building and is recognized as a criminal offence in many countries.[217] Analysis of different approaches to the criminalization of computer access shows that enacted provisions in some cases confuse illegal access with subsequent offences or attempt to limit criminalization of illegal access to grave violations only. Some provisions criminalize the initial access, while other approaches limit the criminal offence only to those cases where the accessed system is protected by security measures[218] or the perpetrator has harmful intentions[219] or data was obtained, modified or damaged. Other legal systems do not criminalize mere access, but focus on subsequent offences.[220]

### 2.5.2 Illegal data acquisition (data espionage)

Sensitive information is often stored in computer systems. If the computer system is connected to the Internet, offenders can try to access this information via the Internet from almost any place in the world.[221] The Internet is increasingly used to obtain trade secrets.[222] The value of sensitive information and the ability to access it remotely makes data espionage highly interesting. In the 1980s, a number of German hackers succeeded in entering US government and military computer systems, obtaining secret information and selling this information to agents from a different country.[223]

Offenders use various techniques to access victims' computers,[224] including software to scan for unprotected ports [225] or circumvent protection measures,[226] as well as "social engineering".[227] The last approach especially, which refers to a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people into breaking normal security procedures, is interesting as it not based on technical means.[228] In the context of illegal access it describes the manipulation of human beings with the intention of gaining access to computer systems.[229] Social engineering is usually very successful, because the weakest link in computer security is often the users operating the computer system. One example is "phishing", which has recently become a key crime committed in cyberspace[230] and describes attempts to fraudulently acquire sensitive information (such as passwords) by masquerading as a trustworthy person or business (e.g. financial institution) in a seemingly official electronic communication.

Although the human vulnerability of users opens the door to the risk of scams, it also offers solutions. Well-educated computer users are not easy victims for offenders using social engineering. As a consequence, user education should be an essential part of any anti-cybercrime strategy.[231] In addition, technical measures can be taken to prevent illegal access. OECD highlights the importance of cryptography for users, as cryptography can help improve data protection.[232] If the person or organization storing information uses proper protection measures, cryptographic protection can be more efficient than any physical protection.[233] The success of offenders in obtaining sensitive information is often due to the absence of protection measures. Since important information is increasingly being stored in computer systems, it is essential to evaluate whether the technical protection measures taken by the users are adequate, or if law-makers need to establish additional protection by criminalizing data espionage.[234]

Although offenders usually target business secrets, data stored on private computers are also increasingly targeted.[235] Private users often store bank-account and credit-card information on their computer.[236] Offenders can use this information for their own purposes (e.g. bank-account details to make money transfers) or sell it to a third party.[237] Credit-card records are for example sold for up to USD 60.[238] Hackers' focus on private computers is interesting, as the profits from business secrets are generally higher than the profits to be made from obtaining or selling single credit-card information. However, since private computers are generally less well protected, data espionage based on private computers is likely to become even more profitable.

There are two approaches to obtaining information. Offenders can access a computer system or data storage device and extract information; or try to manipulate the user to make them disclose the information or access codes that enable offenders to access information ("phishing").

Offenders often use computer tools installed on victims' computers or malicious software called spyware to transmit data to them.[239] Various types of spyware have been discovered over recent years, such as keyloggers.[240] Keyloggers are software tools that record every keystroke typed on an infected computer's keyboard.[241] Some keyloggers send all recorded information to the offender, as soon as the computer is connected to the Internet. Others perform an initial sort and analysis of the data recorded (e.g. focusing on potential credit-card information[242]) to transmit only major data discovered. Similar devices are also available as hardware devices that are plugged in between the keyboard and the computer system to record keystrokes on the keyboard. Hardware-based keyloggers are more difficult to install and detect, as they require physical access to the computer system.[243] However, classical anti-spyware and anti-virus software is largely unable to identify them.[244]

Apart from accessing computer systems, offenders can also obtain data by manipulating the user. Recently, offenders have developed effective scams to obtain secret information (e.g. bank-account information and credit-card data) by manipulating users using social engineering techniques.[245] "Phishing" has recently become one of the most important crimes related to cyberspace.[246] The term "phishing" is used to describe a type of crime that is characterized by attempts to fraudulently acquire sensitive information, such as passwords, by masquerading as a trustworthy person or business (e.g. financial institution) in an apparently official electronic communication.[247]

### 2.5.3 Illegal interception

Offenders can intercept communications between users[248] (such as e-mails) or other forms of data transfers (when users upload data onto webservers or access web-based external storage media[249]) in order to record the information exchanged. In this context, offenders can in general target any communication infrastructure (e.g. fixed lines or wireless) and any Internet service (e.g. e-mail, chat or VoIP communications[250]).

Most data-transfer processes among Internet infrastructure providers or Internet service providers are well protected and difficult to intercept.[251] However, offenders search for weak points in the system. Wireless technologies are enjoying greater popularity and have in the past proved vulnerable.[252] Nowadays, hotels, restaurants and bars offer customers Internet access through wireless access points. However, the signals in the data exchanges between the computer and the access point can be received within a radius of up to 100 metres.[253] Offenders who wish to intercept a data-exchange process can do so from any location within this radius. Even where wireless communications are encrypted, offenders may be able to decrypt the recorded data.[254]

To gain access to sensitive information, some offenders set up access points close to locations where there is a high demand for wireless access[255] (e.g. near bars and hotels). The station location is often named in such a way that users searching for an Internet access point are more likely to choose the fraudulent access point. If users rely on the access provider to ensure the security of their communication without implementing their own security measures, offenders can easily intercept communications.

The use of fixed lines does not prevent offenders from intercepting communications.[256] Data transmissions passing along a wire emit electromagnetic energy.[257] If offenders use the right equipment, they can detect and record these emissions[258] and may be able to record data transfers between users' computers and the connected system, and also within the computer system.[259]

Most countries have moved to protect the use of telecommunication services by criminalizing the illegal interception of phone conversations. However, given the growing popularity of IP-based services, law-makers may need to evaluate to what extent similar protection is offered to IP-based services.[260]

### 2.5.4 Data interference

Computer data are vital for private users, businesses and administrations, all of which depend on the integrity and availability of data.[261] Lack of access to data can result in considerable (financial) damage. Offenders can violate the integrity of data and interfere with them by deleting, suppressing or altering computer data.[262] One common example of the deletion of data is the computer virus.[263] Ever since computer technology was first developed, computer viruses have threatened users who failed to install proper protection.[264] Since then, the number of computer viruses has risen significantly.[265] Not only has the number of virus attacks increased, but also the techniques and functions of viruses (payload[266]) have changed.

Previously, computer viruses were distributed through storage devices such as floppy disks, whilst today most viruses are distributed via the Internet as attachments either to e-mails or to files that users download.[267] These efficient new methods of distribution have massively accelerated virus infection and vastly increased the number of infected computer systems. The computer worm SQL Slammer[268] was estimated to have infected 90 per cent of vulnerable computer systems within the first 10 minutes of its distribution.[269] The financial damage caused by virus attacks in 2000 alone was estimated to amount to some USD 17 billion.[270] In 2003, it was still more than USD 12 billion.[271]

Most first-generation computer viruses either deleted information or displayed messages. Recently, payloads have diversified.[272] Modern viruses are able to install back-doors enabling offenders to take remote control of the victim's computer or encrypt files so that victims are denied access to their own files, until they pay money to receive the key.[273]

### 2.5.5 System interference

The same concerns over attacks against computer data apply to attacks against computer systems. More businesses are incorporating Internet services into their production processes, with benefits of 24-hour availability and worldwide accessibility.[274] If offenders succeed in preventing computer systems from operating smoothly, this can result in great financial losses for victims.[275]

Attacks can be carried out by physical attacks on the computer system.[276] If offenders are able to access the computer system, they can destroy hardware. For most criminal legal systems, remote physical cases do not pose major problems, as they are similar to classic cases of damage or destruction of property. However, for highly profitable e-commerce businesses, the financial damages caused by attacks on the computer system are often far greater than the mere cost of computer hardware.[277]

More challenging for legal systems are web-based scams. Examples of these remote attacks against computer systems include computer worms[278] and denial-of-service (DoS) attacks.[279]

Computer worms[280] are a subgroup of malware (like computer viruses). They are self-replicating computer programs that harm the network by initiating multiple data-transfer processes. They can influence computer systems by hindering the smooth running of the computer system, using system resources to replicate themselves over the Internet or generating network traffic that can close down availability of certain services (such as websites).

While computer worms generally influence the whole network without targeting specific computer systems, DoS attacks target specific computer systems. A DoS attack makes computer resources unavailable to their intended users.[281] By targeting a computer system with more requests than the computer system can handle, offenders can prevent users from accessing the computer system, checking e-mails, reading the news, booking a flight or downloading files. In 2000, within a short time, several DoS attacks were launched against well-known companies such as CNN, eBay and Amazon.[282] Similar attacks were reported in 2009 on government and commercial websites in the US and South Korea.[283] As a result, some of the services were not available for several hours and even days.[284]

The prosecution of DoS and computer-worm attacks poses serious challenges to most criminal law systems, as these attacks may not involve any physical impact on computer systems. Apart from the basic

need to criminalize web-based attacks,[285] the question of whether the prevention and prosecution of attacks against critical infrastructure needs a separate legislative approach is under discussion.

## 2.6 Content-related offences

**Bibliography (selected):** *Akdeniz*, Governance of Hate Speech on the Internet in Europe, in Governing the Internet Freedom and Regulation in the OSCE Region; *Carr*, Child Abuse, Child Pornography and the Internet, 2004; *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International, 2006, page 144 *et seq.*; *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf; *Healy*, Child Pornography: An International Perspective, 2004; *Jenkins*, Beyond Tolerance, Child Pornography on the Internet, 2001; *Lanning*, Child Molesters: A Behavioral Analysis, 2001; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*; *Siebert*, Protecting Minors on the Internet: An Example from Germany, in Governing the Internet Freedom and Regulation in the OSCE Region, page 150, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf; *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005; *Wortley/Smallbone*, Child Pornography on the Internet, Problem-Oriented Guides for Police, USDOJ, 2006; *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/.

This category covers content that is considered illegal, including child pornography, xenophobic material or insults related to religious symbols.[286] The development of legal instruments to deal with this category is far more influenced by national approaches, which can take into account fundamental cultural and legal principles. For illegal content, value systems and legal systems differ extensively between societies. The dissemination of xenophobic material is illegal in many European countries,[287] but can be protected by the principle of freedom of speech[288] in the United States.[289] The use of derogatory remarks in respect of the Holy Prophet is criminal in many Arabic countries, but not in some European countries.[290]

Legal approaches to criminalize the illegal content should not interfere with the right to freedom of expression. The right to freedom of expression is for example defined by principle 1 (b) of the Johannesburg Principles on National Security and Freedom of Expression.[291] However, principle 1 (c) clarifies that the right to freedom of expression may be subject to restrictions. While a criminalization of illegal content is therefore not *per se* precluded, it has to be strictly limited. Such limitations are especially discussed with regard to the criminalization of defamation.[292] The 2008 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression and others points out that vague notions such as providing communications and the glorification or promotion of terrorism or extremism should not be criminalized.[293]

These legal challenges are complex, as information made available by one computer user in one country can be accessed from nearly anywhere in the world.[294] If "offenders" create content that is illegal in some countries, but not in the country they are operating from, prosecution of the "offenders" is difficult, or impossible.[295]

There is much lack of agreement regarding the content of material and to what degree specific acts should be criminalized. The different national views and difficulties in prosecuting violations committed outside the territory of an investigating country have contributed to the blocking of certain types of content on the Internet. Where agreement exists on preventing access to websites with illegal content hosted outside the country, states can maintain strict laws, block websites and filter content.[296]

There are various approaches to filter systems. One solution requires access providers to install programs analysing the websites being visited and to block websites on a blacklist.[297] Another solution is the installation of filter software on users' computers (a useful approach for parents who wish to control the content their children can view, as well as for libraries and public Internet terminals).[298]

Attempts to control content on the Internet are not limited to certain types of content that are widely accepted to be illegal. Some countries use filter technology to restrict access to websites addressing political topics. OpenNet Initiative[299] reports that censorship is currently practised by about two dozen countries.[300]

### 2.6.1 Erotic or pornographic material (excluding child pornography)

Sexually-related content was among the first content to be commercially distributed over the Internet, which offers advantages to retailers of erotic and pornographic material including:

- exchange of media (such as pictures, movies, live coverage) without the need for cost-intensive shipping;[301]
- worldwide[302] access, reaching a significantly larger number of customers than retail shops;
- the Internet is often viewed as an anonymous medium (often erroneously[303]) – an aspect that consumers of pornography appreciate, in view of prevailing social opinions.

Recent research has identified as many as 4.2 million pornographic websites that may be available on the Internet at any time.[304] Besides websites, pornographic material can be distributed through file-sharing systems[305] and instant messaging systems.

Different countries criminalize erotic and pornographic material to different extents. Some countries permit the exchange of pornographic material among adults and limit criminalization to cases where minors access this kind of material,[306] seeking to protect minors.[307] Studies indicate that child access to pornographic material could negatively influence their development.[308] To comply with these laws, "adult verification systems" have been developed.[309] Other countries criminalize any exchange of pornographic material even among adults,[310] without focusing on specific groups (such as minors).

For countries that criminalize interaction with pornographic material, preventing access to pornographic material is a challenge. Beyond the Internet, authorities can in many instances detect and prosecute violations of the prohibition of pornographic material. On the Internet, however, as pornographic material is often readily available on servers outside the country, enforcement is difficult. Even where authorities are able to identify websites containing pornographic material, they may have no powers to enforce removal of offensive content by providers.

The principle of *national sovereignty* does not generally permit a country to carry out investigations within the territory of another country, without permission from local authorities.[311] Even when authorities seek the support of countries where offensive websites are hosted, successful investigation and criminal sanctions may be hindered by the principle of "dual criminality".[312]

To prevent access to pornographic content, countries with exceptionally strict laws are often limited to prevention (such as filter technology[313]) to limit access to certain websites.[314]

### 2.6.2 Child pornography

The Internet has become a prime channel for the distribution of child pornography. In the 1970s and 1980s, offenders engaging in the exchange of child pornography faced serious threats.[315] At that time, the commercial child pornography market focused mainly on Europe and the US[316] and the material was locally produced, expensive and difficult to obtain.[317] Approaches to buy or sell child pornography entailed a number of risks that no longer – or at least not to a degree – exist today. In the past, producers did not have the capability to develop photography and films.[318] They were dependent on services offered by businesses, which increased the chances of law-enforcement agents identifying child pornography through reports from businesses handling the development.[319] The availability of video cameras changed this situation for the first time.[320] But the risks were not only related to production. Getting access to child pornography was similarly fraught with risks for the offender. Orders were placed by responding to advertisements in newspapers.[321] Means of communication between seller and collector, and hence the market itself, were limited.[322] Until the mid-1990s, child pornography was primarily transported through

postal services, and successful investigations led to the detection of a significant number of offenders.[323] In the view of experts, law enforcement was at that time able to meet the challenges.[324]

The situation changes dramatically with the availability of Internet-based data-exchange applications. While in the past, law enforcement was confronted with analogue material, today the vast majority of discovered material is digital.[325] Since the mid-1990s, offenders have increasingly used network services for the distribution of such material.[326] The resulting problems in terms of detecting and investigating child-pornography cases have been acknowledged.[327] The Internet is today the main channel for trading regular pornography[328] as well as child pornography.[329]

Several reasons for the shift from analogue to digital distribution can be identified. The Internet gives less technically skilled users the impression they can act invisibly from others. If the offender does not employ anonymous communication technology, this impression is erroneous. But the fact that using sophisticated means of anonymous communication can hinder the identification of the offender is a matter of concern in respect of the exchange of child pornography online.[330] In addition, this development has been supported by the decreasing price of technical devices and services used for the production and trading of child pornography, such as recording equipment and hosting services.[331] Since websites and Internet services are open to around two billion Internet users, the number of potential customers has also expanded.[332] There are concerns that the fact that access is easier attracts people who would not have taken the risk of being caught trying to obtain child pornography outside the Internet.[333] With the shift from analogue to digital media, an increasing number of child-pornography images discovered through investigations were reported.[334] Another aspect that probably supported this development is the fact that digital information can in general be duplicated without a loss of quality.[335] While in the past consumers of child pornography wishing to duplicate and trade the material were hindered by the loss in quality from reproduction, today a downloaded file can become the source for further duplications. One of the consequences of this development is that, even when the offender who produced the material in the first place is arrested and his files are confiscated, it becomes difficult to “remove” files once they have been traded over the Internet.[336]

In contrast to differing views on adult pornography, child pornography is broadly condemned and offences related to child pornography are widely recognized as criminal acts.[337] International organizations are engaged in the fight against online child pornography,[338] with several international legal initiatives, including: the 1989 United Nations Convention on the Rights of the Child;[339] the 2003 European Union Council Framework Decision on combating the sexual exploitation of children and child pornography;[340] and the 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, among others.[341]

Sadly, these initiatives seeking to control the network distribution of pornography have proved little deterrent to perpetrators, who use the Internet to communicate and exchange child pornography.[342] An increase in bandwidth has supported the exchange of movies and picture archives.

Research into the behaviour of child pornography offenders shows that 15 per cent of arrested people with Internet-related child pornography in their possession had more than 1 000 pictures on their computer; 80 per cent had pictures of children aged between 6 and 12 years on their computer;[343] 19 per cent had pictures of children younger than the age of 3[344]; and 21 per cent had pictures depicting violence.[345]

The sale of child pornography is highly profitable,[346] with collectors willing to pay great amounts for movies and pictures depicting children in a sexual context.[347] Search engines find such material quickly.[348] Most material is exchanged in password-protected closed forums, which regular users and law-enforcement agencies can rarely access. Undercover operations are thus vital in the fight against child pornography.[349]

Two key factors in the use of ICTs for the exchange of child pornography act as obstacles to the investigation of these crimes:

### 1 The use of virtual currencies and anonymous payment[350]

Cash payment enables buyers of certain goods to hide their identity, so cash is dominant in many criminal businesses. The demand for anonymous payments has led to the development of virtual payment systems and virtual currencies enabling anonymous payment.[351] Virtual currencies may not require identification and validation, preventing law-enforcement agencies from tracing money flows back to offenders. Recently, a number of child pornography investigations have succeeded in using traces left by payments to identify offenders.[352] However, where offenders make anonymous payments, it is difficult for them to be tracked.[353] If such anonymous currencies are used by criminals it restricts the ability of law enforcement to identify suspects by following money transfers[354] – for example in cases related to commercial child pornography.[355]

#### 2 The use of encryption technology[356]

Perpetrators are increasingly encrypting their messages. Law-enforcement agencies note that offenders are using encryption technology to protect information stored on their hard disks,[357] seriously hindering criminal investigations.[358]

In addition to a broad criminalization of acts related to child pornography, other approaches such as the implementation of obligations on Internet services to register users or to block or filter the access to websites related to child pornography are currently under discussion.[359]

### *2.6.3 Racism, hate speech, glorification of violence*

Radical groups use mass communication systems such as the Internet to spread propaganda.[360] The number of websites offering racist content and hate speech has risen in recent years[361] – a study in 2005 suggested a rise of 25 per cent in the number of webpages promoting racial hatred, violence and xenophobia between 2004 and 2005.[362] In 2006, over 6 000 such websites existed on the Internet.[363]

Internet distribution offers several advantages for offenders, including lower distribution costs, non-specialist equipment and a global audience. Examples of incitement-to-hatred websites include websites presenting instructions on how to build bombs.[364] Besides propaganda, the Internet is used to sell certain goods, e.g. Nazi-related items such as flags with symbols, uniforms and books, readily available on auction platforms and specialized web-shops.[365] The Internet is also used to send e-mails and newsletters and distribute video clips and television shows through popular archives such as YouTube.

Not all countries criminalize these offences.[366] In some countries, such content may be protected by principles of freedom of speech.[367] Opinions differ as to how far the principle of freedom of expression applies with regard to certain topics, often hindering international investigations. One example of conflict of laws is the case involving the service provider Yahoo! in 2001, when a French court ordered Yahoo! (based in the US) to block the access of French users to Nazi-related material.[368] Based on the First Amendment of the United States Constitution, the sale of such material is legal under United States law. Following the First Amendment, a US court decided that the French order was unenforceable against Yahoo! in the United States.[369]

The disparities between countries on these issues were evident during the drafting of the Council of Europe Convention on Cybercrime. The Convention on Cybercrime seeks to harmonize cybercrime-related laws to ensure that international investigations are not hindered by conflicts of laws.[370] Not all parties engaged in negotiations could agree on a common position on the criminalization of the dissemination of xenophobic material, so this entire topic was excluded from the Convention on Cybercrime and instead addressed in a separate First Protocol.[371] Otherwise, some countries (including the United States) might have been unable to sign the Convention on Cybercrime.

### *2.6.4 Religious offences*

A growing number[372] of websites present material that is in some countries covered by provisions related to religious offences, e.g. anti-religious written statements.[373] Although some material documents objective facts and trends (e.g. decreasing church attendance in Europe), this information may be

considered illegal in some jurisdictions. Other examples include the defamation of religions or the publication of cartoons.

The Internet offers advantages for those who wish to debate or deal critically with a subject – people can leave comments, post material or write articles without having to disclose their identity. Many discussion groups are based on the principle of freedom of speech.[374] Freedom of speech is a key driver behind the Internet's success, with portals that are used specifically for user-generated content.[375] Whilst it is vital to protect this principle, even in the most liberal countries the application of principles of freedom of speech is governed by conditions and laws.

The differing legal standards on illegal content reflect the challenges of regulating content. Even where the publication of content is covered by provisions relating to freedom of speech in the country where the content is available, this material can be accessed from countries with stricter regulations. The "cartoon dispute" in 2005 demonstrated the potential for conflict. The publication of twelve editorial cartoons in the Danish newspaper Jyllands-Posten led to widespread protests across the Muslim world.[376]

As with illegal content, the availability of certain information or material is a criminal offence in some countries. The protection of different religions and religious symbols differs from country to country. Some countries criminalize the use of derogatory remarks in respect of the Holy Prophet[377] or the defiling of copies of the Holy Quran,[378] while other countries may adopt a more liberal approach and may not criminalize such acts.

### 2.6.5 Illegal gambling and online games

Internet games and gambling are one of the fastest-growing areas in the Internet.[379] Linden Labs, the developer of the online game Second Life,[380] reports that some ten million accounts have been registered.[381] Reports show that some such games have been used to commit crimes, including[382] the exchange and presentation of child pornography,[383] fraud,[384] gambling in virtual online casinos[385] and libel (e.g. leaving slanderous or libellous messages).

Some estimates project growth in estimated online gambling revenues from USD 3.1 billion in 2001 to USD 24 billion in 2010 for Internet gambling[386] (although compared with revenues from traditional gambling, these estimates are still relatively small[387]).

The regulation of gambling over and outside the Internet varies between countries[388] – a loophole that has been exploited by offenders, as well as legal businesses and casinos. The effect of different regulations is evident in Macau. After being returned by Portugal to China in 1999, Macau has become one of the world's biggest gambling destinations. With estimated annual revenues of USD 6.8 billion in 2006, it took the lead from Las Vegas (USD 6.6 billion).[389] Macau's success derives from the fact that gambling is illegal in China[390] and thousands of gamblers travel from Mainland China to Macau to play.

The Internet allows people to circumvent gambling restrictions.[391] Online casinos are widely available, most of them hosted in countries with liberal laws or no regulations on Internet gambling. Users can open accounts online, transfer money and play games of chance.[392] Online casinos can also be used in money-laundering and activities financing terrorism.[393] If offenders use online casinos within the laying phase that do not keep records or are located in countries without money-laundering legislation, it is difficult for law-enforcement agencies to determine the origin of funds.

It is difficult for countries with gambling restrictions to control the use or activities of online casinos. The Internet is undermining some countries' legal restrictions on access by citizens to online gambling.[394] There have been several legislative attempts to prevent participation in online gambling:[395] notably, the US Internet Gambling Prohibition Enforcement Act of 2006 seeks to limit illegal online gambling by prosecuting financial services providers if they carry out settlement of transactions associated with illegal gambling.[396]

### 2.6.6 Libel and false information

The Internet can be used to spread misinformation, just as easily as information.[397] Websites can present

false or defamatory information, especially in forums and chat rooms, where users can post messages without verification by moderators.[398] Minors are increasingly using web forums and social networking sites where such information can be posted as well.[399] Criminal behaviour[400] can include (for example) the publication of intimate photographs or false information about sexual behaviours.[401]

In most cases, offenders take advantage of the fact that providers offering cheap or free publication do not usually require identification of authors or may not verify ID.[402] This makes the identification of offenders complicated. Furthermore, there may be no or little regulation of content by forum moderators. These advantages have not prevented the development of valuable projects such as the online user-generated encyclopaedia, Wikipedia,[403] where strict procedures exist for the regulation of content. However, the same technology can also be used by offenders to publish false information (e.g. about competitors)[404] or disclose secret information (e.g. the publication of state secrets or sensitive business information).

It is vital to highlight the increased danger presented by false or misleading information. Defamation can seriously injure the reputation and dignity of victims to a considerable degree, as online statements are accessible to a worldwide audience. The moment information is published over the Internet, the author often loses control of this information. Even if the information is corrected or deleted shortly after publication, it may already have been duplicated ("mirroring") and made available by people that are unwilling to rescind or remove it. In this case, information may still be available on the Internet, even if it has been removed or corrected by the original source.[405] Examples include cases of "runaway e-mails", where millions of people can receive salacious, misleading or false e-mails about people or organizations, where the damage to reputations may never be restored, regardless of the truth or otherwise of the original e-mail. Therefore the freedom of speech[406] and protection of the potential victims of libel needs to be well balanced.[407]

### 2.6.7 Spam and related threats

"Spam" describes the emission of unsolicited bulk messages.[408] Although various scams exist, the most common one is e-mail spam. Offenders send out millions of e-mails to users, often containing advertisements for products and services, but frequently also malicious software. Since the first spam e-mail was sent in 1978,[409] the tide of spam e-mails has increased dramatically.[410] Today, e-mail provider organizations report that as many as 85 to 90 per cent of all e-mails are spam.[411] The main sources of spam e-mails in 2007 were: the United States (19.6 per cent of the recorded total); People's Republic of China (8.4 per cent); and the Republic of Korea (6.5 per cent).[412]

Most e-mail providers have reacted to rising levels of spam e-mails by installing anti-spam filter technology. This technology identifies spam using keyword filters or blacklists of spammers' IP addresses.[413] Although filter technology continues to develop, spammers find ways around these systems – for example, by avoiding keywords. Spammers have found many ways to describe "Viagra", one of the most popular products offered in spam, without using the brand name.[414]

Success in the detection of spam e-mails depends on changes in the way spam is distributed. Instead of sending messages from a single mail server (which is technically easier for e-mail providers to identify, due to the limited number of sources[415]), many offenders use botnets[416] to distribute unsolicited e-mails. By using botnets based on thousands of computer systems,[417] each computer might send out only a few hundred e-mails. This makes it more difficult for e-mail providers to identify spam by analysing the information about senders and more difficult for law-enforcement agencies to track offenders.

Spam e-mails are highly profitable as the cost of sending out billions of e-mails is low – and even lower where botnets are involved.[418] Some experts suggest the only real solution in the fight against spam is to raise transmission costs for senders.[419] A report published in 2007 analysed the costs and profits of spam e-mails. Based on the results of the analysis, the cost of sending out 20 million e-mails is around USD 500.[420] Since costs for offenders are low, sending spam is highly profitable, especially if offenders are able to send billions of e-mails. A Dutch spammer reported a profit of around USD 50 000 by sending out at least 9 billion spam e-mails.[421]

In 2005, the OECD published a report analysing the impact of spam on developing countries.[422] Developing countries often express the view that Internet users in their countries suffer more from the impact of spam and Internet abuse. Spam is a serious issue in developing countries, where bandwidth and Internet access are scarcer and more expensive than in industrialized countries.[423] Spam consumes valuable time and resources in countries where Internet resources are rarer and more costly.

### 2.6.8 Other forms of illegal content

The Internet is not only used for direct attacks, but also as a forum for soliciting, offers and incitement to commit crimes[424] unlawful sale of products and providing information and instructions for illegal acts (e.g. how to build explosives).

Many countries have put in place regulations on the trade of certain products. Different countries apply different national regulations and trade restrictions to various products such as military equipment.[425] A similar situation exists for medicines – medicines which are available without restriction in some countries may need prescription in others.[426] Cross-border trade may make it difficult to ensure that access to certain products is restricted within a territory.[427] Given the popularity of the Internet, this problem has grown. Webshops operating in countries with no restrictions can sell products to customers in other countries with restrictions, undermining these limitations.

Prior to the Internet, it was difficult for most people to access instructions on how to build weapons. The necessary information was available (e.g. in books dealing with chemical aspects of explosives), but time-consuming to find. Today, information on how to build explosives is available over the Internet[428] and ease of access to information increases the likelihood of attacks.

## 2.7 Copyright and trademark related offences

**Bibliography (selected):** Androutsellis-Theotokis/Spinellis, A Survey of Peer-to-Peer Content Distribution Technologies, 2004, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; Bakken, Unauthorized use of Another's Trademark on the Internet, UCLA Journal of Law and Technology Vol. 7, Issue 1; Baesler, Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf; Clarke/Sandberg/Wiley/Hong, Freenet: a distributed anonymous information storage and retrieval system, 2001; Cunard/Hill/Barlas, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; Fischer, The 21st Century Internet: A Digital Copy Machine: Copyright Analysis, Issues, and Possibilities, Virginia Journal of Law and Technology, Vol. 7, 2002; Johnson/McGuire/Willey, Why File-Sharing Networks Are Dangerous, 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf; Lohmann, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf; Penn, Copyright Law: Intellectual Property Protection in Cyberspace, Journal of Technology Law and Policy, Vol. 7, Issue 2; Rayburn, After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001; Schoder/Fischbach/Schmitt, Core Concepts in Peer-to-Peer Networking, 2005, available at: www.idea-group.com/downloads/excerpts/Subramanian01.pdf; Sifferd, The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology, Vanderbilt Journal of Entertainment Law & Practice, 2002, 4, 93.

One of the vital functions of the Internet is the dissemination of information. Companies use the Internet to distribute information about their products and services. In terms of piracy, successful companies may face problems on the Internet comparable to those that exist outside the network. Their brand image and corporate design may be used for the marketing of counterfeit products, with counterfeiters copying logos as well as products and trying to register the domain related to that particular company. Companies that distribute products directly over the Internet[429] can face legal problems with copyright violations. Their products may be downloaded, copied and distributed.

### 2.7.1 Copyright-related offences

With the switch from analogue to digital,[430] digitization[431] has enabled the entertainment industry to add additional features and services to movies on DVD, including languages, subtitles, trailers and bonus material. CDs and DVDs have proved more sustainable than records and videotapes.[432]

Digitization has opened the door to new copyright violations. The basis for current copyright violations is fast and accurate reproduction. Before digitization, copying a record or a videotape always resulted in a degree of loss of quality. Today, it is possible to duplicate digital sources without loss of quality, and also, as a result, to make copies from any copy. The most common copyright violations include the exchange of copyright-protected songs, files and software in file-sharing systems[433] or through sharehosting services and the circumvention of digital rights management (DRM) systems.[434]

File-sharing systems are peer-to-peer[435]-based network services that enable users to share files,[436] often with millions of other users.[437] After installing file-sharing software, users can select files to share and use software to search for other files made available by others for download from hundreds of sources. Before file-sharing systems were developed, people copied records and tapes and exchanged them, but file-sharing systems permit the exchange of copies by many more users.

Peer-to-peer (P2P) technology plays a vital role in the Internet. In 2007, over 50 per cent of consumer Internet traffic was generated by P2P networks.[438] The number of users is growing all the time – a report published by the OECD estimates that some 30 per cent of French Internet users have downloaded music or files in file-sharing systems,[439] with other OECD countries showing similar trends.[440] File-sharing systems can be used to exchange any kind of computer data, including music, movies and software.[441] Historically, file-sharing systems have been used mainly to exchange music, but the exchange of videos is becoming more and more important.[442]

The technology used for file-sharing services is highly sophisticated and enables the exchange of large files in short periods of time.[443] First-generation file-sharing systems depended on a central server, enabling law-enforcement agencies to act against illegal file-sharing in the Napster network.[444] Unlike first-generation systems (especially the famous Napster service), second-generation file-sharing systems are no longer based on a central server providing a list of files available between users.[445] The decentralized concept of second-generation file-sharing networks makes it more difficult to prevent them from operating. However, due to direct communications, it is possible to trace users of a network by their IP-address.[446] Law-enforcement agencies have had some success investigating copyright violations in file-sharing systems. More recent versions of file-sharing systems enable forms of anonymous communication and will make investigations more difficult.[447]

File-sharing technology is not only used by ordinary people and criminals, but also by regular businesses.[448] Not all files exchanged in file-sharing systems violate copyrights. Examples of its legitimate use include the exchange of authorized copies or artwork within the public domain.[449]

Nevertheless, the use of file-sharing systems poses challenges for the entertainment industry.[450] It is unclear to what extent falls in sales of CD/DVDs and cinema tickets are due to the exchange of titles in file-sharing systems. Research has identified millions of file-sharing users[451] and billions of downloaded files.[452] Copies of movies have appeared in file-sharing systems before they were officially released in cinemas[453] at the cost of copyright-holders. The recent development of anonymous file-sharing systems will make the work of copyright-holders more difficult, as well as that of law-enforcement agencies.[454]

The entertainment industry has responded by implementing technology designed to prevent users from making copies of CDs and DVDs such as content scrambling systems (CSS),[455] an encryption technology preventing content on DVDs from being copied.[456] This technology is a vital element of new business models seeking to assign access rights to users more precisely. Digital rights management (DRM)[457] describes the implementation of technologies allowing copyright-holders to restrict the use of digital media, where customers buy limited rights only (e.g. the right to play a song during one party). DRM offers the possibility of implementing new business models that reflect copyright-holders' and users' interests more accurately and could reverse declines in profits.

One of the biggest difficulties with these technologies is that copyright-protection technology can be circumvented.[458] Offenders have developed software tools that enable the users to make copy-protected files available over the Internet[459] free of charge or at low prices. Once DRM protection is removed from a file, copies can be made and played without limitation.

Efforts to protect content are not limited to songs and films. Some TV stations (especially pay-TV channels) encrypt programmes to ensure that only paying customers can receive the programme. Although protection technologies are advanced, offenders have succeeded in falsifying the hardware used as access control or have broken the encryption using software tools.[460]

Without software tools, regular users are less able to commit such offences. Discussions on the criminalization of copyright violations not only focus on file-sharing systems and the circumvention of technical protection, but also on the production, sale and possession of "illegal devices" or tools that are designed to enable the users to carry out copyright violations.[461]

### 2.7.2 Trademark-related offences

Trademark violations, a well-known aspect of global trade, are similar to copyright violations. Violations related to trademarks have transferred to cyberspace, with varying degrees of criminalization under different national penal codes.[462] The most serious offences include the use of trademarks in criminal activities with the aim of misleading users and domain name related offences.

The good reputation of a company is often linked directly with its trademarks. Offenders use brand names and trademarks fraudulently in a number of activities, including phishing,[463] where millions of e-mails are sent out to Internet users resembling e-mails from legitimate companies, e.g. including trademarks.[464]

A further issue related to trademark violations is domain-related offences[465] such as cybersquatting,[466] which describes the illegal process of registering a domain name identical or similar to a trademark of a product or a company.[467] In most cases, offenders seek to sell the domain for a high price to the company[468] or to use it to sell products or services misleading users through their supposed connection to the trademark. [469] Another example of a domain-related offence is "domain hijacking" or the registration of domain names that have accidentally lapsed.[470]

## 2.8 Computer-related offences

**Bibliography (selected):** *Bywell/Oppenheim*, Fraud on Internet Auctions, Aslib Proceedings, 53 (7), page 265 *et seq.*; *Clarke*, Technology, Criminology and Crime Science, European Journal on Criminal Policy and Research, Vol. 10, 2004, page 55; *Elston/Stein*, International Cooperation in On-Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, available at: www.isrcl.org/Papers/Elston%20and%20Stein.pdf; *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, 2005; *Gercke*, Internet-related Identity Theft, 2007; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000; *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, Crime Law Soc Change, Vol. 46, page 270; *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* Identity Theft – A discussion paper, 2004; *Paget*, Identity Theft – McAfee White Paper, page 10, 2007; *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1; *Sieber*, Council of Europe Organised Crime Report 2004; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, Trends & Issues in Crime and Criminal Justice, No. 121; *Snyder*, Online Auction Fraud: Are the Auction Houses Doing All They Should or Could to Stop Online Fraud, Federal Communications Law Journal, 52 (2), page 453 *et seq.*

This category covers a number of offences that need a computer system to be committed. Unlike previous categories, these broad offences are often not as stringent in the protection of legal principles. The category includes computer-related fraud, computer-related forgery, phishing, identity theft and misuse of devices.

### 2.8.1 Fraud and computer-related fraud

Computer-related fraud is one of the most popular crimes on the Internet,[471] as it enables the offender to use automation[472] and software tools to mask criminals' identities.

Automation enables offenders to make large profits from a number of small acts. [473] One strategy used by offenders is to ensure that each victim's financial loss is below a certain limit. With a "small" loss, victims are less likely to invest time and energy in reporting and investigating such crimes.[474] One example of such a scam is the Nigeria Advanced Fee Fraud.[475]

Although these offences are carried out using computer technology, most criminal law systems categorize them not as computer-related offences, but as regular fraud.[476] The main distinction between computer-related and traditional fraud is the target of the fraud. If offenders try to influence a person, the offence is generally recognized as fraud. Where offenders target computer or data-processing systems, offences are often categorized as computer-related fraud. Those criminal law systems that cover fraud, but do not yet include the manipulation of computer systems for fraudulent purposes, can often still prosecute the above-mentioned offences. The most common fraud offences include online auction fraud and advanced fee fraud.

#### Online auction fraud[477]

Online auctions are now one of the most popular e-commerce services. In 2006, goods worth more than USD 20 billion were sold on eBay, the world's largest online auction marketplace.[478] Buyers can access varied or specialist niche goods from around the world. Sellers enjoy a worldwide audience, stimulating demand and boosting prices.

Offenders committing crimes over auction platforms can exploit the absence of face-to-face contact between sellers and buyers.[479] The difficulty of distinguishing between genuine users and offenders has resulted in auction fraud being among the most popular of cybercrimes.[480] The two most common methods include[481] offering non-existent goods for sale and requesting buyers to pay prior to delivery[482] and buying goods and asking for delivery, with no intention of paying.

In response, auction providers have developed protection systems such as the feedback/comments system. After each transaction, buyer and sellers leave feedback for use by other users[483] as neutral information about the reliability of sellers/buyers. In this case, "reputation is everything" and without an adequate number of positive comments, it is harder for offenders to persuade targets to either pay for non-existent goods or, conversely, to send out goods without receiving payment first. However, criminals have responded and circumvented this protection through using accounts from third parties.[484] In this scam called "account takeover",[485] offenders try to get hold of user names and passwords of legitimate users to buy or sell goods fraudulently, making identification of offenders more difficult.

#### Advance fee fraud[486]

In advance fee fraud, offenders send out e-mails asking for recipients' help in transferring large amounts of money to third parties and promise them a percentage, if they agree to process the transfer using their personal accounts.[487] The offenders then ask them to transfer a small amount to validate their bank account data (based on a similar perception as lotteries – respondents may be willing to incur a small but certain loss, in exchange for a large but unlikely gain) or just send bank account data directly. Once they transfer the money, they will never hear from the offenders again. If they send their bank account information, offenders may use this information for fraudulent activities. Evidence suggests that thousands of targets reply to e-mails.[488] Current researches show that, despite various information campaigns and initiatives, advance fee frauds are still growing – in terms of both the number of victims and total losses.[489]

### 2.8.2 Computer-related forgery

Computer-related forgery describes the manipulation of digital documents.[490] The offence can for example be committed by creating a document that appears to originate from a reliable institution,

manipulating electronic images (for example, pictures used as evidence in court) or altering text documents.

The falsification of e-mails is an essential element of phishing, which is a serious challenge for law-enforcement agencies worldwide.[491] "Phishing" seeks to make targets disclose personal/secret information.[492] Often, offenders send out e-mails that look like communications from legitimate financial institutions used by the target.[493] The e-mails are designed in a way that it is difficult for targets to identify them as fake e-mails.[494] The e-mail asks recipient to disclose and/or verify certain sensitive information. Many victims follow the advice and disclose information enabling offenders to make online transfers etc.[495]

In the past, prosecutions involving computer-related forgery were rare, because most legal documents were tangible documents. Digital documents play an ever more important role and are used more often. The substitution of classic documents by digital documents is supported by legal means for their use, e.g. by legislation recognizing digital signatures.

Criminals have always tried to manipulate documents. With digital forgeries, digital documents can now be copied without loss of quality and are easily manipulated. For forensic experts, it is difficult to prove digital manipulations, unless technical protection[496] is used to protect a document from being falsified.[497]

### 2.8.3 Identity theft

The term identity theft – which is neither consistently defined nor consistently used – describes the criminal act of fraudulently obtaining and using another person's identity.[498] These acts can be carried out without the help of technical means[499] as well as online by using Internet technology.[500]

Wide media coverage,[501] the results of various surveys analysing the extent of and loss caused by identity theft,[502] as well as numerous legal and technical analyses[503] published in recent years could easily lead to the conclusion, that identity-related offences are a 21st-century phenomenon.[504] But this is not the case, as offences related to impersonation and the falsification and misuse of identity documents have existed for more than a century.[505] Already back in the 1980s, the press intensively reported on the misuse of identity-related information.[506] The emerging use of digital identities and information technology only changed the methods and targets of the offenders.[507] Increasing use of digital information opened up new possibilities for offenders to gain access to identity-related information.[508] Thus, the transformation process from industrialized nations to information societies[509] has had a big influence on the development of identity-theft offences. Nonetheless, despite the large number of Internet-related identity-theft cases, digitization did not fundamentally change the offence itself, but merely created new targets and facilitated the development of new methods.[510] The impact of the increasing use of Internet technology seems to be overestimated. Based on the results of a method analysis of identity-related offences, identity theft to a large degree remains an offline crime.[511] Less than 20 per cent of the offences in the US in 2007[512] were online scams and data breaches.[513] The persisting importance of offline crimes is surprising, insofar as the digitization and moreover the globalization of network-based services has led to increasing use of digital identity-related information.[514] Identity-related information is of growing importance, both in the economy and in social interaction. In the past, a "good name" and good personal relations dominated business as well as daily transactions.[515] With the transfer to electronic commerce, face-to-face identification is hardly possible, and as a consequence identity-related information has become much more important for people participating in social and economic interaction.[516] This process can be described as instrumentalization,[517] whereby an identity is translated into quantifiable identity-related information. This process, along with the distinction between the more philosophical aspect of the term "identity" (defined[518] as the collection of personal characteristics) and the quantifiable identity-related information that enables the recognition of a person, is of great importance. The transformation process is not just relevant to Internet-related features of identity theft, as the impact of the development goes far beyond computer networks. Nowadays, the requirements of non face-to-face transactions, such as trust and security,[519] dominate the economy in general and not just e-commerce businesses. An example is the use of payment cards with a PIN (personal identification number) for purchasing goods in a supermarket.

In general, the offence described as identity theft contains three different phases.[520] In the first phase the offender obtains identity-related information. This part of the offence can for example be carried out by using malicious software or phishing attacks. The second phase is characterized by interaction with identity-related information prior to the use of the information within criminal offences.[521] An example is the sale of identity-related information.[522] Credit-card records are for example sold for up to USD 60.[523] The third phase is the use of the identity-related information in relation with a criminal offence. In most cases, the access to identity-related data enables the perpetrator to commit further crimes.[524] The perpetrators are therefore not focusing on the set of data itself but the ability to use the data in criminal activities. Examples for such offence can be the falsification of identification documents or credit-card fraud. [525]

The methods used to obtain data in phase one cover a wide range of acts. The offender can use physical methods, for example stealing computer storage devices with identity-related data, searching trash ("dumpster diving"[526]) or mail theft.[527] In addition, they can use search engines to find identity-related data. "Googlehacking" or "Googledorks" are terms that describe the use of complex search-engine queries to filter through large amounts of search results for information related to computer security issues as well as personal information that can be used in identity-theft scams. One aim of the perpetrator can for example be to search for insecure password protection systems in order to obtain data from the system.[528] Reports highlight the risks involved with the legal use of search engines for illegal purposes.[529] Similar problems are reported with regard to file-sharing systems. The United States Congress discussed recently the possibilities of exploiting file-sharing systems to obtain personal information that can be abused for identity theft.[530] Apart from that, the offenders can make use of insiders, who have access to stored identity-related information, to obtain that information. The 2007 CSI Computer Crime and Security Survey[531] shows that more than 35 per cent of the respondents attribute a percentage of their organization's losses greater than 20 per cent to insiders. Finally the perpetrators can use social engineering techniques to persuade the victim to disclose personal information. In recent years perpetrators have developed effective scams to obtain secret information (e.g. bank-account information and credit-card data) by manipulating users through social engineering techniques.[532]

The type of data the perpetrators target varies.[533] The most relevant data are social security and passport numbers, date of birth, address and phone numbers, and passwords.

### Social security number (SSN) or passport number

The SSN used, for example, in the United States is a classic example of a single identity-related data item that perpetrators target. Although the SSN was created to keep an accurate record of earnings, it is currently widely used for identification purposes.[534] The perpetrators can use the SSN and passport information to open financial accounts, to take over existing financial accounts, to obtain credit or run up debt.[535]

### Date of birth, address and phone numbers

Such data can in general only be used to commit identity theft if they are combined with other pieces of information (e.g. the SSN).[536] Having access to additional information like date of birth and address can help the perpetrator to circumvent verification processes. One of the greatest dangers related to that information is the fact that it is currently available on a large scale on the Internet – either published voluntarily in one of the various identity-related fora[537] or based on legal requirements as imprint on websites.[538]

### Password for non-financial accounts

Having access to passwords for accounts allows perpetrators to change the settings of the account and use it for their own purposes.[539] They can for example take over an e-mail account and use it to send out mails with illegal content or take over the account of a user of an auction platform and use the account to sell stolen goods.[540]

#### Password for financial accounts

Like the SSN, information regarding financial accounts is a popular target for identity theft. This includes cheque and saving accounts, credit cards, debit cards, and financial planning information. Such information is an important source for an identity thief to commit financial cybercrimes.

Identity theft is a serious and growing problem.[541] In the first half of 2004, 3 per cent of United States households fell victim to identity theft.[542] In the United Kingdom, the cost of identity theft to the British economy has been calculated at GBP 1.3 billion every year.[543] Estimates of losses caused by identity theft in Australia vary from less than USD 1 billion to more than USD 3 billion per year.[544] The 2006 Identity Fraud Survey estimates the losses in the United States at USD 56.6 billion in 2005.[545] Losses may be not only financial, but may also include damage to reputations.[546] In reality, many victims do not report such crimes, while financial institutions often do not wish to publicize customers' bad experiences. The actual incidence of identity theft is likely to far exceed the number of reported losses.[547]

Identity theft is based on the fact that there are few instruments to verify the identity of users over the Internet. It is easier to identify individuals in the real world, but most forms of online identification are more complicated. Sophisticated identification tools (e.g. using biometric information) are costly and not widely used. There are few limits on online activities, making identity theft easy and profitable.[548]

### *2.8.4 Misuse of devices*

Cybercrime can be committed using only fairly basic equipment.[549] Committing offences such as libel or online fraud needs nothing more than a computer and Internet access and can be carried out from a public Internet café. More sophisticated offences can be committed using specialist software tools.

The tools needed to commit complex offences are widely available over the Internet,[550] often without charge. More sophisticated tools cost several thousand dollars.[551] Using these software tools, offenders can attack other computer systems at the press of a button. Standard attacks are now less efficient, as protection software companies analyse the tools currently available and prepare for standard hacking attacks. High-profile attacks are often individually designed for specific targets.[552] Software tools[553] are available that enable the offender to carry out DoS attacks[554], design computer viruses, decrypt encrypted communication or illegally access computer systems.

A second generation of software tools has now automated many cyberscams and enables offenders to carry out multiple attacks within a short time. Software tools also simplify attacks, allowing less experienced computer users to commit cybercrime. Spam-toolkits are available that enable virtually anybody to send out spam e-mails.[555] Software tools are now available that can be used to upload and download files from file-sharing systems. With greater availability of specially-designed software tools, the number of potential offenders has risen dramatically. Different national and international legislative initiatives are being undertaken to address such software tools – for example, by criminalizing their production, sale or possession.[556]

## 2.9 Combination offences

**Bibliography (selected):** *Arquilla/Ronfeldt*, in The Future of Terror, Crime and Militancy, 2001; *Brandon,* Virtual Caliphate: Islamic extremists and the internet, 2008, available at: www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf; *Conway*, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006; *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001); *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45, page 1033 *et seq.*; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*; *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.2, 2010, available at: www.eset.com/resources/white-

papers/Stuxnet_Under_the_Microscope.pdf; *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996; *Rollins/Wilson*, Terrorist Capabilities for Cyberattack, 2007; *Schperberg*, Cybercrime: Incident Response and Digital Forensics, 2005; *Shackelford*, From Nuclear War to Net War: Analogizing Cyberattacks in International Law, Berkeley Journal of International Law, Vol. 27; *Shimeall/Williams/Dunlevy*, Countering cyberwar, NATO review, Winter 2001/2002; *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001; *Stenersen*, The Internet: A Virtual Training Camp?, in Terrorism and Political Violence, 2008; *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010; *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Wilson* in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003.

There are several terms used to describe complex scams that combine a number of different offences. Examples include terrorist use of the Internet, cyberlaundering and phishing.

### 2.9.1 Terrorist use of the Internet

In the 1990s, discussion about the use of the network by terrorist organizations focused on network-based attacks against critical infrastructure such as transportation and energy supply ("cyberterrorism") and the use of information technology in armed conflicts ("cyberwarfare").[557] The success of virus and botnet attacks has clearly demonstrated weaknesses in network security. Successful Internet-based attacks by terrorists are possible,[558] but it is difficult to assess the significance of threats[559]. Back then, the degree of interconnection was small compared to nowadays, and it is very likely that this – apart from the interest of the states to keep successful attacks confidential – is one of the main reasons why very few such incidents were reported. At least in the past, therefore, falling trees posed a greater risk for energy supply than successful hacking attacks.[560]

This situation changed after the 9/11 attacks, which prompted the start of an intensive discussion about the use of ICTs by terrorists.[561] This discussion was facilitated by reports[562] that the offenders used the Internet in their preparation of the attack.[563] Although the attacks were not cyberattacks, insofar as the group that carried out the 9/11 attack did not carry out an Internet-based attack, the Internet played a role in the preparation of the offence.[564] In this context, different ways in which terrorist organizations use the Internet were discovered.[565] Today, it is known that terrorists use ICTs and the Internet for:

- propaganda
- information gathering
- preparation of real-world attacks
- publication of training material
- communication
- terrorist financing
- attacks against critical infrastructures.

This shift in the focus of the discussion had a positive effect on research related to cyberterrorism as it highlighted areas of terrorist activities that were rather unknown before. But despite the importance of a comprehensive approach, the threat of Internet-related attacks against critical infrastructure should not be removed from the central focus of the discussion. The vulnerability of and the growing reliance[566] on information technology makes it necessary to include Internet-related attacks against critical infrastructure in strategies to prevent and fight cyberterrorism.

Despite the more intensive research, however, the fight against cyberterrorism remains difficult. A comparison of the different national approaches shows many similarities in the strategies.[567] One of the reasons for this development is the fact that the international communities recognized that the threats of international terrorism require global solutions.[568] But it is currently uncertain if this approach is

successful or if the different legal systems and different cultural backgrounds require different solutions. An evaluation of this issue carries unique challenges because apart from reports about major incidents there are very few data available that could be used for scientific analysis. The same difficulties arise with regard to the determination of the level of threat related to the use of information technology by terrorist organizations. This information is very often classified and therefore only available to the intelligence sector.[569] Not even a consensus on the term "terrorism" has yet been achieved.[570] A CRS report for the United States Congress for example states that the fact that one terrorist booked a flight ticket to the United States via the Internet is proof that terrorists used the Internet in preparation of their attacks.[571] This seems to be a vague argumentation, as the booking of a flight ticket does not become a terrorist-related activity just because it is carried out by a terrorist.

### Propaganda

In 1998, only 12 out of the 30 foreign terrorist organizations that are listed by the United States State Department maintained websites to inform the public about their activities.[572] In 2004, the United States Institute of Peace reported that nearly all terrorist organizations maintain websites – among them Hamas, Hezbollah, PKK and Al Qaida.[573] Terrorists have also started to use video communities (such as YouTube) to distribute video messages and propaganda.[574] The use of websites and other forums are signs of a more professional public relations focus of subversive groups.[575] Websites and other media are used to disseminate propaganda,[576] to describe and publish justifications[577] of their activities and to recruit[578] new and contact existing members and donors.[579] Websites have been used recently to distribute videos of executions.[580]

### Information gathering

Considerable information about possible targets is available over the Internet.[581] For example, architects involved in the construction of public buildings often publish plans of buildings on their websites. Today, high-resolution satellite pictures are available free of change on various Internet services that years ago were only available to very few military institutions in the world.[582]. Instructions on how to build bombs and even virtual training camps that provide instructions on the use of weapons in an e-learning approach have been discovered.[583] In addition, sensitive or confidential information that is not adequately protected from search robots can be accessed via search engines.[584] In 2003, the United States Department of Defense was informed that a training manual linked to Al Qaeda contained information that public sources could be used to find details about potential targets.[585] In 2006, the New York Times reported that basic information related to the construction of nuclear weapons were published on a government website that provided evidence about the Iraq approaches to develop nuclear weapons.[586] A similar incident was reported in Australia, where detailed information about potential targets for terrorist attacks was available on government websites.[587] In 2005, the press in Germany reported that investigators found that manuals on how to build explosives were downloaded from the Internet onto the computer of two suspects that tried to attack public transportation with self-built bombs.[588]

### Preparation of real-world attacks

There are different ways that terrorists can make use of information technology in preparing their attack. Sending out e-mails or using forums to leave messages are examples that will be discussed in the context of communication. Here more direct ways of online preparation are discussed. Reports have been published which point out that terrorists are using online games in the preparation of attacks.[589] There are various different online games available that simulate the real world. A player of such games can make use of characters (avatar) to act in this virtual world. Theoretically, these online games could be used to simulate attacks, but it is not yet certain to what extent online games are already involved in that activity.[590]

### Publication of training material

The Internet can be used to spread training material such as instructions on how to use weapons and how to select targets. Such material is available on a large scale from online sources.[591] In 2008, Western secret

services discovered an Internet server that provided a basis for the exchange of training material as well as communication.[592] Different websites were reported to be operated by terrorist organizations to coordinate activities.[593]

### Communication

The use of information technology by terrorist organizations is not limited to running websites and research in databases. In the context of the investigations after the 9/11 attacks, it was reported that the terrorists used e-mail communication for coordination of their attacks.[594] The press reported on the exchange via e-mail of detailed instructions about the targets and the number of attackers.[595] By using encryption technology and means of anonymous communication, the communicating parties can make it even more difficult to identify and monitor terrorist communication.

### Terrorist financing

Most terrorist organizations depend on financial resources they receive from third parties. Tracing back these financial transactions has become one of the major approaches in the fight against terrorism after the 9/11 attacks. One of the main difficulties in this respect is the fact that the financial resources required to carry out attacks are not necessarily large.[596] There are several ways in which Internet services can be used for terrorist financing. Terrorist organizations can make use of electronic payment systems to enable online donations.[597] They can use websites to publish information how to donate, e.g. which bank account should be used for transactions. An example of such an approach is the organization "Hizb al-Tahrir", which published bank-account information for potential donors.[598] Another approach is the implementation of online credit-card donations. The Irish Republican Army (IRA) was one of the first terrorist organizations that collected donations via credit card.[599] Both approaches carry the risk that the published information will be discovered and used to trace back financial transactions. It is therefore likely that anonymous electronic payment systems will become more popular. To avoid discovery, terrorist organizations are trying to hide their activities by involving non-suspicious players such as charity organizations. Another (Internet-related) approach is the operation of fake webshops. It is relatively simple to set up an online shop on the Internet. One of the biggest advantages of the network is the fact that businesses can be operated worldwide. Proving that financial transactions that took place on those sites are not regular purchases but donations is not at all easy. It would be necessary to investigate every transaction – which can be difficult if the online shop is operated in a different jurisdiction or anonymous payment systems are used.[600]

### Attacks against critical infrastructures

In addition to regular computer crimes such as fraud and identity theft, attacks against critical information infrastructures could become a goal for terrorists. The growing reliance on information technology makes critical infrastructure more vulnerable to attacks.[601] This is especially the case with regard to attacks against interconnected systems that are linked by computer and communication networks.[602] In those cases, the disruption caused by a network-based attack goes beyond the failure of a single system. Even short interruptions to services could cause huge financial damage to e-commerce businesses – not only for civil services but also for military infrastructure and services.[603] Investigating or even preventing such attacks presents unique challenges.[604] Unlike physical attacks, the offenders do not need to be present at the place where the effect of the attack occurs.[605] And while carrying out the attack the offenders can use means of anonymous communication and encryption technology to conceal their identity.[606] As highlighted above, investigating such attacks requires special procedural instruments, investigation technology and trained personnel.[607]

Critical infrastructure is widely recognized as a potential target for terrorist attacks as it is by definition vital for a state's sustainability and stability.[608] An infrastructure is considered to be critical if its incapacity or destruction would have a debilitating impact on the defence or economic security of a state.[609] These are in particular: electrical power systems, telecommunication systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems and emergency services. The degree of civil disturbance caused by the disruption of services by Hurricane Katrina in the United States

highlights the dependence of society on the availability of those services.[610] The malicious software "Stuxnet" underlines the emerging threat posed by Internet-based attacks focusing on critical infrastructure.[611] In 2010, a security firm in Belarus discovered a new malicious software.[612] Research into the manipulations caused by the software, the designer and the motivation is still ongoing and by far not all the facts have been discovered, especially in regard to attribution and motivation of the designer.[613] However, especially with regard to the functioning of the software, there seems to be a rather solid fact basis by now:

The complex software, with more than 4 000 functions,[614] was reported to target industrial control systems (ICS)[615] – in particular those produced by the technology company Siemens.[616] It was distributed through removable drives and used four zero-day exploits for the infection of computer systems.[617] Infected computer systems have mainly been reported from Iran, Indonesia and Pakistan, but also from the US and European countries.[618] Although the malicious software is frequently characterized as highly sophisticated, there are reports that question the degree of sophistication.[619]

As indicated above, the determination of attribution and motive is more difficult and still highly uncertain. News reports and studies speculate that the software could have targeted the uranium enrichment facilities in Iran and caused a delay in the country's nuclear programme.[620]

Two main conclusions can be drawn from the discovery of the malicious software. First of all, the incident underlines that critical infrastructure is largely dependent on computer technology and attacks are possible. Secondly, the fact that the software was distributed among other methods, through removable drives highlights that simply disconnecting computer systems from the Internet does not prevent attacks.

The dependence of critical infrastructure on ICT goes beyond the energy and nuclear industry. This can be demonstrated by highlighting some of incidents related to air transportation, which is in most countries also considered part of the critical infrastructure. One potential target of an attack is the check-in system. The check-in systems of most airports in the world are already based on interconnected computer systems.[621] In 2004, the Sasser computer worm[622] infected millions of computers around the world, among them computer systems of major airlines, which forced the cancellation of flights.[623]

Another potential target is online ticketing systems. Today, a significant number of tickets are purchased online. Airlines use information technology for various operations. All major airlines allow their customers to buy tickets online. Like other e-commerce activities, those online services can be targeted by offenders. One common technique used to attack web-based services is denial-of-service (DoS) attacks.[624] In 2000, within a short time, several DoS attacks were launched against well-known companies such as CNN, e-Bay and Amazon.[625] As a result, some of the services were not available for several hours or even days.[626] Airlines have been affected by DoS attacks as well. In 2001 the Lufthansa website was the target of an attack.[627]

Finally, a further potential target for Internet-related attacks against critical air transportation infrastructure is the airport control system. The vulnerability of computer-controlled flight control systems was demonstrated by a hacking attack against Worcester Airport in the US in 1997.[628] During the hacking attack, the offender disabled phone services to the airport tower and shut down the control system managing the runway lights.[629]

### 2.9.2 Cyberwarfare

After the attacks against computer systems in Estonia in 2007 and Georgia in 2008 and more recently after the discovery of the "Stuxnet"[630] computer virus, the term cyberwarfare has frequently been employed to describe the situation although – as described more in detail below – the use of terminology is problematic.

#### Terminology and definitions

There is neither a consistent terminology nor a widely accepted definition of cyberwarfare. Other terms used are information warfare, electronic warfare, cyberwar, netwar, information operations.[631] Those terms are in general employed to describe the utilization of ICTs in conducting warfare using the Internet.

More restrictive definitions define such activities as an approach to armed conflict focusing on the management and use of information in all its forms and at all levels to achieve a decisive military advantage especially in the joint and combined environment.[632] Other, broader definitions cover any electronic conflict in which information is a strategic asset worthy of conquest or destruction.[633]

### Development of the debate

The topic has been a controversial matter of discussion for decades.[634] Attention originally focused on the substitution of classic warfare by computer-mediated or computer-based attacks.[635] In this regard, the ability to take down any enemy without getting involved in a fight was one of the key components at the heart of the debate from the outset.[636] In addition, network-based attacks are generally cheaper than traditional military operations[637] and can be carried out even by small states. Despite some concrete cases that are often quoted, major aspects of the debate remain highly hypothetical.[638] The two instances that are most frequently cited are computer attacks against Estonia and Georgia. However, the classification of an attack as an act of war requires that certain criteria be fulfilled.

In 2007, Estonia experienced heated debate over the removal of a Second World War memorial, including street riots in the capital.[639] Apart from traditional forms of protest, Estonia at that time discovered several waves of computer-related attacks against government and private business websites and online services[640], including defacement of websites[641], attacks against domain name servers and distributed denial of service attacks (DDoS), where botnets were used.[642] With regard to the latter, experts explained afterwards that successful attacks against the official website of governmental organizations in Estonia[643] could only take place due to inadequate protection measures.[644] The impact of the attacks as well as their origin were subsequently the subject of controversial discussion. While news reports[645] and articles[646] indicated that the attacks came close to shutting down the country's digital infrastructure, more reliable research shows that the impact of the attacks was limited in terms of both the computer systems affected and the duration of unavailability of services.[647] Similar debate took place with regard to the determination of the origin of the attack. While during the attack the territory of the Russian Federation was reported to be the origin of the attack[648], analysis of the attacks showed that they in fact involved more than 170 countries.[649] Even if politically motivated, an attack does not necessarily constitute an act of war. As a consequence, the Estonia case needs to be excluded from the list. Despite being computer-related attacks against government and private business websites and online services[650], including defacement of websites[651] and distributed denial of service attacks (DDoS)[652], such attacks cannot be characterized as cyberwarfare as they neither constituted an act of force nor took place during a conflict between two sovereign states.

Of the two above-mentioned attacks, the 2008 attack on computer systems in Georgia is the closest to being war-related. In the context of a traditional armed conflict[653] between the Russian Federation and Georgia, several computer-related attacks targeting Georgian government websites and businesses[654] (including the defacement of websites and distributed denial of service attacks) were discovered.[655] Just as in the Estonian incident, the origin of the attack against Georgia was much debated afterwards. Although some news reports[656] seemed to pinpoint the geographic origin of the attack, technology-focused research points to the use of botnets, which makes the origin much more difficult to determine.[657] The inability to determine the origin of the attacks together with the fact that the acts discovered differ significantly from traditional warfare makes it difficult to characterize them as cyberwarfare.

Inasmuch as the debate about this phenomenon is quite important, it should be pointed out that such attacks are not an unprecedented phenomenon. Propaganda is spread through the Internet and attacks against computer systems of military alliances are a rather common concept. Already during the war in Yugoslavia, attacks against NATO computer systems originating from Serbia were discovered.[658] In response, NATO Member States were reported to have been involved in similar attacks against computer systems in Serbia.[659] Further computer-related propaganda and other forms of psychological operations (PSYOPS) designed to undermine the other side's resolve were intensively utilized.[660]

#### Importance of differentiation

Potentially war-related acts show many similarities to other forms of abuse of ICT, such as cybercrime and terrorist use of the Internet. As a consequence, the terms "cybercrime", "terrorist use of the Internet" and "cyberwarfare" are frequently used interchangeably. But a differentiation is of great importance since the applicable legal frameworks differ significantly. While cybercrime is in general addressed by acts criminalizing such conduct, the rules and procedures related to warfare are largely regulated by international law, and particularly the Charter of the United Nations.

### *2.9.3 Cyberlaundering*

The Internet is transforming money-laundering. For larger amounts, traditional money-laundering techniques still offer a number of advantages, but the Internet offers several advantages. Online financial services offer the option of enacting multiple, worldwide financial transactions very quickly. The Internet has helped overcome the dependence on physical monetary transactions. Wire transfers replaced the transport of hard cash as the original first step in suppressing physical dependence on money, but stricter regulations to detect suspicious wire transfers have forced offenders to develop new techniques. The detection of suspicious transactions in the fight against money-laundering is based on obligations of the financial institutions involved in the transfer.[661]

Money-laundering is generally divided into three phases: placement, layering and integration.

With regard to the placement of large amounts of cash, the use of the Internet might perhaps not offer that many tangible advantages.[662] However, the Internet is especially useful for offenders in the layering (or masking) phase. In this context, the investigation of money-laundering is especially difficult when money-launderers use online casinos for layering.[663]

The regulation of money transfers is currently limited and the Internet offers offenders the possibility of cheap and tax-free money transfers across borders. Current difficulties in the investigation of Internet-based money-laundering techniques often derive from the use of virtual currencies and the use of online casinos.

#### The use of virtual currencies

One of the key drivers in the development of virtual currencies were micro-payments (e.g. for the download of online articles costing USD 0.10 or less), where the use of credit cards is problematic. With the growing demand for micro-payments, virtual currencies, including "virtual gold currencies", were developed. Virtual gold currencies are account-based payment systems where the value is backed by gold deposits. Users can open e-gold accounts online, often without registration. Some providers even enable direct peer-to-peer (person-to-person) transfer or cash withdrawals.[664] Offenders can open e-gold accounts in different countries and combine them, complicating the use of financial instruments for money-laundering and terrorist financing. Account-holders may also use inaccurate information during registration to mask their identity.[665]

In addition to simple virtual currencies there are also currencies that combine the virtual aspect with anonymity. One example is *Bitcoin*, a virtual currency using peer-to-peer technology.[666] Although it is a decentralized systems that does not require central intermediaries to ensure the validity of transactions authorities successful attacks in 2011 underline the vulnerability/risks related to such decentralized virtual currencies.[667] If such anonymous currencies are used by criminals it restricts the ability of law enforcement to identify suspects by following money transfers[668] – for example in cases related to commercial child pornography.[669]

#### The use of online casinos

Unlike a real casino, large financial investments are not needed to establish online casinos.[670] In addition, the regulations on online and offline casinos often differ between countries.[671] Tracing money transfers and proving that funds are not prize winnings, but have instead been laundered, is only possible if casinos keep records and provide them to law-enforcement agencies.

Current legal regulation of Internet-based financial services is not as stringent as traditional financial regulation. Apart from gaps in legislation, difficulties in regulation arise from challenges in customer verification, since accurate verification may be compromised, if the financial service provider and customer never meet.[672] In addition, the lack of personal contact makes it difficult to apply traditional know-your-customer procedures. Furthermore, the Internet transfers often involve the cross-border participation of providers in various countries. Finally monitoring transactions is particularly difficult if providers allow customers to transfer value in a peer-to-peer model.

### 2.9.4 Phishing

Offenders have developed techniques to obtain personal information from users, ranging from spyware[673] to "phishing" attacks.[674] "Phishing" describes acts that are carried out to make victims disclose personal/secret information.[675] There are different types of phishing attacks,[676] but e-mail-based phishing attacks contain three major phases. In the first phase, offenders identify legitimate companies offering online services and communicating electronically with customers whom they can target, e.g. financial institutions. Offenders design websites resembling the legitimate websites ("spoofing sites") requiring victims to perform normal log in procedures, enabling offenders to obtain personal information (e.g. account numbers and online banking passwords).

In order to direct users to spoofing sites, offenders send out e-mails resembling e-mails from the legitimate company,[677] often resulting in trademark violations.[678] The false e-mails ask recipients to log in for updates or security checks, sometimes with threats (e.g. to close the account) if users do not cooperate. The false e-mail generally contains a link that victim should follow to the spoof site, to avoid users manually entering the correct web address of the legitimate bank. Offenders have developed advanced techniques to prevent users from realizing that they are not on the genuine website.[679]

As soon as personal information is disclosed, offenders log in to victims' accounts and commit offences such as the transfer of money, application for passports or new accounts, etc. The rising number of successful attacks proves phishing's potential.[680] More than 55 000 unique phishing sites were reported to APWG[681] in April 2007.[682] Phishing techniques are not limited to accessing passwords for online banking only. Offenders may also seek access codes to computers, auction platforms and social security numbers, which are particularly important in the United States and can give rise to "identity theft" offences.[683]

82 Other terminology used includes information technology crime and high-tech crime. See, in this context: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, International Journal of Law and Information Technology, 2002, Vol. 10, No. 2, page 144.

83 Regarding approaches to define and categorize cybercrime, see for example: Cybercrime, Definition and General Information, Australian Institute for Criminology, available at: www.aic.gov.au/topics/cybercrime/definitions.html; Explanatory Report to the Council of Europe Convention on Cybercrime, No. 8; *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview/; *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf; Cybercrime, Report of the Parliamentary Joint Committee on the Australian Crime Commission, 2004, page 5, available at: www.aph.gov.au/Senate/Committee/acc_ctte/completed_inquiries/2002-04/cybercrime/report/report.pdf; *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3; *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37; *Forst,* Cybercrime: Appellate Court Interpretations, 1999, page 1.

[84] *Nhan/Bachmann* in Maguire/Okada (eds), Critical Issues in Crime and Justice, 2011, page 166.

[85] Regarding this relationship, see also: *Sieber* in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004, page 86.

[86] Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: www.uncjin.org/Documents/congr10/10e.pdf.

[87] With regard to the definition, see also: *Kumar*, Cyber Law, A view to social security, 2009, page 29.

[88] See, for example: *Carter*, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf; *Charney*, Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41, Issue 7, page 489 *et seq.*; *Goodman*, Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469.

[89] The Stanford Draft International Convention was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Stanford Draft is published in: The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[90] *Arti*cle 1, Definitions and Use of Terms,

For the purposes of this Convention:

1. "cyber crime" means conduct, with respect to cyber systems, that is classified as an offense punishable by this Convention;

[...]

[91] See: *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3.

[92] *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37

[93] Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention, see below: § 6.2.; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No. 4, 2001, page 889 *et seq.*

[94] Universal serial bus (USB)

[95] Article 4 – Data Interference:

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
(2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

[96] For difficulties related to the application of a cybercrime definition to real-world crimes, see: *Brenner*, Cybercrime Metrics: Old Wine, New Bottles?, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue4/v9i4_a13-Brenner.pdf.

[97] In civil law countries, the use of such a legal term could lead to conflicts with the principle of certainty.

[98] Some of the most well-known cybercrime offences are illegal access, illegal interception of computer data, data interference, computer-related fraud, computer-related forgery, dissemination of child pornography. For an overview see: *Sieber*, Council of Europe Organised Crime Report 2004; ABA International Guide to Combating Cybercrime, 2002; *Williams*, Cybercrime, 2005, in Miller, Encyclopaedia of Criminology.

[99] *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2003, available at: www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf.

[100] Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. Regarding the Convention on Cybercrime see: *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

[101] The same typology is used by the ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008. The report is available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[102] Art. 2 (Illegal access), Art. 3 (Illegal interception), Art. 4 (Data interference), Art. 5 (System interference), Art. 6 (Misuse of devices). For more information about the offences, see below: § 6.2.

[103] Art. 7 (Computer-related forgery), Art. 8 (Computer-related fraud). For more information about the offences, see below: § 6.2.

[104] Art. 9 (Offences related to child pornography). For more information about the offences, see below: § 6.2.

[105] Art. 10 (Offences related to infringements of copyright and related rights). For more information about the offences, see below: § 6.2.

[106] See below: § 2.5.

[107] See below: § 2.6.

[108] See below: § 2.7.

[109] See below: § 2.8.

[110] See below: § 2.9.1

[111] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Criminal Responsibility for Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4. Regarding the legal response to phishing, see: *Lynch*, Identity Theft in Cyberspace: Crime Control, Berkeley Tech. Law Journal, 2005, 259; *Hoffhagle*, Identity Theft: Making the Known Unknowns Known, Harvard Journal of Law & Technology, Vol. 21, No. 1, 2007, page 97 *et seq.*

[112] Regarding the related challenges, see: *Slivka/Darrow*; Methods and Problems in Computer Security, Journal of Computers and Law, 1975, page 217 *et seq.*

[113] *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*

[114] See: *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 5, available at: www.mekabay.com/overviews/history.pdf.

[115] *Ruggles/Miller/Kuh/Lebergott/Orcutt/Pechman*, Report of the Committee on the Preservation and Use of Economic Data, 1965, available at: www.archive.org/details/ReportOfTheCommitteeOnThePreservationAndUseOfEconomicData1965.

[116] *Miller*, The Assault on Privacy-Computers, 1971.

[117] *Westin/Baker*, Data Banks in a Free Society, 1972.

[118] For an overview about the debate in the US and Europe, see: *Sieber*, Computer Crime and Criminal Law, 1977.

[119] *Quinn*, Computer Crime: A Growing Corporate Dilemma, The Maryland Law Forum, Vol. 8, 1978, page 48.

[120] *Stevens*, Identifying and Charging Computer Crimes in the Military, Military Law Review, Vol. 110, 1985, page 59.

[121] *Gemignani*, Computer Crime: The Law in '80, Indiana Law Review, Vol. 13, 1980, page 681.

[122] *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*

[123] For an overview about cases see: *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 5, available at: www.mekabay.com/overviews/history.pdf.

[124] *Freed*, Materials and cases on computer and law, 1971, page 65.

[125] *Bequai*, The Electronic Criminals – How and why computer crime pays, Barrister, Vol. 4, 1977, page 8 *et seq.*

[126] Criminological Aspects of Economic Crimes, 12th Conference of Directors of Criminological Research Institutes, Council of Europe, Strasbourg, 1976, page 225 *et seq.*; Staff Study of Computer Security in Federal Programs; Committee on Governmental Operations, the 95th Congress 1 Session, United States Senate, February 1977.

[127] *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*; *Bequai*, Computer Crime: A Growing and Serious Problem, Police Law Quarterly, Vol. 6, 1977, page 22.

[128] *Nycum*, Legal Problems of Computer Abuse, Washington University Law Quarterly, 1977, page 527.

[129] Regarding the number of the cases in early cybercrime investigations, see: *Schjolberg*, Computers and Penal Legislation, A study of the legal politics and a new technology, 1983, page 6, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf.

[130] *Quinn*, Computer Crime: A Growing Corporate Dilemma, The Maryland Law Forum, Vol. 8, 1978, page 58, Notes – A Suggested Legislative Approach to the Problem of Computer Crime, Washington and Lee Law Review, 1981, page 1173.

[131] *Nycum*, The criminal law aspects of computer abuse: Applicability of federal criminal code to computer abuse, 1976.

[132] Federal Computer Systems Protection Act of 1977. For more information, see: *Schjolberg*, Computer-related Offences, Council of Europe, 2004, page 2, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf; *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*; *Nycum*, Legal Problems of Computer Abuse, Washington University Law Quarterly, 1977, page 531.

[133] Third Interpol Symposium on International Fraud, France 1979.

[134] Computer Abuse: The Emerging Crime and the Need for Legislation, Fordham Urban Law Journal, 1983, page 73.

[135] *BloomBecker*, The Trial of Computer Crime, Jurimetrics Journal, Vol. 21, 1981, page 428; *Schmidt*, Legal Proprietary Interests in Computer Programs: The American Experience, Jurimetrics Journal, Vol. 21, 1981, 345 *et seq.*; *Denning*, Some Aspects of Theft of Computer Software, Auckland University Law Review, Vol. 4, 1980, 273 *et seq.*; *Weiss*, Pirates and Prizes: The Difficulties of Protecting Computer Software, Western State University Law Review, Vol. 11, 1983, page 1 *et seq.*; *Bigelow*, The Challenge of Computer Law, Western England Law Review, Vol. 7, 1985, page 401; *Thackeray*, Computer-Related Crimes, Jurimetrics Journal, 1984, page 300 *et seq.*

[136] *Andrews*, The Legal Challenge Posed by the new Technology, Jurismetrics Journal, 1983, page 43 *et seq.*

[137] *Yee*, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 *et seq.*; Who is Calling your Computer Next? Hacker!, Criminal Justice Journal, Vol. 8, 1985, page 89 *et seq.*; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review Vol. 33, 1984, page 777 *et seq.*

[138] *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 23, available at: www.mekabay.com/overviews/history.pdf.

[139] *Schjolberg*, Computer-related Offences, Council of Europe, 2004, page 4, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf.

[140] Computer-related criminality: Analysis of Legal Politics in the OECD Area, 1986.

[141] Computer-related crime: Recommendation No. R. (89) 9.

[142] Regarding the transnational dimension of cybercrime see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7.

[143] Regarding the impact of the speed of data exchange on cybercrime investigation, see: § 3.2.10.

[144] Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 17; Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9.

[145] A/RES/45/121 adopted by the UN General Assembly on 14 December 1990. The full text of the resolution is available at: www.un.org/documents/ga/res/45/a45r121.htm

[146] UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5), available at: www.uncjin.org/Documents/EighthCongress.html.

[147] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. For more information, see: § 2.9.4.

[148] Botnets is a short term for a group of compromised computers running a software that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4.

[149] *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006.

[150] *Velasco San Martin,* Jurisdictional Aspects of Cloud Computing, 2009; *Gercke*, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*

[151] *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 308, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

[152] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

[153] Regarding the emerging importance of crime statistics, see: *Osborne/Wernicke*, Introduction to Crime Analysis, 2003, page 1 *et seq.*, available at: www.crim.umontreal.ca/cours/cri3013/osborne.pdf.

[154] 2009 Internet Crime Report, Internet Crime Complaint Center, 2009, available at: www.ic3.gov/media/annualreport/2009_IC3Report.pdf.

[155] German Crime Statistics 2009, available at www.bka.de. As this number also includes traditional crimes that involved Internet technology at any stage of the offence, the increase of cases cannot necessarily be used to determine the specific development in the typology-based crime fields.

[156] Regarding the related difficulties, see: United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 229, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[157] Regarding challenges related to crime statistics in general, see: *Maguire* in Maguire/Morgan/Reiner, The Oxford Handbook of Criminology, 2007, page 241 *et seq.* available at: www.oup.com/uk/orc/bin/9780199205431/maguire_chap10.pdf.

[158] See in this context: Overcoming barriers to trust in crimes statistics, UK Statistics Authority, 2009, page 9, available at: www.statisticsauthority.gov.uk/.../overcoming-barriers-to-trust-in-crime-statistics--england-and-wales---interim-report.pdf.

[159] *Alvazzi del Frate*, Crime and criminal justice statistics challenges in Harrendorf/Heiskanen/Malby, International Statistics on Crime and Justice, 2010, page 168, available at: www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf.

[160] Computer Crime, Parliamentary Office of Science and Technology, Postnote No. 271, Oct. 2006, page 3.

[161] Regarding the related challenges, see: *Kabay*, Understanding Studies and Surveys of Computer Crime, 2009, available at: www.mekabay.com/methodology/crime_stats_methods.pdf.

[162] The US Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform the authorities, so that they can be better informed about criminal activities on the Internet. "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack," explained Mark Mershon, acting head of the FBI's New York office." See Heise News, 27.10.2007, – available at: www.heise-security.co.uk/news/80152. See also: Comments on Computer Crime – Senate Bill S. 240, Memphis State University Law Review, 1980, page 660.

[163] See *Mitchison/Urry*, Crime and Abuse in e-Business, IPTS Report, available at: www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm; *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol. 2, page, 310, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

[164] See *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 310, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf; *Smith*, Investigating Cybercrime: Barriers and Solutions, 2003, page 2, available at: www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf.

[165] In fact, newspapers as well as TV stations limit their coverage of successful Internet investigations to spectacular cases such as the identification of a paedophile by descrambling manipulated pictures of the suspect. For more information about the case and the coverage, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin; as well as the information provided on the Interpol website, available at: www.interpol.int/Public/THB/vico/Default.asp.

[166] See SOCA, International crackdown on mass marketing fraud revealed, 2007, available at: www.soca.gov.uk/downloads/massMarketingFraud.pdf.

[167] In the 2006 NW3C Internet Crime report, only 1.7 per cent of the reported total USD losses were related to the Nigerian Letter Fraud, but those cases that were reported had an average loss of USD 5 100 each. The number of reported offences is very low, while the average loss of those offences is the high.

[168] With regard to this conclusion, see also: Cybercrime, Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO Document GAO-07-705, page 22. *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

[169] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

[170] See in this context: *Hyde-Bales/Morris/Charlton*, The police recording of computer crime, UK Home Office Development and Practice Report, 2004.

[171] Symantec Global Internet Security Threat Report, Trends for 2009, 2010, available at www.symantec.com/business/theme.jsp?themeid=threatreport, page 15.

[172] National Fraud Information Center, 2007 Internet Fraud Statistics, 2008, available at: www.fraud.org/internet/intstat.htm.

[173] See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report.

[174] 2nd ISSA/UCD Irish Cybercrime Survey, 2008, available at: www.issaireland.org/2nd%20ISSA%20UCD%20Irish%20Cybercrime%20Survey%20-%20Results%2017DEC08.pdf.

[175] Symantec Intelligence Quarterly, April-June 2010, available at www.symantec.com/business/theme.jsp?themeid=threatreport.

[176] 2010 CSO CyberSecurity Watch Survey, 2010.

[177] 2008 CSI Computer Crime and Security Survey, 2009, page 15.

[178] Symantec Global Internet Security Threat Report, Trends for 2009, 2010, available at: www.symantec.com/business/theme.jsp?themeid=threatreport, page 7,

[179] See 2005 FBI Computer Crime Survey, page 10.

[180] See: § 2.4.

[181] *Choo/Smith/McCusker*, Future directions in technology-enabled crime: 2007-09, Australian Institute of Criminology, Research and Public Policy series, No. 78, page 62; ECPAT, Violence against Children in Cyberspace, 2005, page 54; Council of Europe Organized Crime Situation Report 2005, Focus on Cybercrime, page 41.

[182] *Bialik*, Measuring the Child-Porn Trade, The Wall Street Journal, 18.04.2006.

[183] Computer Security Institute (CSI), United States.

[184] The CSI Computer Crime and Security Survey 2007 is available at: www.gocsi.com/

[185] See CSI Computer Crime and Security Survey 2007, page 1, available at: www.gocsi.com/. Having regard to the composition of the respondents, the survey is likely to be relevant for the United States only.

[186] With regard to this conclusion, see also: Cybercrime, Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO Document GAO-07-705, page 22, available at: www.gao.gov/new.items/d07705.pdf. *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

[187] See below: § 2.4.

[188] Regarding the development of computer systems, see: *Hashagen*, The first Computers – History and Architectures.

[189] See in this context, for example, the Explanatory Report to the Council of Europe Convention on Cybercrime, No. 81: "The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception."

[190] From a legal perspective, there is no real need to differentiate between "computer hackers" and "computer crackers" as – in the context of illegal access – both terms are used to describe persons who enter a computer system without right. The main difference is the motivation. The term "hacker" is used to describe a person who enjoys exploring the details of programmable systems, without breaking the law. The term "cracker" is used to describe a person who breaks into computer systems in general by violating the law.

[191] In the early years of IT development, the term "hacking" was used to describe the attempt to get more out of a system (software or hardware) than it was designed for. Within this context, the term "hacking" was often used to describe a constructive activity.

[192] See *Levy*, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: www.aic.gov.au/publications/htcb/htcb005.pdf; *Taylor*, Hacktivism: In Search of lost ethics? in *Wall*, Crime and the Internet, 2001, page 61; *Yee*, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 *et seq.*; Who is Calling your Computer Next? Hacker!, Criminal Justice Journal, Vol. 8, 1985, page 89 *et seq.*; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review Vol. 33, 1984, page 777 *et seq.*

[193] See the statistics provided by HackerWatch. The Online-Community HackerWatch publishes reports about hacking attacks. Based on their sources, more than 250 million incidents were reported; *Biegel,* Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 *et seq.* in the month of August 2007. Source: www.hackerwatch.org.

[194] For an overview of victims of hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 *et seq.*; Regarding the impact, see *Biegel,* Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 *et seq.*

[195] *Sieber*, Council of Europe Organised Crime Report 2004, page 65.

[196] *Musgrove*, Net Attack Aimed at Banking Data, Washington Post, 30.06.2004.

[197] *Sieber*, Council of Europe Organised Crime Report 2004, page 66.

[198] *Sieber*, Council of Europe Organised Crime Report 2004, page 65. Regarding the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.

[199] Hacking into a computer system and modifying information on the first page to prove the ability of the offender can – depending on the legislation in place – be prosecuted as illegal access and data interference. For more information, see below: § 6.2.1 and § 6.2.4.

[200] The term "hacktivism" combines the words hack and activism. It describes hacking activities performed to promote a political ideology. For more information, see: *Anderson*, Hacktivism and Politically Motivated Computer Crime, 2005, available at: www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf. Regarding cases of political attacks, see: *Vatis*, cyberattacks during the war on terrorism: a predictive analysis, available at: www.ists.dartmouth.edu/analysis/cyber_a1.pdf.

[201] A hacker left messages on the website that accused the United States and Israel of killing children. For more information, see BBC News, "UN's website breached by hackers", available at: http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6943385.stm

[202] The abuse of hacked computer systems often causes difficulties for law-enforcement agencies, as electronic traces do not often lead directly to the offender, but first of all to the abused computer systems.

[203] Regarding different motivations and possible follow-up acts, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1;

[204] The Online-Community HackerWatch publishes reports about hacking attacks. Based on their sources, more than 250 million incidents were reported in the month of August 2007. Source: www.hackerwatch.org.

[205] Regarding the supportive aspects of missing technical protection measures, see *Wilson*, Computer Attacks and Cyber Terrorism, Cybercrime & Security, IIV-3, page 5.

[206] See Heise News, Online-Computer werden alle 39 Sekunden angegriffen, 13.02.2007, available at: www.heise.de/newsticker/meldung/85229. The report is based on an analysis from Professor Cukier.

[207] For an overview of examples of successful hacking attacks, see http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotriontе*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 *et seq.*

[208] Regarding threats from Cybercrime toolkits, see Opening Remarks by ITU Secretary-General, 2nd Facilitation Meeting for WSIS Action Line C5, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/sg-opening-remarks-14-may-2007.pdf. See in this context also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 29, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[209] For an overview of the tools used, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

[210] Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see: *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

[211] Websense Security Trends Report 2004, page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

[212] For an overview of the tools used, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

[213] *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9, available at: www.212cafe.com/download/e-book/A.pdf.

[214] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.250.

[215] For an overview of the tools used to perform high-level attacks, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf; *Erickson*, Hacking: The Art of Exploitation, 2003.

[216] Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see: *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. For more information about botnets see below: § 3.2.9.

[217] See *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

[218] See in this context Art. 2, sentence 2, Convention on Cybercrime.

[219] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.264.

[220] One example of this is the German Criminal Code, which criminalized only the act of obtaining data (Section 202a) until 2007, when the provision was changed. The following text is taken from the old version of Section 202a – Data Espionage:

(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.

(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

[221] For the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 *et seq.*; *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 *et seq.*

[222] Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2003, page 1, available at: www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf.

[223] For more information about that case, see: *Stoll*, Stalking the wily hacker, available at: http://pdf.textfiles.com/academics/wilyhacker.pdf; *Stoll*, The Cuckoo's Egg, 1998.

[224] See *Sieber*, Council of Europe Organised Crime Report 2004, page 88 *et seq.*; *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

[225] *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf.

[226] Examples are software tools that are able to break passwords. Another example is a software tool that records keystrokes (keylogger). Keyloggers are available as software solutions or hardware solutions.

[227] See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

[228] See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[229] For more information, see *Mitnick/Simon/Wozniak*, The Art of Deception: Controlling the Human Element of Security.

[230] See the information offered by an anti-phishing working group, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See: *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4.

[231] Regarding the elements of an Anti-Cybercrime Strategy, see below: § 4.

[232] "Users should have access to cryptography that meets their needs, so that they can trust in the security of information and communications systems, and the confidentiality and integrity of data on those systems" – See OECD Guidelines for Cryptography Policy, V 2, available at: www.oecd.org/document/11/0,3343,en_2649_34255_1814731_1_1_1_1,00.html.

[233] Physical research proves that it can take a very long time to break encryption, if proper technology is used. See *Schneier*, Applied Cryptography, page 185. For more information regarding the challenge of investigating cybercrime cases that involve encryption technology, see below: § 3.2.14.

[234] The Council of Europe Convention on Cybercrime contains no provision criminalizing data espionage.

[235] Regarding the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 *et seq.*

[236] Regarding the impact of this behaviour for identity theft, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf

[237] *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

[238] See: 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2, available at: www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf.

[239] See *Hackworth*, Sypware, Cybercrime & Security, IIA-4. Regarding user reactions to the threat of spyware, see: *Jaeger/ Clarke*, The Awareness and Perception of Spyware amongst Home PC Computer Users, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Jaeger%20Clarke%20-%20The%20Awareness%20and%20Perception%20of%20Spyware%20amongst%20Home%20PC%20Computer%20Users.pdf

[240] See *Hackworth*, Sypware, Cybercrime & Security, IIA-4, page 5.

[241] For further information about keyloggers, see: http://en.wikipedia.org/wiki/Keylogger; Netadmintools Keylogging, available at: www.netadmintools.com/part215.html

[242] It is easy to identify credit-card numbers, as they in general contain 16 digits. By excluding phone numbers using country codes, offenders can identify credit-card numbers and exclude mistakes to a large extent.

[243] One approach to gain access to a computer system in order to install a keylogger is, for example, to gain access to the building where the computer is located using social engineering techniques, e.g. a person wearing a uniform from the fire brigade pretending to check emergency exits has a good chance of gaining access to a building, if more extensive security is not in place. Further approaches can be found in *Mitnick*, The Art of Deception: Controlling the Human Element of Security, 2002.

[244] Regular hardware checks are a vital part of any computer security strategy.

[245] See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

[246] See the information offered by an anti-phishing working group, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606.

[247] For more information on the phenomenon of phishing, see below: § 2.9.4.

[248] *Leprevost*, Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues, Development of surveillance technology and risk of abuse of economic information, 2.4, available at: http://cryptome.org/stoa-r3-5.htm.

[249] With the fall in price of server storage space, the external storage of information has become more popular. Another advantage of external storage is that information can be accessed from every Internet connection.

[250] Regarding the interception of VoIP to assist law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf. Regarding the potential of VoIP and regulatory issues, see: *Braverman*, VoIP: The Future of Telephony is now…if regulation doesn't get in the way, The Indian Journal of Law and Technology, Vol.1, 2005, page 47 *et seq.*, available at: www.nls.ac.in/students/IJLT/resources/1_Indian_JL&Tech_47.pdf.

[251] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 30, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[252] *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2, page 6 *et seq.*

[253] The radius depends on the transmitting power of the wireless access point. See http://de.wikipedia.org/wiki/WLAN.

[254] With regard to the time necessary for decryption, see below: § 3.2.14.

[255] Regarding the difficulties in Cybercrime investigations that include wireless networks, see *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2; *Urbas/Krone*, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: www.aic.gov.au/publications/tandi2/tandi329t.html.

[256] *Sieber*, Council of Europe Organised Crime Report 2004, page 97.

[257] With regard to the interception of electromagnetic emissions, see: Explanatory Report to the Convention on Cybercrime, No. 57.

[258] See http://en.wikipedia.org/wiki/Computer_surveillance#Surveillance_techniques.

[259] e.g. the electromagnetic emission caused by transmitting the information displayed on the screen from the computer to the screen.

[260] For more details on legal solutions, see below: § 6.2.4.

[261] See in this context also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 32, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[262] *Sieber*, Council of Europe Organised Crime Report 2004, page 107.

[263] A computer virus is software that is able to replicate itself and infect a computer, without the permission of the user, to harm the computer system. See *Spafford*, The Internet Worm Program: An Analysis, page 3; *Cohen*, Computer Viruses – Theory and Experiments, available at: http://all.net/books/virus/index.html; *Adleman*, An Abstract Theory of Computer Viruses, Advances in Cryptography – Crypto, Lecture Notes in Computer Science, 1988, page 354 *et seq.* Regarding the economic impact of computer viruses, see: *Cashell/Jackson/Jickling/Webel*, The Economic Impact of Cyber-Attacks, page 12; Symantec Internet Security Threat Report,Trends for July-December 2006, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/entwhitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

[264] *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 23, available at: www.mekabay.com/overviews/history.pdf.

[265] *White/Kephart/Chess*, Computer Viruses: A Global Perspective, available at: www.research.ibm.com/antivirus/SciPapers/White/VB95/vb95.distrib.html.

[266] Payload describes the function the virus performs after it is installed on victims' computers and activated. Examples of the payload are displaying messages or performing certain activities on computer hardware, such as opening the CD drive or deleting or encrypting files.

[267] Regarding the various installation processes, see: The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, page 21 *et seq.*, available at: www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

[268] See BBC News, Virus-like attack hits web traffic, 25.01.2003, http://news.bbc.co.uk/2/hi/technology/2693925.stm;

[269] Critical Infrastructure Protection Department Of Homeland Security Faces Challenges In Fulfilling Cybersecurity Responsibilities, GAO, 2005 GAO-05-434, page 12, available at: www.gao.gov/new.items/d05434.pdf.

[270] *Cashell/Jackson/Jickling/Webel*, The Economic Impact of Cyber-Attacks, page 12, available at: www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

[271] *Cashell/Jackson/Jickling/Webel*, The Economic Impact of Cyber-Attacks, page 12, available at: www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

[272] See *Szor*, The Art of Computer Virus Research and Defence, 2005.

[273] One example of a virus that encrypts files is the Aids Info Disk or PC Cyborg Trojan. The virus hid directories and encrypted the names of all files on the C-drive. Users were asked to 'renew their licence' and contact PC Cyborg

Corporation for payment. For more information, see: *Bates*, "Trojan Horse: AIDS Information Introductory Diskette Version 2.0" in *Wilding/Skulason*, Virus Bulletin, 1990, page 3.

[274] In 2000, a number of well-known United States e-commerce businesses were targeted by denial-of-service attacks. A full list of the attacks business is provided by *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

[275] Regarding the possible financial consequences, see: *Campbell/Gordon/Loeb/Zhou*, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, page 431-448.

[276] Examples include: Inserting metal objects in computer devices to cause electrical shorts, blowing hairspray into sensitive devices or cutting cables. For more examples, see *Sieber*, Council of Europe Organised Crime Report 2004, page 107.

[277] Regarding the possible financial consequences, see: *Campbell/Gordon/Loeb/Zhou*, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, page 431-448.

[278] *Sieber*, Council of Europe Organised Crime Report 2004, page 107.

[279] A denial-of-service (DoS) attack aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

[280] The term "worm" was used by *Shoch/Hupp*, The 'Worm' Programs – Early Experience with a Distributed Computation, published in 1982. This publication is available for download: http://vx.netlux.org/lib/ajm01.html. With regard to the term 'worm', they refer to the science-fiction novel, "The Shockwave Rider" by John Brunner, which describes a program running loose through a computer network.

[281] For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP.

[282] See *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 14, available at: http://media.hoover.org/documents/0817999825_1.pdf. The attacks took place between 07.02.2000 and 09.02.2000. For a full list of attacked companies and the dates of the attacks, see: *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf.

[283] July, 2009 South Korea and US DDosc Attacks, Arbor Networks, 2009, available at: www.idcun.com/uploads/pdf/July_KR_US_DDoS_Attacks.pdf.

[284] *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html;

[285] Regarding the different approaches, see below: § 6.2.6.

[286] For reports on cases involving illegal content, see *Sieber*, Council of Europe Organised Crime Report 2004, page 137 *et seq.*

[287] One example of the wide criminalization of illegal content is Sec. 86a German Penal Code. The provision criminalizes the use of symbols of unconstitutional parties: Section 86a: Use of Symbols of Unconstitutional Organizations:

(1) Whoever: 1. domestically distributes or publicly uses, in a meeting or in writings (Section 11 subsection (3)) disseminated by him, symbols of one of the parties or organizations indicated in Section 86 subsection (1), nos. 1, 2 and 4; or 2. produces, stocks, imports or exports objects which depict or contain such symbols for distribution or use domestically or abroad, in the manner indicated in number 1, shall be punished with imprisonment for not more than three years or a fine.
(2) Symbols, within the meaning of subsection (1), shall be, in particular, flags, insignia, uniforms, slogans and forms of greeting. Symbols which are so similar as to be mistaken for those named in sentence 1 shall be deemed to be equivalent thereto.
(3) Section 86 subsections (3) and (4), shall apply accordingly.

[288] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[289] Concerns over freedom of expression (e.g. the First Amendment to the United States Constitution) explain why certain acts of racism were not made illegal by the Convention on Cybercrime, but their criminalization was included in the First Additional Protocol. See Explanatory Report to the First Additional Protocol, No. 4.

[290] The 2006 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression points out that "in many countries, overbroad rules in this area are abused by the powerful to limit non-traditional, dissenting, critical, or minority voices, or discussion about challenging social issues". In 2008 the Joint Declaration highlights that international organizations, including the United Nations General Assembly and Human Rights Council, should desist from the further adoption of statements supporting the idea of defamation of religions.

[291] 1996 Johannesburg Principles on National Security, Freedom of Expression and Access to Information.

[292] The 2002 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression points out that "defamation is not a justifiable restriction on freedom of expression; all criminal defamation laws should be abolished and replaced, where necessary, with appropriate civil defamation laws".

[293] International Mechanisms for Promoting Freedom of Expression, Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation, by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, and the ACHPR (African Commission on Human and Peoples Rights) Special Rapporteur on Freedom of Expression and Access to Information, 2008.

[294] See below: §§ 3.2.6 and 3.2.7.

[295] In many cases, the principle of dual criminality hinders international cooperation.

[296] Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion about filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%

20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches, see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

297 Regarding this approach, see: *Stadler*, Multimedia und Recht 2002, page 343 *et seq.*; *Mankowski*, Multimedia und Recht 2002, page 277 *et seq.*

298 See *Sims*, Why Filters Can't Work, available at: http://censorware.net/essays/whycant_ms.html; *Wallace*, Purchase of blocking software by public libraries is unconstitutional, available at: http://censorware.net/essays/library_jw.html.

299 The OpenNet Initiative is a transatlantic group of academic institutions that reports on internet filtering and surveillance. Harvard Law School and the University of Oxford participate in the network, among others. For more information, see: www.opennet.net.

300 *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

301 Depending on the availability of broadband access.

302 Access is in some countries is limited by filter technology. Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion about filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No. 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches,
see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

303 With regard to the electronic traces that are left and the instruments needed to trace offenders, see below: § 6.5.

304 *Ropelato*, Internet Pornography Statistics, available at: http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

305 About a third of all files downloaded in file-sharing systems contained pornography. *Ropelato*, Internet Pornography Statistics, available at: http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

306 One example for this approach can be found in Sec. 184 German Criminal Code (Strafgesetzbuch):

> Section 184 Dissemination of Pornographic Writings
> (1) Whoever, in relation to pornographic writings (Section 11 subsection (3)):
> 1. offers, gives or makes them accessible to a person under eighteen years of age; […]

307 Regarding this aspect, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 36, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

308 See: *Nowara/Pierschke*, Erzieherische Hilfen fuer jugendliche Sexual(straf)taeter, Katamnesestudie zu den vom Land Nordrhein-Westfalen gefoerterten Modellprojekten, 2008.

309 See *Siebert*, Protecting Minors on the Internet: An Example from Germany, in Governing the Internet Freedom and Regulation in the OSCE Region, page 150, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

310 One example is the 2006 Draft Law, Regulating the protection of Electronic Data and Information and Combating Crimes of Information (Egypt):
Sec. 37: Whoever makes, imitates, obtains, or possesses, for the purpose of distribution, publishing, or trade, electronically processed pictures or drawings that are publicly immoral, shall be punished with detention for a period

not less than six months, and a fine not less than five hundred thousand Egyptian pounds, and not exceeding seven hundred thousand Egyptian pounds, or either penalty.

311 National sovereignty is a fundamental principle in International Law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

312 Regarding the principle of "dual criminality", see below: § 6.6.2.

313 Regarding technical approaches in the fight against obscenity and indecency on the Internet, see: *Weekes*, Cyber-Zoning a Mature Domain: The Solution to Preventing Inadvertent Access to Sexually Explicit Content on the Internet, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue1/v8i1_a04-Weekes.pdf.

314 Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion about filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

315 Regarding the risk of detection with regard to non Internet-related acts, see: *Lanning*, Child Molesters: A Behavioral Analysis, 2001, page 63.

316 *Healy*, Child Pornography: An International Perspective, 2004, page 4.

317 *Wortley/Smallbone*, Child Pornography on the Internet, Problem-Oriented Guides for Police, USDOJ, 2006, page, 1.

318 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8 *et seq.*

319 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

320 *Lanning*, Child Molesters: A Behavioral Analysis, 2001, page 62; Rights of the Child, Commission on Human Rights, 61st session, E/CN.4/2005/78, page 8; *Healy*, Child Pornography: An International Perspective, 2004, page 5; Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 19.

321 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

322 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

323 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

324 *Jenkins*, Beyond Tolerance, Child Pornography on the Internet, 2001, page 41.

325 Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 17.

326 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9.

327 Vienna Commitment against Child Pornography on the Internet, 1st October 1999; Europol, Child Abuse in relation to Trafficking in Human Beings Fact Sheet January 2006, page 2; *Jenkins*, Beyond Tolerance, Child Pornography on the Internet, 2001, page 49.

[328] *Bloxsome/Kuhn/Pope/Voges*, The Pornography and Erotica Industry: Lack of Research and Need for a Research Agenda, Griffith University, Brisbane, Australia: 2007 International Nonprofit and Social Marketing Conference, 27-28 Sep 2007, page 196.

[329] Europol, Child Abuse in relation to Trafficking in Human Beings Fact Sheet January 2006, page 1; *Eneman*, A Critical Study of ISP Filtering Child Pornography, 2006, page 1. *McCulloch*, Interpol and Crimes against Children – in Quayle/Taylor, Viewing child pornography on the Internet: Understanding the offence, managing the offender, helping the victims, 2005.

[330] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9; Promotion and Protection of the Right of Children, Sale of children, child prostitution and child pornography, UN General Assembly, 51st session, A/51/456, No. 29.

[331] *Eneman*, A Critical Study of ISP Filtering Child Pornography, 2006, page 1; Promotion and Protection of the Right of Children, Sale of children, child prostitution and child pornography, UN General Assembly, 51st session, A/51/456, No. 29; *Choo/Smith/McCusker*, Future directions in technology-enabled crime: 2007-09, Australian Institute of Criminology, Research and Public Policy series, No. 78, page 62.

[332] According to ITU, there were over 2 billion Internet users by the end of 2010, of which 1.2 billion in developing countries. For more information see: ITU ICT Facts and Figures 2010, page 3, available at: www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

[333] *Carr*, Child Abuse, Child Pornography and the Internet, 2004, page 7.

[334] See in this context, for example: *Carr*, Child Abuse, Child Pornography and the Internet, 2004, page 8.

[335] *Lanning*, Child Molesters: A Behavioral Analysis, 2001, page 64.

[336] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 12.

[337] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[338] See, for example, the "G8 Communique", Genoa Summit, 2001, available at: www.g8.gc.ca/genoa/july-22-01-1-e.asp.

[339] United Nations Convention on the Right of the Child, A/RES/44/25, available at: www.hrweb.org/legal/child.html. Regarding the importance of cybercrime legislation see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 35, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[340] Council Framework Decision on combating the sexual exploitation of children and child pornography, 2004/68/JHA, available at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf.

[341] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No: 201, available at: http://conventions.coe.int.

[342] *Sieber*, Council of Europe Organised Crime Report 2004, page 135. Regarding the means of distribution, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 10 *et seq.*, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

[343] See: *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 5, available at: www.missingkids.com/en_US/publications/NC144.pdf.

[344] See: *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 5, available at: www.missingkids.com/en_US/publications/NC144.pdf.

[345] For more information, see: Child Pornography: Model Legislation & Global Review, 2010, page 3, available at: www.icmec.org/en_X1/icmec_publications/English__6th_Edition_FINAL_.pdf.

[346] See *Walden*, Computer Crimes and Digital Investigations, 2007, page 66.

[347] It is possible to make big profits in a rather short period of time by offering child pornography – this is one way how terrorist cells can finance their activities, without depending on donations.

[348] Police authorities and search engines forms alliance to beat child pornography, available at: http://about.picsearch.com/p_releases/police-authorities-and-search-engines-forms-alliance-to-beat-child-pornography/; "Google accused of profiting from child porn", available at: www.theregister.co.uk/2006/05/10/google_sued_for_promoting_illegal_content/print.html.

[349] See ABA, International Guide to Combating Cybercrime, page 73.

[350] Regarding the use of electronic currencies in money-laundering activities, see: *Ehrlich*, Harvard Journal of Law & Technology, Volume 11, page 840 *et seq.*

[351] For more information, see: *Wilson*, Banking on the Net: Extending Bank Regulations to Electronic Money and Beyond., (1997) 30 Creighton Law Review 671 at 690.

[352] *Smith*, Child pornography operation occasions scrutiny of millions of credit card transactions, available at: www.heise.de/english/newsticker/news/print/83427.

[353] With regard to the concept see for example: *Nakamoto* (name reported to be used as alias), Bitcoin: A Peer-to-Peer Electronic Cash System, available at: www.bitcoin.org/bitcoin.pdf.

[354] Regarding the basic concept of such investigation see: Following the Money 101: A Primer on Money-Trail Investigations, Coalition for International Justice, 2004, available at: www.media.ba/mcsonline/files/shared/prati_pare.pdf.

[355] Regarding approaches to detect and prevent such transfers see: Financial Coalition Against Child Pornography, Report on Trends in Online Crime and Their Potential Implications for the Fight Against Commercial Child Pornography, Feb. 2011, available at:

[356] See below: § 3.2.14.

[357] Based on the "National Juvenile Online Victimization Study", 12 per cent of arrested possessors of Internet-related child pornography used encryption technology to prevent access to their files. *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

[358] See below: § 3.2.14.

[359] For an overview of the different obligations of Internet service providers that are already implemented or under discussion, see: *Gercke*, Obligations of Internet Service Providers with regard to child pornography: legal issue, 2009, available at www.coe.int/cybercrime.

[360] Radical groups in the United States recognized the advantages of the Internet for furthering their agenda at an early stage. See: *Markoff*, Some computer conversation is changing human contact, NY-Times, 13.05.1990.

[361] *Sieber*, Council of Europe Organised Crime Report 2004, page 138.

[362] *Akdeniz*, Governance of Hate Speech on the Internet in Europe, in "Governing the Internet Freedom and Regulation in the OSCE Region", page 91, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[363] See: Digital Terrorism & Hate 2006, available at: www.wiesenthal.com.

[364] *Whine*, Online Propaganda and the Commission of Hate Crime, available at: www.osce.org/documents/cio/2004/06/3162_en.pdf

[365] See: ABA International Guide to Combating Cybercrime, page 53.

[366] Regarding the criminalization in the United States, see: *Tsesis*, Prohibiting Incitement on the Internet, Virginia Journal of Law and Technology, Vol. 7, 2002, available at: www.vjolt.net/vol7/issue2/v7i2_a05-Tsesis.pdf.

[367] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[368] See: *Greenberg*, A Return to Liliput: The Licra vs. Yahoo! Case and the Regulation of Online Content in the World Market, Berkeley Technology Law Journal, Vol. 18, page 1191 *et seq.*; *Van Houweling*; Enforcement of Foreign Judgements, The First Amendment, and Internet Speech: Note for the Next Yahoo! v. Licra, Michigan Journal of International Law, 2003, page 697 *et seq.*; Development in the Law, The Law of Media, Harvard Law Review, Vol. 120, page 1041.

[369] See: Yahoo Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme, 169 F.Supp. 2d 1181, 1192 (N.D. Cal 2001). Available at: www.courtlinkeaccess.com/DocketDirect/FShowDocket.asp?Code=21313829894194994194493893493893796151919991.

[370] *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International, 2006, page 144.

[371] See: Explanatory Report to the First Additional Protocol, No. 4.

[372] See: *Barkham*, Religious hatred flourishes on web, The Guardian, 11.05.2004, available at: www.guardian.co.uk/religion/Story/0,,1213727,00.html.

[373] Regarding legislative approaches in the United Kingdom see *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.192.

[374] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman,* Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[375] *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[376] For more information on the "cartoon dispute", see: the Times Online, 70.000 gather for violent Pakistan cartoons protest, available at: www.timesonline.co.uk/tol/news/world/asia/article731005.ece; *Anderson*, Cartoons of Prophet Met With Outrage, Washington Post, available at: www.washingtonpost.com/wp-dyn/content/article/2006/01/30/AR2006013001316.html; *Rose*, Why I published those cartoons, Washington Post, available at: www.washingtonpost.com/wp-dyn/content/article/2006/02/17/AR2006021702499.html.

[377] Sec. 295-C of the Pakistan Penal Code:
295-C. Use of derogatory remarks, etc., in respect of the Holy Prophet: Whoever by words, either spoken or written, or by visible representation or by any imputation, innuendo, or insinuation, directly or indirectly, defiles the sacred name of the Holy Prophet Mohammed (Peace be Upon Him) shall be punished with death, or imprisonment for life, and shall also be liable to fine.

[378] Sec. 295-B of the Pakistan Penal Code:
295-B. Defiling, etc., of Holy Qur'an : Whoever wilfully defiles, damages or desecrates a copy of the Holy Qur'an or of an extract there from or uses it in any derogatory manner or for any unlawful purpose shall be punishable with imprisonment for life.

[379] Regarding the growing importance of Internet gambling, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf ; *Brown/Raysman*, Property Rights in Cyberspace Games and other novel legal issues in virtual property, The Indian Journal of Law and Technology, Vol. 2, 2006, page 87 *et seq.* available at: www.nls.ac.in/students/IJLT/resources/2_Indian_JL&Tech_87.pdf.

[380] www.secondlife.com.

[381] The number of accounts published by Linden Lab. See: www.secondlife.com/whatis/. Regarding Second Life in general, see: *Harkin*, Get a (second) life, Financial Times, available at: www.ft.com/cms/s/cf9b81c2-753a-11db-aea1-0000779e2340.html.

[382] Heise News, 15.11.2006, available at: www.heise.de/newsticker/meldung/81088; DIE ZEIT, 04.01.2007, page 19.

[383] BBC News, 09.05.2007 Second Life 'child abuse' claim, available at: http://news.bbc.co.uk/1/hi/technology/6638331.stm.

[384] *Leapman*, Second Life world may be haven for terrorists, Sunday Telegraph, 14.05.2007, available at: www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/05/13/nternet13.xml; *Reuters*, UK panel urges real-life treatment for virtual cash, 14.05.2007, available at: http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/.

[385] See: *Olson*, Betting No End to Internet Gambling, Journal of Technology Law and Policy, Vol. 4, Issue 1, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.

[386] Christiansen Capital Advisor. See www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm.

[387] The revenue of United States casinos in 2005 (without Internet gambling) was more than USD 84 billion, from: *Landes*, Layovers And Cargo Ships: "The Prohibition Of Internet Gambling And A Proposed System Of Regulation", page 915, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf;

[388] See, for example, GAO, "Internet Gambling – An Overview of the Issues", available at: www.gao.gov/new.items/d0389.pdf. Regarding the WTO Proceedings "US Measures Affecting the Cross-Border Supply of Gambling and Betting Services", see: www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm; Article 21.5 panel concluded that the United States had failed to comply with the recommendations and rulings of the DSB.

[389] For more information, see: BBC News, Tiny Macau overtakes Las Vegas, at: http://news.bbc.co.uk/2/hi/business/6083624.stm.

[390] See Art. 300 China Criminal Code:
Whoever, for the purpose of reaping profits, assembles a crew to engage in gambling, opens a gambling house, or makes an occupation of gambling, is to be sentenced to not more than three years of fixed-term imprisonment, criminal detention, or control, in addition to a fine.

[391] Besides gambling in Macau, Chinese have started to use Internet gambling intensively. See: Online Gambling challenges China's gambling ban, available at: www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

[392] For more information, see: http://en.wikipedia.org/wiki/Internet_casino.

[393] See: OSCE Report on Money Laundering Typologies 2000 – 2001, page 3, available at: www.oecd.org/dataoecd/29/36/34038090.pdf; *Coates*, Online casinos used to launder cash, available at: www.timesonline.co.uk/tol/news/politics/article620834.ece?print=yes&randnum=1187529372681.

[394] See, for example, Online Gambling challenges China's gambling ban, available at: www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

[395] For an overview of the early United States legislation, see: *Olson*, Betting No End to Internet Gambling, Journal of Technology Law and Policy, Vol. 4, Issue 1, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.

[396] See § 5367 Internet Gambling Prohibition Enforcement Act.

[397] See *Reder/O'Brien*, Corporate Cybersmear: Employers File John Doe Defamation Lawsuits Seeking The Identity Of Anonymous Employee Internet Posters, Mich. Telecomm. Tech. L. Rev. 195, 2002, page 196, available at www.mttlr.org/voleight/Reder.pdf.

[398] Regarding the situation in blogs, see*: Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts" Washington University Law Review, 2006, page 1157 *et seq.*, available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 *et seq.*, available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol. 84, 2006, page 1187 *et seq.*, available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

[399] Regarding the privacy concerns related to social networks, see: *Hansen/Meissner* (ed.), Linking digital identities, page 8 – An executive summary is available in English (page 8-9). The report is available at: www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

[400] Regarding the controversial discussion about the criminalization of defamation, see: Freedom of Expression, Free Media and Information, Statement of Mr McNamara, US Delegation to the OSCE, October 2003, available at: http://osce.usmission.gov/archive/2003/10/FREEDOM_OF_EXPRESSION.pdf; *Lisby*, No Place in the Law: Criminal Libel in American Jurisprudence, 2004, available at: http://www2.gsu.edu/~jougcl/projects/40anniversary/criminallibel.pdf. Regarding the development of the offence, see: *Walker*, Reforming the Crime of Libel, New York Law School Law Review, Vol. 50, 2005/2006, page 169, available at: www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf;

Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: www.article19.org/pdfs/standards/definingdefamation.pdf.

401 See *Sieber*, Council of Europe Organised Crime Report 2004, page 105.

402 With regard to the challenges of investigating offences linked to anonymous services see below: § 3.2.l2.

403 See: www.wikipedia.org

404 See *Sieber*, Council of Europe Organised Crime Report 2004, page 145.

405 Similar difficulties can be identified with regard to the availability of information through the cache function of search engines and web archives, such as www.archive.org.

406 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

407 See in this context: *Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts, Washington University Law Review, 2006, page 1157 *et seq.*, available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 *et seq.*, available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol. 84, 2006, page 1187 *et seq.*, available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

408 For a more precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

409 *Tempelton*, Reaction to the DEC Spam of 1978, available at: www.templetons.com/brad/spamreact.html.

410 Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

411 The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails were spam. See: www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf. The provider Postini published a report in 2007 identifying up to 75 per cent spam e-mail, see www.postini.com/stats/. The Spam-Filter-Review identifies up to 40 per cent spam e-mail, see: http://spam-filter-review.toptenreviews.com/spam-statistics.html. Article in The Sydney Morning Herald, 2006: The year we were spammed a lot, 16 December 2006; www.smh.com.au/news/security/2006-the-year-we-were-spammed-a-lot/2006/12/18/1166290467781.html.

412 2007 Sophos Report on Spam-relaying countries, available at: www.sophos.com/pressoffice/news/articles/2007/07/dirtydozjul07.html.

413 For more information about the technology used to identify spam e-mails, see: *Hernan/Cutler/Harris*, Email Spamming Countermeasures: Detection and Prevention of Email Spamming, available at: www.ciac.org/ciac/bulletins/i-005c.shtml. For an overview on different approaches, see: BIAC ICC Discussion Paper on SPAM, 2004, available at: www.itu.int/osg/csd/spam/contributions/ITU%20workshop%20on%20spam%20BIAC%20ICCP%20Spam%20Discussion%20Paper.pdf.

414 *Lui/Stamm*, Fighting Unicode-Obfuscated Spam, 2007, page 1, available at: www.ecrimeresearch.org/2007/proceedings/p45_liu.pdf.

415 Regarding the filter technologies available, see: *Goodman*, Spam: Technologies and Politics, 2003, available at: http://research.microsoft.com/~joshuago/spamtech.pdf. Regarding user-oriented spam prevention techniques, see: *Rotenberg/Liskow*, ITU WSIS Thematic Meeting On Countering Spam, ConsumerPerspectives On Spam: Challenges And Challenges, available at: www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

416 Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see: *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf.

[417] Current analyses suggest that up to a quarter of all computer systems may have been recruited to act as part of botnets, see: *Weber*, Criminals may overwhelm the web, BBC News, 25.01.2007, available at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6298641.stm.

[418] Regarding international approaches in the fight against botnets, see: ITU Botnet Mitigation Toolkit, Background Information, ICT Application and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunication Development Sector, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit-background.pdf.

[419] See: *Allmann*, The Economics of Spam, available at: http://acmqueue.org/modules.php?name=Content&pa=showpage&pid=108; *Prince*, ITU Discussion Paper "Countering Spam: How to Craft an Effective Anti-Spam Law", page 3 with further references, available at: www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf.

[420] Bulk discounts for spam, Heise News, 23.10.2007, available at: www.heise-security.co.uk/news/97803.

[421] *Thorhallsson*, A User Perspective on Spam and Phishing, in Governing the Internet Freedom and Regulation in the OSCE Region, page 208, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[422] Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[423] See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[424] See *Sieber*, Council of Europe Organised Crime Report 2004, page 140.

[425] See for example the United States International Traffic in Arms Regulation or the Wassenaar Agreement, which is a convention on arms control. 40 countries already participate in the agreement. For more information, see: www.wassenaar.org/publicdocuments/whatis.html or *Grimmett*, Military Technology and Conventional Weapons Export Controls: The Wassenaar Arrangement.

[426] See in this context: Council of Europe, Resolution ResAP(2007)2 on good practices for distributing medicines via mail order which protect patient safety and the quality of the delivered medicine, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=ResAP(2007)2&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

[427] See for example *Henney*, Cyberpharmacies and the role of the US Food And Drug Administration, available at: https://tspace.library.utoronto.ca/html/1807/4602/jmir.html; *De Clippele*, Legal aspects of online pharmacies, Acta Chir Belg, 2004, 104, page 364, available at: www.belsurg.org/imgupload/RBSS/DeClippele_0404.pdf; *Basal*, What's a Legal System to Do? The Problem of Regulating Internet Pharmacies, available at: www.tnybf.org/success%20stories/2006%20Meyer%20Scholarship%20Recipient%20Essay.pdf.

[428] See: See *Conway*, Terrorist Uses of the Internet and Fighting Back, Information and Security, 2006, page 16, United States Department of Justice 1997 Report on the availability of bomb-making information, available at: www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html; *Sieber*, Council of Europe Organised Crime Report 2004, page 141.

[429] E.g. by offering the download of files containing music, movies or books.

[430] Regarding the ongoing transition process, see: OECD Information Technology Outlook 2006, Highlights, page 10, available at: www.oecd.org/dataoecd/27/59/37487604.pdf.

[431] See *Hartstack*, Die Musikindustrie unter Einfluss der Digitalisierung, 2004, page 34 *et seq.*

[432] Besides these improvements, digitization has speeded up the production of copies and lowered the costs that were one of the key drivers for the industry to perform the transition to digital-based technologies.

[433] *Sieber*, Council of Europe Organised Crime Report 2004, page 148.

[434] Digital Rights Management describes access control technology used to limit the usage of digital media. For further information, see: *Cunard/Hill/Barlas*, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf; *Baesler*, Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf.

[435] Peer-to-Peer (P2P) describes direct connectivity between participants in networks instead of communicating over conventional centralized server-based structures. See: *Schroder/Fischbach/Schmitt*, Core Concepts in Peer-to-Peer Networking, 2005, available at: www.idea-group.com/downloads/excerpts/Subramanian01.pdf; *Androutsellis-Theotokis/Spinellis*, A Survey of Peer-to-Peer Content Distribution Technologies, 2004, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf.

[436] GAO, File Sharing, Selected Universities Report Taking Action to Reduce Copyright Infringement, available at: www.gao.gov/new.items/d04503.pdf; *Ripeanu/Foster/Iamnitchi*, Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design, available at: http://people.cs.uchicago.edu/~matei/PAPERS/ic.pdf. United States Federal Trade Commission, Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues, page 3, available at: www.ftc.gov/reports/p2p05/050623p2prpt.pdf; *Saroiu/Gummadi,/Gribble*, A Measurement Study of Peer-to-Peer File Sharing Systems, available at: www.cs.washington.edu/homes/gribble/papers/mmcn.pdf.

[437] In 2005, 1.8 million users used Gnutella. See *Mennecke*, eDonkey2000 Nearly Double the Size of FastTrack, available at: www.slyck.com/news.php?story=814.

[438] See: Cisco, Global IP Traffic Forecast and Methodology, 2006-2011, 2007, page 4, available at: www.cisco.com/application/pdf/en/us/guest/netsol/ns537/c654/cdccont_0900aecd806a81aa.pdf.

[439] See: OECD Information Technology Outlook 2004, page 192, available at: www.oecd.org/dataoecd/22/18/37620123.pdf.

[440] One example is Germany, where a regularly updated report of the Federation of the phonographic businesses pointed out that, in 2006, 5.1 million users in Germany downloaded music in file-sharing systems. The report is available at: www.ifpi.de/wirtschaft/brennerstudie2007.pdf. Regarding the United States, see: *Johnson/McGuire/Willey*, Why File-Sharing Networks Are Dangerous, 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf.

[441] Apart from music, videos and software, even sensitive personal documents are often found in file-sharing systems. See: *Johnson/McGuire/Willey*, Why File-Sharing Networks Are Dangerous, 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf.

[442] While in 2002, music files made up more than 60 per cent of all files exchanged in file-sharing systems in OECD countries, this proportion dropped in 2003 to less than 50 per cent. See: OECD Information Technology Outlook 2004, page 192, available at: www.oecd.org/dataoecd/22/18/37620123.pdf.

[443] *Schoder/Fischbach/Schmitt*, Core Concepts in Peer-to-Peer Networking, 2005, page 11, available at: www.idea-group.com/downloads/excerpts/Subramanian01.pdf; *Cope*, Peer-to-Peer Network, Computerworld, 8.4.2002, available at: www.computerworld.com/networkingtopics/networking/story/0,10801,69883,00.html; *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

[444] Regarding Napster and the legal response, see: *Rayburn,* After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html; *Penn*, Copyright Law: Intellectual Property Protection in Cyberspace, Journal of Technology Law and Policy, Vol. 7, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol7/issue2/penn.pdf.

[445] Regarding the underlying technology, see: *Fischer*, The 21st Century Internet: A Digital Copy Machine: Copyright Analysis, Issues, and Possibilities, Virginia Journal of Law and Technology, Vol. 7, 2002, available at: www.vjolt.net/vol7/issue3/v7i3_a07-Fisher.pdf; *Sifferd*, The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology, Vanderbilt Journal of Entertainment Law & Practice, 2002, 4, 93; *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Herndon*, Who's watching the kids? – The use of peer-to-peer programs to Cyberstalk children, Oklahoma Journal of Law and Technology, Vol. 12, 2004, available at: www.okjolt.org/pdf/2004okjoltrev12.pdf; *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

[446] For more information on investigations in peer-to-peer networks, see: Investigations Involving the Internet and Computer Networks, NIJ Special Report, 2007, page 49 *et seq.*, available at: www.ncjrs.gov/pdffiles1/nij/210798.pdf.

[447] *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Desing, 2005.

[448] Regarding the motivation of users of peer-to-peer technology, see: *Belzley*, Grokster and Efficiency in Music, Virginia Journal of Law and Technology, Vol. 10, Issue 10, 2005, available at: www.vjolt.net/vol10/issue4/v10i4_a10-Belzley.pdf.

[449] For more examples, see: Supreme Court of the United States, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd, I. B., available at: http://fairuse.stanford.edu/MGM_v_Grokster.pdf.

[450] Regarding the economic impact, see: *Liebowitz*, File-Sharing: Creative Destruction or Just Plain Destruction, Journal of Law and Economics, 2006, Vol. 49, page 1 *et seq.*

[451] The latest analysis regarding file-sharing activities in Germany identify up to 7.3 million users who download music files from the Internet. Up to 80 per cent of these downloads are related to file-sharing systems. Source: GfK, Brennerstudie 2005.

[452] The Recording Industry 2006 Privacy Report, page 4, available at: www.ifpi.org/content/library/piracy-report2006.pdf.

[453] One example is the movie "Star Wars – Episode 3" that appeared in file-sharing systems hours before the official premiere. See: www.heise.de/newsticker/meldung/59762 drawing on a MPAA press release.

[454] Regarding anonymous file-sharing systems, see: *Wiley/ Hong*, Freenet: A distributed anonymous information storage and retrieval system, in Proceedings of the ICSI Workshop on Design Issues in Anonymity and Unobservability, 2000.

[455] Content scrambling systems (CSS) is a digital rights management system that is used is most DVD video discs. For details about the encryption used, see: *Stevenson*, Cryptanalysis of Contents Scrambling System, available at: www.dvd-copy.com/news/cryptanalysis_of_contents_scrambling_system.htm.

[456] Regarding further responses of the entertainment industry (especially lawsuits against Internet users), see: *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

[457] Digital rights management describes access control technology used to limit the usage of digital media. For more information, see: *Cunard/Hill/Barlas*, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

[458] *Bloom/Cox/Kalker/Linnartz/Miller/Traw*, Copy Protection for DVD Videos, IV 2, available at: www.adastral.ucl.ac.uk/~icox/papers/1999/ProcIEEE1999b.pdf.

[459] *Siebel*, Council of Europe Organised Crime Report 2004, page 152.

[460] See: www.golem.de/0112/17243.html.

[461] Regarding the similar discussion with regard to tools used to design viruses, see below: § 2.8.4.

[462] See *Bakke*, Unauthorized use of Another's Trademark on the Internet, UCLA Journal of Law and Technology Vol. 7, Issue 1; Regarding trademark violations as a consequence of online-criticism, see: *Prince*, Cyber-Criticism and the Federal Trademark Dilution act: Redefining the Noncommercial use Exemption, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue4/v9i4_a12-Prince.pdf.

[463] The term "phishing" describes an act that is carried out to make targets disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph." linked to popular hacker naming conventions. See *Gecko*, The criminalization of Phishing and Identity Theft, Computer und Resht, 2005, 606; *Ullman*, "The Phishing Guide: Understanding & Preventing Phishing Attacks", available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information, see below: § 2.9.4.

[464] For an overview about what phishing mails and the related spoofing websites look like, see: www.antiphishing.org/phishing_archive/phishing_archive.html.

[465] Regarding the connection with trademark-related offences, see for example: Explanatory Report to the Convention on Cybercrime, No. 42.

[466] Another term used to describe the phenomenon is "domain grabbing". Regarding cybersquatting, see: *Hansen-Young*, Whose Name is it, Anyway? Protecting Tribal Names from cybersquatters, Virginia Journal of Law and Technology, Vol. 10, Issue 6; *Binomial*, Cyberspace Technological Standardization: An Institutional Theory Retrospective, Berkeley Technology Law Journal, Vol. 18, page 1259 *et seq.*; *Struve/Wagner*, Real space Sovereignty in Cyberspace: Problems with the Ant cybersquatting Consumer Protection Act, Berkeley Technology Law Journal, Vol. 17, page 988 *et seq.*; *Travis*, The Battle for Mindshare: The Emerging Consensus that the First Amendment Protects Corporate Criticism and Parody on the Internet, Virginia Journal of Law and Technology, Vol. 10, Issue 3, 2003.

[467] See: *Lipton*, Beyond cybersquatting: taking domain name disputes past trademark policy, 2005, available at: www.law.wfu.edu/prebuilt/w08-lipton.pdf.

[468] This happens especially with the introduction of new top-level-domains. To avoid cybersquatting, the introduction of a new first-level domain is often accompanied by a period where only parties with trademarks can register a domain name. At the end of this phase (often called the "sunrise period"), other users can register their domain.

[469] For case examples, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 112.

[470] For case examples, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 113.

[471] In 2006, the United States Federal Trade Commission received nearly 205 000 Internet-related fraud complaints. See Consumer Fraud and Identity Theft Complaint Data, January – December 2006, Federal Trade Commission, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

[472] Regarding the related challenges, see below.

[473] In 2006, Nearly 50 per cent of all fraud complaints reported to the United States Federal Trade Commission were related to amounts paid between 0-25 US Dollars See Consumer Fraud and Identity Theft Complaint Data, January – December 2006, Federal Trade Commission, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

[474] Regarding the related automation process: § 3.2.8.

[475] The term "advance fee fraud" describes offences in which offenders seek to convince targets to advance a small sum of money in the hope of receiving a much larger sum afterwards. For more information, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 1; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, Trends & Issues in Crime and Criminal Justice, No. 121, available at: www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, Advance fee fraud on the Internet: Nigeria's regulatory response, Computer Law & Security Report, Vol. 21, Issue 3, 237.

[476] For more information, see below: § 6.2.14.

[477] The term auction fraud describes fraudulent activities involving electronic auction platforms over the Internet. Regarding auction fraud, see: *Bywell/Oppenheim*, Fraud on Internet Auctions, Aslib Proceedings, 53 (7), page 265 *et seq.*, available at: www.aslib.co.uk/proceedings/protected/2001/jul-aug/03.pdf; *Snyder*, Online Auction Fraud: Are the Auction Houses Doing All They Should or Could to Stop Online Fraud, Federal Communications Law Journal, 52 (2), page 453 *et seq.*; *Chau/Falooutsos*, Fraud Detection in Electronic Auction, available at: www.cs.cmu.edu/~dchau/papers/chau_fraud_detection.pdf; *Dolan*, Internet Auction Fraud: The Silent Victims, Journal of Economic Crime Management, Vol. 2, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/BA2DF0D2-D6ED-10C7-9CCB88D5834EC498.pdf.

[478] See www.ebay.com.

[479] See *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1.

[480] The United States Internet Crime Complaint Centre (IC3) (a partnership between the FBI and the National White Collar Crime Centre) reported that around 45 per cent of complaints refer to Auction Fraud. See: IC3 Internet Crime Report 2006, available at: www.ic3.gov/media/annualreport/2006_IC3Report.pdf.

[481] Law Enforcement Efforts to combat Internet Auction Fraud, Federal Trade Commission, 2000, page 1, available at: www.ftc.gov/bcp/reports/int-auction.pdf.

[482] See: *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 7, available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

[483] For more information, see for example: http://pages.ebay.com/help/feedback/feedback.html.

[484] Regarding the criminalization of "account takeovers", see: *Gercke*, Multimedia und Recht 2004, issue 5, page XIV.

[485] See Putting an End to Account-Hijacking Identity Theft, Federal Deposit Insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

[486] The term "advance fee fraud" describes offences in which offenders seek to convince targets to advance a small sum of money in the hope of receiving a much larger sum afterwards. For more information, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 1; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, Trends & Issues in Crime and Criminal Justice, No. 121, available at: www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, Advance fee fraud on the Internet: Nigeria's regulatory response,

Computer Law & Security Report, Vol. 21, Issue 3, 237; *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 7, available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

487 Advance Fee Fraud, Foreign & Commonwealth Office, available at: www.fco.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1044901630595.

488 For an overview of estimated losses, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 3 *et seq.*

489 For more information, see: the Ultrascan Survey "419 Advance Fee Fraud", version 1.7, 19.02.2008, available at: www.ultrascan.nl/assets/applets/2007_Stats_on_419_AFF_feb_19_2008_version_1.7.pdf.

490 See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 39, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

491 Regarding phishing, see: *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, 2006, available at: www.usdoj.gov/opa/report_on_phishing.pdf.

492 The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Computer und REcht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

493 "Phishing" scams show a number of similarities to spam e-mails. It is likely that those organized crime groups that are involved in spam are also involved in phishing scams, as they have access to spam databases. Regarding spam, see above: § 2.6.7.

494 Regarding related trademark violations, see above: § 2.7.2.

495 For more information about phishing scams, see below: § 2.9.4.

496 One technical solution to ensure the integrity of data is the use of digital signatures.

497 For case studies, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 94.

498 *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 39, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. Regarding the different definitions of identity theft, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

499 One of the classic examples is the search for personal or secret information in trash or garbage bins ("dumpster diving"). For more information about the relation to identity theft, see: Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

500 Javelin Strategy & Research 2006 Identity Fraud Survey points out that although there were concerns over electronic methods of obtaining information, most thieves still obtain personal information through traditional rather than electronic channels. In the cases where the methods were known, less than 15 per cent obtained online by electronic means. See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys, see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

501 See for example: *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006; *Stone*, U.S. Congress looks at identity theft, International Herald Tribune, 22.03.2007.

502 See for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

[503] See for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006; *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, MMR 2007, 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000.

[504] *Hoar*, Identity Theft: The Crime of the New Millennium, Oregon Law Review, Vol. 80, 2001, page 1421 *et seq.*; *Levi*, Suite Revenge? The Shaping of Folk Devils and Moral Panics about White-Collar Crimes, British Journal of Criminology, 2008, page 8.

[505] See: Discussion Paper Identity Crime, Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, Australia, 2007, page 5.

[506] See *Goodrich*, Identity Theft Awareness in North Central West Virginia, Marshall University, 2003, page 1.

[507] Identity Fraud, Prevalence and Links to Alien Illegal Activities, GAO, 2002, GAO-02-830T, page 6; *Paget,* Identity Theft, McAfee White Paper, 2007, page 6. For an overview of Internet-related phishing, see: *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, ITTC Report on Online Identity Theft Technology and Countermeasures, 2005, page 8 *et seq.*

[508] *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, Crime Law Soc Change, Vol. 46, page 270.

[509] Unlike in the industrial society, members of the information society are no longer connected by their participation in industrialization, but through their access to and the use of ICTs. For more information on the information society, see: *Masuda*, The Information Society as Post-Industrial Society; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; *Hornby/Clarke*, Challenge and Change in the Information Society.

[510] *Clarke*, Technology, Criminology and Crime Science, European Journal on Criminal Policy and Research, Vol. 10, 2004, page 55; Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, 1998, GAO Document: GAO/GGD-98-100BR, page 51.

[511] 2008 Identity Fraud Survey Report, Consumer Version, Javelin Strategy & Research, 200 page 5.

[512] 35 per cent of the overall number of cases.

[513] 2008 Identity Fraud Survey Report, Consumer Version, Javelin Strategy & Research, 200 page 6.

[514] Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, Statement of G. C. Wilshusen, Director, Information Security Issues, 2007, GAO Document: GAO-07_935T, page 4.

[515] *Elston/Stein*, International Cooperation in On-Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, available at: www.isrcl.org/Papers/Elston%20and%20Stein.pdf.

[516] See *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 2006, page 555.

[517] *Ceaton*, The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web, Bulletin of Science Technology Society, 2007, Vol. 27, 2008, page 20.

[518] See Encyclopaedia Britannica 2007.

[519] *Halperin*, Identity as an Emerging Field of Study, Datenschutz und Datensicherheit, 2006, 533.

[520] *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf; For an approach to divide between four phases, see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[521] In some cases perpetrators used the data they obtained to hide their real identity. Regarding this aspect, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

[522] *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

[523] See: 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2, available at: www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf.

[524] Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[525] Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[526] Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

[527] This method is not considered as an Internet-related approach.

[528] For more information, see: *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, 2006.

[529] See: *Nogguchi*, Search engines lift cover of privacy, The Washington Post, 09.02.2004, available at: www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

[530] See: Congress of the United States, Committee on Oversight and Government Reform, 17.10.2007, available at: http://oversight.house.gov/documents/20071017134802.pdf.

[531] The CSI Computer Crime and Security Survey 2007 analysed among other issues the economic impact of cybercrime businesses. It is based on the responses of 494 computer security practitioners from in US corporations, government agencies and financial institutions. The survey is available at: www.gocsi.com/

[532] See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

[533] For more details, see: *Gercke*, Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, Document No: E/CN.15/2009/CRP.13, page 8 *et seq.*

[534] *Garfinkel*, Database nation: The Death of privacy in the 21st Century, 2000, page 33-34; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350.

[535] See *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm.

[536] *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, 2005, page 6; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm.

[537] Examples is the online community Facebook, available at www.facebook.com.

[538] See for example Art. 5 of the Directive 2000/31/Ec Of The European Parliament And Of The Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

[539] Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

[540] Regarding forensic analysis of e-mail communication, see: *Gupta*, Digital Forensic Analysis of E-mail: A Trusted E-mail Protocol, International Journal of Digital Evidence, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

[541] Identity Theft, Prevalence and Cost Appear to be Growing, GAO-02-363.

[542] United States Bureau of Justice Statistics, 2004, available at www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf.

[543] See Identity Theft: Do you know the signs?, The Fraud Advisory Panel, page 1, available at: www.fraudadvisorypanel.org/newsite/PDFs/advice/Identity%20Theft%20Final%20Proof%2011-7-03.pdf.

[544] *Paget*, Identity Theft – McAfee White Paper, page 10, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

[545] See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf.

[546] See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* Identity Theft – A discussion paper, 2004, page 5, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[547] The United States Federal Bureau of Investigation (FBI) requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. The Head of the FBI office in New York is quoted as saying: "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack". See: Heise News, available at: www.heise-security.co.uk/news/80152.

[548] See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* Identity Theft – A discussion paper, 2004, page 5, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[549] The availability of tools to commit cybercrime is one of the key challenges in the fight against cybercrime. For more information, see below: § 3.2.3.

[550] Websense Security Trends Report 2004, page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

[551] For an overview about the tools used, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf. Regarding the price of keyloggers (USD 200-500), see: *Paget*, Identity Theft, White Paper, McAfee, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

[552] See above: § 2.5.1.

[553] For more examples, see: The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, page 23 *et seq.*, available at: www.antiphishing.org/reports/APWG_CrimewareReport.pdf; *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law-enforcement agencies, Michigan Law Journal 2007, page 21, available at: www.michbar.org/journal/pdf/pdf4article1163.pdf.

[554] DoS is an acronym for denial-of-service attack. For more information, see above: § 2.5.5.

[555] These generally contain two elements: Software that automates the process of sending out e-mails by avoiding techniques that enable e-mail providers to identify spam e-mails and a database with thousands or even millions of e-mail addresses. For more information, see: "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", page 25, available at: www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

[556] For more details, see below: § 6.2.14.

[557] *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*

[558] *Rollins/Wilson*, Terrorist Capabilities for Cyberattack, 2007, page 10, available at: www.fas.org/sgp/crs/terror/RL33123.pdf.

[559] The CIA pointed out in 2002 that attacks against critical infrastructure in the United States will become an option for terrorists. Regarding the CIA position, see: *Rollins/Wilson*, Terrorist Capabilities for Cyberattack, 2007, page 13, available at: www.fas.org/sgp/crs/terror/RL33123.pdf. However, the FBI has stated that there is presently a lack of capability to mount a significant cyberterrorism campaign. Regarding the FBI position, see: *Nordeste/Carment*, A Framework for Understanding Terrorist Use of the Internet, 2006, available at: www.csis-scrs.gc.ca/en/itac/itacdocs/2006-2.asp.

[560] See: Report of the National Security Telecommunications Advisory Committee – Information Assurance Task Force – Electric Power Risk Assessment, available at: www.aci.net/kalliste/electric.htm.

[561] See: *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, Cyber-terrorism and Cybersecurity; www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*; *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in Arquilla/Ronfeldt, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, Cyberterrorism, Are We Under

Siege?, American Behavioral Scientist, Vol. 45 page 1033 et seq.; United States Department of State, Pattern of Global Terrorism, 2000, in: Prados, America Confronts Terrorism, 2002, 111 *et seq.*; *Lake*, 6 Nightmares, 2000, page 33 *et seq.*; *Gordon*, Cyberterrorism, available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; US-National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, 2003, page 11 *et seq.*; OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

562 See: *Roetzer*, Telepolis News, 4.11.2001, available at: www.heise.de/tp/r4/artikel/9/9717/1.html.

563 The text of the final message was reported to be: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." The name of the faculties was apparently the code for different targets. For more detail, see: *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, Al Qaeda and the Internet: The danger of "cyberplanning", 2003, available at: http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; *Zeller*, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, available at: www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position ;

564 CNN, News, 04.08.2004, available at: www.cnn.com/2004/US/08/03/terror.threat/index.html.

565 For an overview, see: *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*

566 *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf.

567 Regarding different international approaches as well as national solutions, see: *Sieber* in Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007.

568 One example for such approach is the amendment of the European Union Framework Decision on combating terrorism, COM(2007) 650.

569 Regarding attacks via the Internet: *Arquilla/Ronfeldt*, in The Future of Terror, Crime and Militancy, 2001, page 12; *Vatis* in Cyberattacks During the War on Terrorism, page 14ff.; *Clark*, Computer Security Officials Discount Chances of "Digital Pearl Harbour", 2003; USIP Report, Cyberterrorism, How real is the threat, 2004, page 2; *Lewis*, Assessing the Risks of Cyberterrorism, Cyberwar and Other Cyberthreats; *Wilson* in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003.

570 See, for example: *Record*, Bounding the global war on terrorism, 2003, available at: http://strategicstudiesinstitute.army.mil/pdffiles/PUB207.pdf.

571 *Wilson* in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003, page 4.

572 ADL, Terrorism Update 1998, available at: www.adl.org/terror/focus/16_focus_a.asp.

573 *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 3. Regarding the use of the Internet for propaganda purposes, see also: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

574 Regarding the use of YouTube by terrorist organizations, see: Heise News, news from 11.10.2006, available at: www.heise.de/newsticker/meldung/79311; *Staud* in Sueddeutsche Zeitung, 05.10.2006.

575 *Zanini/Edwards*, The Networking of Terror in the Information Age, in Networks and Netwars: The Future of Terror, Crime, and Militancy, 2001, page 42.

576 United States Homeland Security Advisory Council, Report of the Future of Terrorism, 2007, page 4.

577 Regarding the justification, see: *Brandon,* Virtual Caliphate: Islamic extremists and the internet, 2008, available at: www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf.

578 *Brachman*, High-Tech Terror: Al-Qaeda's Use of New Technology, The Fletcher Forum of World Affairs, Vol. 30:2, 2006, page 149 *et seq.*

579 See: *Conway*, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006, page 16.

580 Videos showing the execution of American citizens Berg and Pearl were made available on websites. See *Weimann* in the USIP Report: How Terrorists use the Internet, 2004, page 5.

[581] Regarding the related challenges, see: *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, page 292.

[582] *Levine*, Global Security, 27.06.2006, available at: www.globalsecurity.org/org/news/2006/060627-google-earth.htm. Regarding the discovery of a secret submarine on a satellite picture provided by a free-of-charge Internet service, see: Der Standard Online, Google Earth: Neues chinesisches Kampf-Uboot entdeckt, 11.07.2007, available at: www.derstandard.at/?url/?id=2952935.

[583] For further reference, see: *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, 292.

[584] For more information regarding the search for secret information with the help of search engines, see: *Long, Skoudis, van Eijkelenborg*, Google Hacking for Penetration Testers.

[585] "Using public sources openly and without resorting to illegal means, it is possible to gather at least eighty per cent of information about the enemy." For further information, see: *Conway*, Terrorist Use of the Internet and Fighting Back, Information & Security, 2006, page 17.

[586] See *Broad*, US Analysts Had flagged Atomic Data on Web Site, New York Times, 04.11.2006.

[587] *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 18.

[588] See Sueddeutsche Zeitung Online, BKA findet Anleitung zum Sprengsatzbau, 07.03.2007, available at: www.sueddeutsche.de/deutschland/artikel/766/104662/print.html.

[589] See US Commission on Security and Cooperation in Europe Briefing, 15.05.2008, available at: http://csce.gov/index.cfm?FuseAction=ContentRecords.ViewTranscript&ContentRecord_id=426&ContentType=H,B&ContentRecordType=B&CFID=18849146&CFTOKEN=53; *O'Brian*, Virtual Terrorists, The Australian, 31.07.2007, available at: www.theaustralian.news.com.au/story/0,25197,22161037-28737,00.html; *O'Hear*, Second Life a terrorist camp?, ZDNet.

[590] Regarding other terrorist related activities in online games, see: *Chen/Thoms*, Cyberextremism in Web 2.0 – An Exploratory Study of International Jihadist Groups, Intelligence and Security Informatics, 2008, page 98 *et seq.*

[591] *Brunst i*n Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; United States Homeland Security Advisory Council, Report of the Future of Terrorism Task Force, January 2008, page 5; *Stenersen*, The Internet: A Virtual Training Camp?, in Terrorism and Political Violence, 2008, page 215 *et seq.*

[592] *Musharbash*, Bin Ladens Intranet, Der Spiegel, Vol. 39, 2008, page 127.

[593] *Weimann*, How Modern Terrorism uses the Internet, 116 Special Report of the United States Institute of Peace, 2004, page 10.

[594] The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, 2007, page 249.

[595] The text of the final message was reported to be: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." The name of the faculties was apparently the code for different targets. For more detail, see: *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, Al Qaeda and the Internet: The danger of "cyberplanning", 2003, available at: http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; Zeller, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, available at: www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position.

[596] The Commission analysing the 9/11 attacks calculated that the costs for the attack could have been between USD 400 000 and 500 000. See 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, page 187. Taking into account the duration of the preparation and the number of people involved, the cost per person was relatively small. Regarding the related challenges, see also: *Weiss*, CRS Report for Congress, Terrorist Financing: The 9/11 Commission Recommendation, page 4.

[597] See in this context: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

[598] *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 7.

[599] See *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 4.

[600] Regarding virtual currencies, see: *Woda*, Money Laundering Techniques with Electronic Payment Systems in Information and Security 2006, page 39.

[601] *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[602] *Lewis*, Assessing the Risks of Cyberterrorism, Cyberwar and Other Cyberthreats, Center for Strategic and International Studies, December 2002.

[603] *Shimeall/Williams/Dunlevy*, Countering cyberwar, NATO review, Winter 2001/2002, available at: www.cert.org/archive/pdf/counter_cyberwar.pdf.

[604] *Gercke*, The slow wake of a global approach against cybercrime, Computer und Recht International, 2006, page 140 *et seq.*

[605] *Gercke*, The Challenge of fighting Cybercrime, Multimedia und Recht, 2008, page 293.

[606] CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

[607] Law Enforcement Tools and Technologies for Investigating Cyberattacks, DAP Analysis Report 2004, available at: www.ists.dartmouth.edu/projects/archives/ISTSGapAnalysis2004.pdf.

[608] *Brunst i*n Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007.

[609] United States Executive Order 13010 – *Critical Infrastructure Protection*. Federal Register, July 17, 1996. Vol. 61, No. 138.

[610] Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve, GAO communication, July 2007, available at: www.gao.gov/new.items/d07706r.pdf.

[611] Regarding the discovery and functions of the computer virus, see: *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.31, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[612] *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

[613] *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

[614] Cybersecurity Communique, American Gas Association, 2010, available at: www.aga.org/membercenter/gotocommitteepages/NGS/Documents/1011StuxnetMalware.pdf.

[615] *Falliere/Murchu/Chien*, W32.Stuxnet Dossier, Symantec, November 2010, page 1; *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.31, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

[616] *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

[617] Symantec W32.Stuxnet Threat and Risk Summary, available at: www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

[618] *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1; Symantec W32.Stuxnet Threat and Risk Summary, available at: www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

[619] See for example: *Leyden*, Lame Stuxnet Worm: "Full of Errors" says Security Consultant, The Register, 19.02.2011.

[620] *Albright/Brannan/Walrond*, Did Stuxnet Take Out 1.000 Centrifuges at the Natanz Enrichment Plant?, Institute for Science and International Security, 22.12.2010; *Broad/Markoff/Sanger*, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, The New York Times, 15.01.2011; *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 2; *Timmerman*, Computer Worm Shuts Down Iranian Centrifuge Plant, Newsmax, 29.11.2010.

[621] *Kelemen*, Latest Information Technology Development in the Airline Industry, 2002, Periodicapolytechnica Ser. Transp. Eng., Vol. 31, No. 1-2, page 45-52, available at: www.pp.bme.hu/tr/2003_1/pdf/tr2003_1_03.pdf; *Merten/Teufel*,

Technological Innovations in the Passenger Process of the Airline Industry: A Hypotheses Generating Explorative Study in O'Conner/Hoepken/Gretzel, Information and Communication Technologies in Tourism 2008.

622 Sasser B Worm, Symantec Quick reference guide, 2004, available at: http://eval.symantec.com/mktginfo/enterprise/other_resources/sasser_quick_reference_guide_05-2004.en-us.pdf.

623 *Schperberg*, Cybercrime: Incident Response and Digital Forensics, 2005; The Sasser Event: History and Implications, Trend Micro, June 2004, available at: http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/wp02sasserevent040812us.pdf.

624 *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP, 1997; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

625 *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence? available at: www.projects.ncassr.org/hackback/ethics00.pdf.

626 *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNet News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html.

627 *Gercke*, The Decision of the District Court of Frankfurt in the Lufthansa Denial of Service Case, Multimedia und Recht, 2005, page 868-869.

628 Improving our Ability to Fight Cybercrime: Oversight of the National Infrastructure Protection Center, Hearing before the Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary United States Senate One Hundred Seventh Congress First Session, July 2001, Serial No. J–107–22, available at: http://cipp.gmu.edu/archive/215_S107FightCyberCrimeNICPhearings.pdf.

629 Critical Infrastructure Protection, Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain, September 2007, GAO-07-1036, available at: www.gao.gov/new.items/d071036.pdf; *Berinato*, Cybersecurity – The Truth About Cyberterrorism, March 2002, available at: www.cio.com/article/print/30933.

630 Regarding the Stuxnet software, see: *Albright/Brannan/Waldrond*, Did Stuxnet Take out 1.000 Centrifuges at the Nataz Enrichment Plant? Preliminary Assessment, Institute for Science and International Security, 2010.

631 *Wilson*, Information Operations and Cyberwar, Capabilities and related Policy Issues, CRS Report for Congress, RL21787, 2006; *Aldrich*, The International Legal Implications of Information Warfare, INSS Occasional Paper 9, 1996.

632 *Aldrich*, The International Legal Implications of Information Warfare, INSS Occasional Paper 9, 1996.

633 *Schwartau*, Information Warfare: Chaos on the Electronic Superhighway, 1994, page 13.

634 *Sharma*, Cyberwars, A Paradigm Shift from Means to Ends, COEP, 2010.

635 Regarding the beginning discussion about Cyberwarfare, see: *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996, available at: www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

636 *Sharma*, Cyberwars, A Paradigm Shift from Means to Ends, COEP, 2010.

637 *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996, page 15, available at: www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

638 *Libicki*, Sub Rosa Cyberwar, COEP, 2010.

639 *Myers*, Estonia removes Soviet-era war memorial after a night of violence, The New York Times, 27.04.2007; Estonia removes Soviet memorial, BBC News, 27.04.2007; *Tanner*, Violence continues over Estonia's removal of Soviet war statue, The Boston Globe, 28.04.2007.

640 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18 *et seq.*; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 8 *et seq.*

641 *Peter*, Cyberassaults on Estonia Typify a New Battle Tactic, Washington Post, 19.05.2007.

642 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 20; *Toth*, Estonia under cyberattack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

[643] Regarding the attack, see: *Toth*, Estonia under cyberattack, available at: www.cert.hu/dmdocuments/Estonia_attack2.pdf

[644] See: *Waterman*: Analysis: Who cybersmacked Estonia, United Press International 2007, available at: www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/.

[645] See for example: *Landler/Markoff*, Digital Fears Emerge After Data Siege in Estonia, The New York Times, 29.05.2007.

[646] *Shackelford*, From Nuclear War to Net War: Analogizing Cyberattacks in International Law, Berkeley Journal of International Law, Vol. 27, page 193.

[647] *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18-20.

[648] Estonia hit by Moscow cyberwar, BBC News, 17.05.2007; *Traynor*; Russia accused of unleashing cyberwar to disable Estonia, The Guardian, 17.05.2007.

[649] *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 23.

[650] *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18 *et seq.*; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 8 *et seq.*

[651] *Peter*, Cyberassaults on Estonia Typify a New Battle Tactic, Washington Post, 19.05.2007.

[652] *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 20; *Toth*, Estonia under cyberattack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

[653] Regarding the background to the conflict, see: Council of Europe Parliamentary Assembly Resolution 1633 (2008), The consequences of the war between Georgia and Russia.

[654] *Tikk/Kaska/Rünnimeri/Kert/Talihärm/Vihul*, Cyberaattacks Against Georgia: Legal Lessons Identified, 2008, page 4; *Hart*, Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar, Washington Post, 14.08.2008; Cybersecurity and Politically, Socially and Religiously Motivated Cyberattacks, European Union, Policy Department External Policies, 2009, page 15; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 10.

[655] *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 23.

[656] See for example: *Partitt,* Georgian blogger Cyxymu blames Russia for cyberattack, The Guardian, 07.08.2009.

[657] *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 75; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 10.

[658] See *Walker*, Information Warfare and Neutrality, *Vanderbilt Journal of Trans-national Law* 33, 2000; *Banks*, Information War Crimes: Mitnick meets Milosevic, 2001, AU/ACSC/019/2001-04.

[659] *Solce*, The Battlefield of Cyberspace: The inevitable new military branch – the cyberforce, Alb. Law Journal of Science and Technology, Vol. 18, page 315.

[660] *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 61.

[661] One of the most important obligations is the requirement to keep records and to report suspicious transactions.

[662] Offenders may tend to make use of the existing instruments, e.g. the services of financial organizations to transfer cash, without the need to open an account or transfer money to a certain account.

[663] For case studies, see: Financial Action Task Force on Money Laundering, "Report on Money Laundering Typologies 2000-2001", 2001, page 8.

[664] See: *Woda*, Money Laundering Techniques With Electronic Payment Systems, Information & Security, Vol. 18, 2006, page 40.

[665] Regarding the related challenges, see below: § 3.2.I.

[666] Regarding the fundermental concept see: Nakamoto (name reported to be used as alias), Bitcoin: A Peer-to-Peer Electronic Cash System, available at: www.bitcoin.org/bitcoin.pdf.

[667] Regarding the attacks see: Cohen, Speed Bumps on the Road to Virtual Cash, NYT, 3.7.2011, available at: www.nytimes.com/2011/07/04/business/media/04link.html.

[668] Regarding the basic concept of such investigation see: Following the Money 101: A Primer on Money-Trail Investigations, Coalition for International Justice, 2004, available at: www.media.ba/mcsonline/files/shared/prati_pare.pdf.

[669] Regarding approaches to detect and prevent such transfers see: Financial Coalition Against Child Pornography, Report on Trends in Online Crime and Their Potential Implications for the Fight Against Commercial Child Pornography, Feb. 2011, available at: http://www.missingkids.com/en_US/documents/FCACPTrendsInOnlineCrimePaper2011.pdf

[670] The costs of setting up an online casino are not significantly larger than other e-commerce businesses.

[671] Regarding approaches to the criminalization of illegal gambling, see below: § 6.2.12.

[672] See: Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2000-2001, 2001, page 2.

[673] Regarding the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.

[674] Regarding the phenomenon of phishing, see: *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, 2006, available at: www.usdoj.gov/opa/report_on_phishing.pdf.

[675] The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, "The Phishing Guide Understanding & Preventing Phishing Attacks", available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

[676] The following section describes e-mail-based phishing attacks, compared to other phishing scams, which may, for example, be based on voice communications. See: *Gonsalves*, Phishers Snare Victims with VoIP, 2006, available at: www.techweb.com/wire/security/186701001.

[677] "Phishing" shows a number of similarities to spam e-mails. It is thus likely that organized crime groups that are involved in spam are also involved in phishing scams, as they make use of the same spam databases. Regarding spam, see above: § 2.6.7.

[678] Regarding related trademark violations, see above: § 2.7.2.

[679] For an overview of what phishing mails and the related spoofing websites look like, see: www.antiphishing.org/phishing_archive/phishing_archive.html.

[680] In some phishing attacks, as many as 5 per cent of victims provided sensitive information on fake websites. See *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf, page 1, that refers to *Loftesness*, Responding to "Phishing" Attacks, Glenbrook Partners (2004).

[681] Anti-Phishing Working Group. For more details, see: www.antiphishing.org.

[682] Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf.

[683] See above: § 2.8.3.

# 3. The challenges of fighting cybercrime

**Bibliography (selected):** *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Bellare/Rogaway*, Introduction to Modern Cryptography, 2005; *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law enforcement agencies, Michigan Law Journal 2007; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2; *Farid*, Detecting Steganographic Messages in Digital Images, Technical Report TR2001-412, 2001; *Friedrich/Goljan*, Practical Steganalysis of Digital Images, Proceedings of SPIE Photonic West 2002: Electronic Imaging, Security and Watermarking of Multimedia Content IV; *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, page 142; *Gercke*, Use of Traffic Data to trace Cybercrime offenders, DUD 2002, page 477 *et seq.*; *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, page 291 *et seq.*; *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2; *Hick/Halpin/Hoskins*, Human Rights and the Internet, 2000; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19; *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*; *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, page 3, available at: www.cert.org/archive/pdf/Botnets.pdf; *Johnson/Duric/Jajodia*, Information Hiding: Steganography and Watermarking, Attacks and Countermeasures, 2001; *Kahn*, Cryptology goes Public, Foreign Affairs, 1979, Vol. 58; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119; *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Picker*, Cyber Security: Of Heterogeneity and Autarky, available at: http://picker.uchicago. edu/Papers/PickerCyber.200.pdf; *Putnam/Elliott,* International Responses to Cyber Crime, in Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism" 2001; *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf; *Ryan*, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics, Virginia Journal of Law and Technology, Vol. 9, 2004; *Sadowsky/Zambrano/Dandjinou*, Internet Governance: A Discussion Document, 2004; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006; *Thomas*, Al Qaeda and the Internet: The Danger of 'Cyberplanning' Parameters 2003; *Wallsten*, Regulation and Internet Use in Developing Countries, 2002.

Recent developments in ICTs have not only resulted in new cybercrimes and new criminal methods, but also new methods of investigating cybercrime. Advances in ICTs have greatly expanded the abilities of law-enforcement agencies. Conversely, offenders may use new tools to prevent identification and hamper investigation. This chapter focuses on the challenges of fighting cybercrime.

## 3.1 Opportunities

Law-enforcement agencies can now use the increasing power of computer systems and complex forensic software to speed up investigations and automate search procedures.[684]

It can prove difficult to automate investigation processes. While a keyword-based search for illegal content can be carried out easily, the identification of illegal pictures is more problematic. Hash-value based approaches are only successful if pictures have been rated previously, the hash value is stored in a database and the picture that was analysed has not been modified.[685]

Forensic software is able to search automatically for child-pornography images by comparing the files on the hard disk of suspects with information about known images. For example, in late 2007, authorities

found a number of pictures of the sexual abuse of children. In order to prevent identification the offender had digitally modified the part of the pictures showing his face before publishing the pictures over the Internet. Computer forensic experts were able to unpick the modifications and reconstruct the suspect's face.[686] Although the successful investigation clearly demonstrates the potential of computer forensics, this case is no proof of a breakthrough in child-pornography investigation. If the offender had simply covered his face with a white spot, identification would have been impossible.

## 3.2 General challenges

### *3.2.1 Reliance on ICTs*

Many everyday communications depend on ICTs and Internet-based services, including VoIP calls or e-mail communications.[687] ICTs are now responsible for the control and management functions in buildings,[688] cars and aviation services.[689] The supply of energy, water and communication services depend on ICTs. The further integration of ICTs into everyday life is likely to continue.[690] Growing reliance on ICTs makes systems and services more vulnerable to attacks against critical infrastructures.[691] Even short interruptions to services could cause huge financial damages to e-commerce businesses.[692] It is not only civil communications that could be interrupted by attacks; the dependence on ICTs is a major risk for military communications.[693]

Existing technical infrastructure has a number of weaknesses, such as the monoculture or homogeneity of operating systems. Many private users and SMEs use Microsoft's operating system,[694] so offenders can design effective attacks by concentrating on this single target.[695]

The dependence of society on ICTs is not limited to the western countries[696]. Developing countries also face challenges in preventing attacks against their infrastructure and users.[697] The development of cheaper infrastructure technologies such as WiMAX[698] has enabled developing countries to offer Internet services to more people. Developing countries can avoid the mistakes of some western countries, which have concentrated mainly on maximizing accessibility, without investing significantly in protection. US experts have explained that successful attacks against the official website of governmental organizations in Estonia[699] could only take place due to inadequate protection measures.[700] Developing countries have a unique opportunity to integrate security measures early on. This may require greater upfront investments, but the integration of security measures at a later point may prove more expensive in the long run.[701]

Strategies must be formulated to prevent such attacks and develop countermeasures, including the development and promotion of technical means of protection, as well as adequate and sufficient laws enabling law-enforcement agencies to fight cybercrime effectively.[702]

### *3.2.2 Number of users*

The popularity of the Internet and its services is growing fast, with over 2 billion Internet users worldwide by 2010.[703] Computer companies and ISPs are focusing on developing countries with the greatest potential for further growth.[704] In 2005, the number of Internet users in developing countries surpassed the number in industrial nations,[705] while the development of cheap hardware and wireless access will enable even more people to access the Internet.[706]

With the growing number of people connected to the Internet, the number of targets and offenders increases.[707] It is difficult to estimate how many people use the Internet for illegal activities. Even if only 0.1 per cent of users committed crimes, the total number of offenders would be more than one million. Although Internet usage rates are lower in developing countries, promoting cybersecurity is not easier, as offenders can commit offences from around the world.[708]

The increasing number of Internet users causes difficulties for the law-enforcement agencies because it is relatively difficult to automate investigation processes. While a keyword-based search for illegal content

can be carried out rather easily, the identification of illegal pictures is more problematic. Hash-value based approaches are for example only successful if the pictures were rated previously, the hash value was stored in a data base, and the picture that was analysed has not been modified.[709]

### 3.2.3 Availability of devices and access

Only basic equipment is needed to commit computer crimes. Committing an offence requires hardware, software and Internet access.

With regard to hardware, the power of computers is growing continuously.[710] There are a number of initiatives to enable people in developing countries to use ICTs more widely.[711] Criminals can commit serious computer crimes with only cheap or second-hand computer technology – knowledge counts for far more than equipment. The date of the computer technology available has little influence on the use of that equipment to commit cybercrimes.

Committing cybercrime can be made easier through specialist software tools. Offenders can download software tools[712] designed to locate open ports or break password protection.[713] Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices.[714]

The last vital element is Internet access. Although the cost of Internet access[715] is higher in most developing countries than in industrialized countries, the number of Internet users in developing countries is growing rapidly.[716] Offenders will generally not subscribe to an Internet service to limit their chances of being identified, but prefer services they can use without (verified) registration. A typical way of getting access to networks is the so-called "wardriving". The term describes the act of driving around searching for accessible wireless networks.[717] The most common methods criminals can use to access the network fairly anonymously are public Internet terminals, open (wireless) networks[718], hacked networks and prepaid services without registration requirements.

Law-enforcement agencies are taking action to restrict uncontrolled access to Internet services to avoid criminal abuse of these services. In Italy and China, for example, the use of public Internet terminals requires the identification of users.[719] However, there are arguments against such identification requirements.[720] Although the restriction of access could prevent crimes and facilitate the investigations of law-enforcement agencies, such legislation could hinder the growth of the information society and the development of e-commerce.[721]

It has been suggested that this limitation on access to the Internet could violate human rights.[722] For example, the European Court has ruled in a number of cases on broadcasting that the right to freedom of expression applies not only to the content of information, but also to the means of transmission or reception. In the case Autronic v. Switzerland,[723] the court held that extensive interpretation is necessary since any restriction imposed on the means necessarily interferes with the right to receive and impart information. If these principles are applied to potential limitations on Internet access, it is possible that such legislative approaches could entail violation of human rights.

### 3.2.4 Availability of information

The Internet has millions of webpages[724] of up-to-date information. Anyone who publishes or maintains a webpage can participate. One example of the success of user-generated platforms is Wikipedia,[725] an online encyclopaedia where anybody can publish.[726]

The success of the Internet also depends on powerful search engines that enable users to search millions of webpages in seconds. This technology can be used for both legitimate and criminal purposes. "Googlehacking" or "Googledorks" describes the use of complex search-engine queries to filter many search results for information on computer security issues. For example, offenders might aim to search for insecure password protection systems.[727] Reports have highlighted the risk of the use of search engines for illegal purposes.[728] An offender who plans an attack can find detailed information on the Internet that explains how to build a bomb using only chemicals available in regular supermarkets.[729] Although information like this was available even before the Internet was developed, it was however,

much more difficult to get access to that information. Today, any Internet user can get access to those instructions.

Criminals can also use search engines to analyse targets.[730] A training manual was found during investigations against members of a terrorist group highlighting how useful the Internet is for gathering information on possible targets.[731] Using search engines, offenders can collect publicly available information (e.g. construction plans from public buildings) that help in their preparations. It has been reported that insurgents attacking British troops in Afghanistan used satellite images from Google Earth.[732]

### 3.2.5 Missing mechanisms of control

All mass communication networks – from phone networks used for voice phone calls to the Internet – need central administration and technical standards to ensure operability. The ongoing discussions about Internet governance suggest that the Internet is no different compared with national and even transnational communication infrastructure.[733] The Internet also needs to be governed by laws, and law-makers and law-enforcement agencies have started to develop legal standards necessitating a certain degree of central control.

The Internet was originally designed as a military network[734] based on a decentralized network architecture that sought to preserve the main functionality intact and in power, even when components of the network were attacked. As a result, the Internet's network infrastructure is resistant to external attempts at control. It was not originally designed to facilitate criminal investigations or to prevent attacks from inside the network.

Today, the Internet is increasingly used for civil services. With the shift from military to civil services, the nature of demand for control instruments has changed. Since the network is based on protocols designed for military purposes, these central control instruments do not exist and it is difficult to implement them retrospectively, without significant redesign of the network. The absence of control instruments makes cybercrime investigations very difficult.[735]

One example of the problems posed by the absence of control instruments is the ability of users to circumvent filter technology[736] using encrypted anonymous communication services.[737] If access providers block certain websites with illegal content (such as child pornography), customers are generally unable to access those websites. But the blocking of illegal content can be avoided, if customers use an anonymous communication server encrypting communications between them and the central server. In this case, providers may be unable to block requests because requests sent as encrypted messages cannot be opened by access providers.

### 3.2.6 International dimensions

Many data transfer processes affect more than one country.[738] The protocols used for Internet data transfers are based on optimal routing if direct links are temporarily blocked.[739] Even where domestic transfer processes within the source country are limited, data can leave the country, be transmitted over routers outside the territory and be redirected back into the country to the final destination.[740] Further, many Internet services are based on services from abroad[741], e.g. host providers may offer webspace for rent in one country based on hardware in another.[742]

If offenders and targets are located in different countries, cybercrime investigations need the cooperation of law-enforcement agencies in all countries affected.[743] National sovereignty does not permit investigations within the territory of different countries without the permission of local authorities.[744] Cybercrime investigations need the support and involvement of authorities in all countries involved.

It is difficult to base cooperation in cybercrime on principles of traditional mutual legal assistance. The formal requirements and time needed to collaborate with foreign law-enforcement agencies often hinder investigations.[745] Investigations often occur in very short time-frames.[746] Data vital for tracing offences are often deleted after only a short time. This short investigation period is problematic, because

traditional mutual legal assistance regime often takes time to organize.[747] The principle of dual criminality[748] also poses difficulties, if the offence is not criminalized in one of the countries involved in the investigation.[749] Offenders may be deliberately including third countries in their attacks in order to make investigation more difficult.[750]

Criminals may deliberately choose targets outside their own country and act from countries with inadequate cybercrime legislation.[751] The harmonization of cybercrime-related laws and international cooperation would help. Two approaches to improve the speed of international cooperation in cybercrime investigations are the G8 24/7 Network[752] and the provisions related to international cooperation in the Council of Europe Convention on Cybercrime.[753]

### 3.2.7 Independence of location and presence at the crime site

Criminals need not be present at the same location as the target. As the location of the criminal can be completely different from the crime site, many cyberoffences are transnational. International cybercrime offences take considerable effort and time. Cybercriminals seek to avoid countries with strong cybercrime legislation.[754]

Preventing "safe havens" is one of the key challenges in the fight against cybercrime.[755] While "safe havens" exist, offenders will use them to hamper investigation. Developing countries that have not yet implemented cybercrime legislation may become vulnerable, as criminals may choose to base themselves in these countries to avoid prosecution. Serious offences affecting victims all over the world may be difficult to stop, due to insufficient legislation in the country where offenders are located. This may lead to pressure on specific countries to pass legislation. One example of this is the "Love Bug" computer worm developed by a suspect in the Philippines in 2000,[756] which infected millions of computers worldwide.[757] Local investigations were hindered by the fact that the development and spreading of malicious software was not at that time adequately criminalized in the Philippines.[758] Another example is Nigeria, which has come under pressure to take action over financial scams distributed by e-mail.

### 3.2.8 Automation

One of the greatest advantages of ICTs is the ability to automate certain processes. Automation has several major consequences: It increases the speed of processes as well as the scale and impact of processes and finally limits the involvement of humans.

Automation reduces the need for cost-intensive manpower, allowing providers to offer services at lower prices.[759] Offenders can use automation to scale up their activities – many millions of unsolicited bulk spam[760] messages can be sent out by automation.[761] Hacking attacks are often also now automated, [762] with as many as 80 million hacking attacks every day[763] due to the use of software tools[764] that can attack thousands of computer systems in hours.[765] By automating processes offenders can gain great profit by designing scams that are based on a high number of offences with a relatively low loss for each victim.[766] The lower the single loss, the higher is the chance that the victim will not report the offence.

Automation of attacks affects developing countries in particular. Due to their limited resources, spam may pose a more serious issue for developing countries than for industrialized countries.[767] The greater numbers of crimes that can be committed through automation pose challenges for law-enforcement agencies worldwide, as they will have to be prepared for many more victims within their jurisdictions.

### 3.2.9 Resources

Modern computer systems that are now coming onto the market are powerful and can be used to extend criminal activities. But it is not just increasing power[768] of single-user computers that poses problems for investigations. Increasing network capacities is also a major issue.

One example is the recent attacks against government websites in Estonia.[769] Analysis of the attacks suggests that they were committed by thousands of computers within a "botnet"[770] or group of compromised computers running programs under external control.[771] In most cases, computers are

infected with malicious software that installs tools allowing perpetrators to take control. Botnets are used to gather information about targets or for high-level attacks.[772]

Over recent years, botnets have become a serious risk for cybersecurity.[773] The size of a botnet can vary, from a few computers to more than a million computers.[774] Current analysis suggests that up to a quarter of all computers connected to the Internet could be infected with software making them part of a botnet.[775] Botnets can be used for various criminal activities, including denial of service attacks,[776] sending out spam,[777] hacking attacks and the exchange of copyright-protected files.

Botnets offer a number of advantages for offenders. They increase both the computer and network capacity of criminals. Using thousands of computer systems, criminals can attack computer systems that would be out of reach with only a few computers to lead the attack.[778] Botnets also make it more difficult to trace the original offender, as the initial traces only lead to the member of the botnets. As criminals control more powerful computer systems and networks, the gap between the capacities of investigating authorities and those under control of criminals is getting wider.

### 3.2.10 Speed of data exchange processes

The transfer of an e-mail between countries takes only a few seconds. This short period of time is one reason for the success of the Internet, as e-mails have eliminated the time for the physical transport of a message. However, this rapid transfer leaves little time for law-enforcement agencies to investigate or collect evidence. Traditional investigations take much longer.[779]

One example is the exchange of child pornography. In the past, pornographic videos were handed over or transported to buyers. Both the handover and transport gave law-enforcement agencies the opportunity to investigate. The main difference between the exchange of child pornography on and off the Internet is transportation. When offenders use the Internet, movies can be exchanged in seconds.

E-mails also demonstrate the importance of immediate response tools that can be used immediately. For tracing and identifying suspects, investigators often need access to data that may be deleted shortly after transfer.[780] A very short response time by the investigative authorities is often vital for a successful investigation. Without adequate legislation and instruments allowing investigators to act immediately and prevent data from being deleted, an effective fight against cybercrime may not be possible.[781]

"Quick freeze procedures"[782] and 24/7 network points[783] are examples of tools that can speed up investigations. Data retention legislation also aims to increase the time available for law-enforcement agencies to carry out investigations. If the data necessary to trace offenders are preserved for a length of time, law-enforcement agencies have a better chance of identifying suspects successfully.

### 3.2.11 Speed of development

The Internet is constantly undergoing development. The creation of a graphical user interface (WWW[784]) marked the start of its dramatic expansion, as previous command-based services were less user-friendly. The creation of the WWW has enabled new applications, as well as new crimes[785]. Law-enforcement agencies are struggling to keep up. Further developments continue, notably with online games and voice over IP (VoIP) communication.

Online games are ever more popular, but it is unclear whether law-enforcement agencies can successfully investigate and prosecute offences committed in this virtual world.[786]

The switch from traditional voice calls to Internet telephony also presents new challenges for law-enforcement agencies. The techniques and routines developed by law-enforcement agencies to intercept classic phone calls do not generally apply to VoIP communications. The interception of traditional voice calls is usually carried out through telecom providers. Applying the same principle to VoIP, law-enforcement agencies would operate through ISPs and service providers supplying VoIP services. However, if the service is based on peer-to-peer technology, service providers may generally be unable to intercept communications, as the relevant data are transferred directly between the communicating partners.[787] Therefore, new techniques are needed.[788]

New hardware devices with network technology are also developing rapidly. The latest home entertainment systems turn TVs into Internet access points, while more recent mobile handsets store data and connect to the Internet via wireless networks.[789] USB (universal serial bus) memory devices with more than 1 GB capacity have been integrated into watches, pens and pocket knives. Law-enforcement agencies need to take these developments into account in their work – it is essential to educate officers involved in cybercrime investigations continuously, so they are up to date with the latest technology and able to identify relevant hardware and any specific devices that need to be seized.

Another challenge is the use of wireless access points. The expansion of wireless Internet access in developing countries is an opportunity, as well as a challenge for law-enforcement agencies.[790] If offenders use wireless access points that do not require registration, it is more challenging for law-enforcement agencies to trace offenders, as investigations lead only to access points.

### 3.2.12 Anonymous communications

Determining the origin of communication is very often a key component of cybercrime investigation. However, the distributed nature of the network[791], as well the availability of certain Internet services, which create uncertainty of origin, make it difficult to identify offenders.[792] The possibility of anonymous communication can be either just a by-product of a service or offered with the intention of avoiding disadvantages for the user. Being mindful of uncertainty of origin is crucial to prevent incorrect conclusions.[793] Examples of such services – which can even be combined – are:

- public Internet terminals (e.g. at airport terminals or Internet cafés);[794]
- network address translation (NAT) devices and virtual private networks (VPN);[795]
- wireless networks;[796]
- prepaid mobile services that do not need registration;
- storage capacities for homepages offered without registration;
- anonymous communication servers;[797]
- anonymous remailers.[798]

Offenders can hide their identities through, for example, the use of fake e-mail addresses.[799] Many providers offer free e-mail addresses. Where personal information has to be entered, it may not be verified, so users can register e-mail addresses without revealing their identity. Anonymous e-mail addresses can be useful e.g. if users wish to join political discussion groups without identification. Anonymous communications may give rise to anti-social behaviour, but they can also allow users to act more freely.[800]

Given that users leave various traces, there is a need for instruments to protect them from profiling activities.[801] Therefore, various states and organizations support the principle of anonymous use of Internet e-mail services. This principle is expressed, for instance, in the European Union Directive on Privacy and Electronic Communications.[802] One example of a legal approach to protect user privacy can be found in Article 37 of the European Union Regulation on Data Protection.[803] However, some countries are addressing the challenges of anonymous communications by implementing legal restrictions.[804] Italy, for instance, requires public Internet access providers to identify users before they start using the service.[805]

These measures aim to help law-enforcement agencies identify suspects, but they can be easily avoided. Criminals may use unprotected private wireless networks or SIM-cards from countries not requiring registration. It is unclear whether the restriction of anonymous communications and anonymous access to the Internet should play a more important role in cybersecurity strategies.[806]

### 3.2.13 Failure of traditional investigation instruments

Investigating and prosecuting cybercrime requires Internet-specific tools and instruments that enable competent authorities to carry out investigations.[807] In this context, instruments to identify the offender

and collect the evidence required for the criminal proceedings are essential.[808] These instruments may be the same as those used in traditional terrorist investigations unrelated to computer technology. But in a growing number of Internet-related cases, traditional investigation instruments are not sufficient to identify an offender. One example is the interception of voice-over-IP (VoIP) communication.[809] In recent decades, states have developed investigation instruments, such as wiretapping, that enable them to intercept landline as well as mobile-phone communications.[810] The interception of traditional voice calls is usually carried out through telecom providers.[811] Applying the same principle to VoIP, law-enforcement agencies would operate through Internet service providers (ISPs) and service providers supplying VoIP services. However, if the service is based on peer-to-peer technology, service providers may generally be unable to intercept communications, as the relevant data is transferred directly between the communicating partners.[812] Therefore, new technical solutions together with related legal instruments are necessary.

### 3.2.14 Encryption technology

Another factor that can complicate the investigation of cybercrime is encryption technology,[813] which protects information from access by unauthorized people and is a key technical solution in the fight against cybercrime.[814] Encryption is a technique of turning a plain text into an obscured format by using an algorithm.[815] Like anonymity, encryption is not new,[816] but computer technology has transformed the field. For a long time it was subject to secrecy. In an interconnected environment, such secrecy is difficult to maintain.[817]

The widespread availability of easy-to-use software tools and the integration of encryption technology in the operating systems[818] now makes it possible to encrypt computer data with the click of a mouse and thereby increases the chance of law-enforcement agencies being confronted with encrypted material.[819] Various software products are available that enable users to protect files against unauthorized access.[820] But it is uncertain to what extent offenders already use encryption technology to mask their activities.[821] One survey on child pornography suggested that only 6 per cent of arrested child-pornography possessors used encryption technology[822], but experts highlight the threat of an increasing use of encryption technology in cybercrime cases.[823]

There are different technical strategies to cover encrypted data and several software tools are available to automate these processes.[824] Strategies range from analysing[825] weakness in the software tools used to encrypt files,[826] searching for encryption passphrases[827] and trying typical passwords, to complex and lengthy brute-force attacks. The term “brute-force attack” is used to describe the process of identifying a code by testing every possible combination.[828] Depending on encryption technique and key size, this process could take decades.[829] For example, if an offender uses encryption software with a 20-bit encryption, the size of the keyspace is around one million. Using a current computer processing one million operations per second, the encryption could be broken in less than one second. However, if offenders use a 40-bit encryption, it could take up to two weeks to break the encryption.[830] In 2002, the Wall Street Journal was for example able to successfully decrypt files found on an Al Qaeda computer that were encrypted with 40-bit encryption.[831] Using a 56-bit encryption, a single computer would take up to 2 285 years to break the encryption. If offenders use a 128-bit encryption, a billion computer systems operating solely on the encryption could take thousands of billions years to break it.[832] The latest version of the popular encryption software PGP permits 1 024-bit encryption.

Current encryption software goes far beyond the encryption of single files. The latest version of Microsoft’s operating systems, for example, allows the encryption of an entire hard disk.[833] Users can easily install encryption software. Although some computer forensic experts believe that this function does not threaten them,[834] the widespread availability of this technology for any user could result in greater use of encryption. Tools are also available to encrypt communications – for example, e-mails and phone calls[835] – that can be sent using VoIP.[836] Using encrypted VoIP technology, offenders can protect voice conversations from interception.[837]

Techniques can also be combined. Using software tools, offenders can encrypt messages and exchange them in pictures or images – this technology is called steganography.[838] For investigative authorities, it is

difficult to distinguish the harmless exchange of holiday pictures and the exchange of pictures with encrypted hidden messages.[839]

The availability and use of encryption technologies by criminals is a challenge for law-enforcement agencies. Various legal approaches to address the problem are currently under discussion,[840] including: potential obligations for software developers to install a back-door for law-enforcement agencies; limitations on key strength; and obligations to disclose keys, in the case of criminal investigations.[841] But encryption technology is not only used by offenders – there are various ways such technology is used for legal purposes. Without adequate access to encryption technology, it may be difficult to protect sensitive information. Given the growing number of attacks,[842] self-protection is an important element of cybersecurity.

### *3.2.15 Summary*

The investigation and prosecution of cybercrime presents a number of challenges for law-enforcement agencies. It is vital not only to educate the people involved in the fight against cybercrime, but also to draft adequate and effective legislation. This section has reviewed key challenges to promoting cybersecurity and areas where existing instruments may prove insufficient and the implementation of special instruments may be necessary.

## 3.3 Legal challenges

### *3.3.1 Challenges in drafting national criminal laws*

Proper legislation is the foundation for the investigation and prosecution of cybercrime. However, law-makers must continuously respond to Internet developments and monitor the effectiveness of existing provisions, especially given the speed of developments in network technology.

Historically, the introduction of computer-related services or Internet-related technologies has given rise to new forms of crime, soon after the technology was introduced. One example is the development of computer networks in the 1970s – the first unauthorized access to computer networks occurred shortly afterwards.[843] Similarly, the first software offences appeared soon after the introduction of personal computers in the 1980s, when these systems were used to copy software products.

It takes time to update national criminal law to prosecute new forms of online cybercrime. Indeed, some countries have not yet finished with this adjustment process. Offences that have been criminalized under national criminal law need to be reviewed and updated. For example, digital information must have equivalent status as traditional signatures and printouts.[844] Without the integration of cybercrime-related offences, violations cannot be prosecuted.

The main challenge for national criminal legal systems is the delay between the recognition of potential abuses of new technologies and necessary amendments to the national criminal law. This challenge remains as relevant and topical as ever as the speed of network innovation accelerates. Many countries are working hard to catch up with legislative adjustments.[845] In general, the adjustment process has three steps: adjustment to national law, identification of gaps in the penal code, and drafting of new legislation.

#### Adjustments to national law must start with the recognition of an abuse of new technology

Specific departments are needed within national law-enforcement agencies, which are qualified to investigate potential cybercrimes. The development of computer emergency response teams (CERTs),[846] computer incident response teams (CIRTs), computer security incident response teams (CSIRTs) and other research facilities have improved the situation.

#### Identification of gaps in the penal code

To ensure effective legislative foundations, it is necessary to compare the status of criminal legal provisions in the national law with requirements arising from the new kinds of criminal offences. In many cases, existing laws may be able to cover new varieties of existing crimes (e.g. laws addressing forgery

may just as easily be applied to electronic documents). The need for legislative amendments is limited to those offences that are omitted or insufficiently covered by the national law.

#### Drafting of new legislation

Based on experience, it may be difficult for national authorities to execute the drafting process for cybercrime without international cooperation, due to the rapid development of network technologies and their complex structures.[847] Drafting cybercrime legislation separately may result in significant duplication and waste of resources, and it is also necessary to monitor the development of international standards and strategies. Without the international harmonization of national criminal legal provisions, the fight against transnational cybercrime will run into serious difficulties, due to inconsistent or incompatible national legislations. Consequently, international attempts to harmonize different national penal laws are increasingly important.[848] National law can greatly benefit from the experience of other countries and international expert legal advice.

### 3.3.2 New offences

In most cases, crimes committed using ICTs are not new crimes, but scams modified to be committed online. One example is fraud – there is not much difference between someone sending a letter with the intention to mislead another person and an e-mail with the same intention.[849] If fraud is already a criminal offence, adjustment of national law may not be necessary to prosecute such acts.

The situation is different if the acts performed are no longer addressed by existing laws. In the past, some countries had adequate provisions for regular fraud, but were unable to deal with offences where a computer system was influenced, rather than a human. For these countries, it has been necessary to adopt new laws criminalizing computer-related fraud, in addition to the regular fraud. Various examples show how the extensive interpretation of existing provisions cannot substitute for the adoption of new laws.

Apart from adjustment for well-known scams, law-makers must continuously analyse new and developing types of cybercrime to ensure their effective criminalization. One example of a cybercrime that has not yet been criminalized in all countries is theft and fraud in computer and online games.[850] For a long time, discussions about online games focused on youth protection issues (e.g. the requirement for verification of age) and illegal content (e.g. access to child pornography in the online game "Second Life").[851] New criminal activities are constantly being discovered. Virtual currencies in online games may be "stolen" and traded in auction platforms.[852] Some virtual currencies have a value in terms of real currency (based on an exchange rate), giving the crime a 'real' dimension.[853] Such offences may not be prosecutable in all countries. In order to prevent safe havens for offenders, it is vital to monitor developments worldwide.

### 3.3.3 Increasing use of ICTs and the need for new investigative instruments

Offenders use ICTs in various ways in the preparation and execution of their offences.[854] Law-enforcement agencies need adequate instruments to investigate potential criminal acts. Some instruments (such as data retention[855]) could interfere with the rights of innocent Internet users.[856] If the severity of the criminal offence is out of proportion with the intensity of interference, the use of investigative instruments could be unjustified or unlawful. As a result, some instruments that could improve investigation have not yet been introduced in a number of countries.

The introduction of investigative instruments is always the result of a trade-off between the advantages for law-enforcement agencies and interference with the rights of innocent Internet users. It is essential to monitor ongoing criminal activities to evaluate whether threat levels change. Often, the introduction of new instruments has been justified on the basis of the "fight against terrorism", but this is more of an far-reaching motivation, rather than a specific justification *per se*.

### 3.3.4 Developing procedures for digital evidence

Especially due the low costs[857] compared to the storage of physical documents, the number of digital documents is increasing.[858] Digitization and the emerging use of ICTs has a great impact on procedures related to the collection of evidence and its use in court.[859] As a consequence of this development, digital evidence has been introduced as a new source of evidence.[860] It is defined as any data stored or transmitted using computer technology that supports the theory of how an offence occurred.[861] Handling digital evidence is accompanied with unique challenges and requires specific procedures.[862] One of the most difficult aspects is to maintain the integrity of the digital evidence.[863] Digital data are highly fragile and can easily be deleted[864] or modified. This is especially relevant for information stored in the system memory RAM that is automatically deleted when the system is shut down[865] and therefore requires special preservation techniques.[866] In addition, new developments can have great impact on dealing with digital evidence. An example is cloud computing. In the past, investigators were able to focus on the suspects' premises when searching for computer data. Today, they need to take into consideration that digital information might be stored abroad and can only be accessed remotely, if necessary.[867]

Digital evidence plays an important role in various phases of cybercrime investigations. It is in general possible to separate four phases.[868] The first phase is identification of the relevant evidence.[869] It is followed by collection and preservation of the evidence.[870] The third phase includes the analysis of computer technology and digital evidence. Finally, the evidence needs to be presented in court.

In addition to the procedures that relate to the presentation of digital evidence in court, the ways in which digital evidence is collected requires special attention. The collection of digital evidence is linked to computer forensics. The term 'computer forensics' describes the systematic analysis of IT equipment for the purpose of searching for digital evidence.[871] The fact that the amount of data stored in digital format is constantly increasing, highlights the logistic challenges of such investigations.[872] Approaches to automated forensic procedures using, for example, hash-value based searches for known child-pornography images[873] or a keyword search[874] therefore play an important role in addition to manual investigations.[875]

Depending on the requirement of the specific investigation, computer forensics could for example include analysing the hardware and software used by a suspect[876], supporting investigators in identifying relevant evidence,[877] recovering deleted files,[878] decrypting files[879] and identifying Internet users by analysing traffic data.[880]

684 See: *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632B-FF420389C0633B1B.pdf ; *Reith*, An Examination of Digital Forensic Models, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

685 Regarding hash-value based searches for illegal content, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 546 *et seq.*; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233.

686 For more information about the case, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin; as well as the information provided on the Interpol website, available at: www.interpol.int/Public/THB/vico/Default.asp

687 It was reported that the United States Department of Defense had to shut down their e-mail system after a hacking attack. See: www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

[688] Examples include the control of air-conditioning, access and surveillance systems, as well as the control of elevators and doors.

[689] See *Goodman*, The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 69, available at: http://media.hoover.org/documents/0817999825_69.pdf.

[690] *Bohn/Coroama/Langheinrich/Mattern/Rohs,* Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications, Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 *et seq.*, available at: www.vs.inf.ethz.ch/res/papers/hera.pdf.

[691] Regarding the impact of attacks, see: *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 3, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[692] A demonstration of the impact of even short interruptions to Internet and computer services was the harm caused by the computer worm "Sasser". In 2004, the worm affected computers running versions of Microsoft's Windows operating system. As a result of the worm, a number of services were interrupted. Among them were the US airline "Delta Airlines" that had to cancel several trans-Atlantic flights because its computer systems had been swamped by the worm, whilst the electronic mapping services of the British Coastguard were disabled for a few hours. See Heise News, 04.01.2005, available at: www.heise.de/newsticker/meldung/54746; BBC News, "Sasser net worm affects millions", 04.05.2004, available at: http://news.bbc.co.uk/1/hi/technology/3682537.stm.

[693] *Shimeall/Williams/Dunlevy*, Countering cyber war, NATO review, Winter 2001/2002, page 16, available at: www.cert.org/archive/pdf/counter_cyberwar.pdf.

[694] One analysis by "Red Sheriff" in 2002 stated that more than 90 per cent of users worldwide use Microsoft`s operating systems (source: www.tecchannel.de – 20.09.2002).

[695] Regarding the discussion on the effect of the monoculture of operating systems on cybersecurity, see *Picker*, Cyber Security: Of Heterogeneity and Autarky, available at: http://picker.uchicago.edu/Papers/PickerCyber.200.pdf; Warning: Microsoft 'Monoculture', Associated Press, 15.02.2004, available at www.wired.com/news/privacy/0,1848,62307,00.html; *Geer and others*, CyberInsecurity: The Cost of Monopoly, available at: http://cryptome.org/cyberinsecurity.htm.

[696] With regard to the effect of spam on developing countries, see: Spam issues in developing countries, 2005, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[697] Regarding the integration of developing countries in the protection of network infrastructure, see: Chairman's Report on ITU Workshop On creating trust in Critical Network Infrastructures, available at: www.itu.int/osg/spu/ni/security/docs/cni.10.pdf; World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

[698] WiMAX (Worldwide Interoperability for Microwave Access) is a technology that provides wireless data services over long distances. For more information, see: The WiMAX Forum, available at www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, WiMAX Technology for Broadband Wireless Access.

[699] Regarding the attack, see: *Toth*, Estonia under cyberattack, available at: www.cert.hu/dmdocuments/Estonia_attack2.pdf

[700] See: *Waterman*: Analysis: Who cyber smacked Estonia, United Press International 2007, available at: www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/.

[701] Regarding cybersecurity in developing countries, see: World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

[702] See below: § 4.

[703] According to ITU, there were over 2 billion Internet users by the end of 2010, of which 1.2 billion in developing countries. For more information see: ITU ICT Facts and Figures 2010, page 3, available at: www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

[704] See *Wallsten*, Regulation and Internet Use in Developing Countries, 2002, page 2.

[705] See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

[706] An example for new technology in this area is WiMAX (Worldwide Interoperability for Microwave Access), a standards-based wireless technology that provides broadband connections over long distances. Each WiMAX node could enable high-speed Internet connectivity in a radius of up to 50 km. For more information, see: The WiMAX Forum at www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

[707] Regarding the necessary steps to improve cybersecurity, see: World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

[708] The fact that the offenders are not only based in western countries is proven by current analysis that suggests for example that an increasing number of phishing websites are hosted in developing countries. For more details, see: Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf. Regarding phishing, see above: § 2.9.4.

[709] Regarding hash-value based searches, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233.

[710] Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law). For more information, see *Moore*, Cramming more components onto integrated circuits, Electronics, Volume 38, Number 8, 1965, available at: ftp://download.intel.com/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf; *Stokes*, Understanding Moore's Law, available at: http://arstechnica.com/articles/paedia/cpu/moore.ars/.

[711] "World Information Society Report 2007", ITU, Geneva, available at: www.itu.int/wisr/

[712] "Websense Security Trends Report 2004", page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

[713] *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf.

[714] In order to limit the availability of such tools, some countries criminalize their production and offer. An example of such a provision can be found in Art. 6 of the Council of Europe Convention on Cybercrime. See below: § 6.2.15.

[715] Regarding the costs, see: The World Information Society Report, 2007, available at: www.itu.int/wisr/

[716] See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

[717] For more information, see: *Ryan*, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue3/v9i3_a07-Ryan.pdf

[718] With regard to the advantages of wireless networks for the development of ICT infrastructure in developing countries, see: The Wireless Internet Opportunity for Developing Countries, 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

[719] One example of an approach to restrict the use of public terminals for criminal offences is Art. 7 of the Italian Decree-Law No. 144. Decree-Law 27 July 2005, No. 144 – "Urgent measures for combating international terrorism". For more information about the Decree-Law, see for example the article "Privacy and data retention policies in selected countries", available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[720] See below: § 6.5.13.

[721] Regarding the impact of censorship and control, see: *Burnheim*, The right to communicate, The Internet in Africa, 1999, available at: www.article19.org/pdfs/publications/africa-internet.pdf

[722] Regarding the question whether access to the Internet is a human right, see: *Hick/Halpin/Hoskins*, Human Rights and the Internet, 2000; Regarding the declaration of Internet Access as a human right in Estonia, see: Information and Communications Technology, in UNDP Annual Report 2001, page 12, available at: www.undp.org/dpa/annualreport2001/arinfocom.pdf; Background Paper on Freedom of Expression and Internet Regulation, 2001, available at: www.article19.org/pdfs/publications/freedom-of-expression-and-internet-regulation.pdf.

[723] Autronic v. Switzerland, Application No. 12726/87, Judgement of 22 May 1990, para. 47. Summary available at: http://sim.law.uu.nl/sim/caselaw/Hof.nsf/2422ec00f1ace923c1256681002b47f1/cd1bcbf61104580ec1256640004c1d0b?OpenDocument.

[724] The Internet Systems Consortium identified 490 million Domains (not webpages). See the Internet Domain Survey, July 2007, available at: www.isc.org/index.pl?/ops/ds/reports/2007-07/; The Internet monitoring company Netcraft reported in August 2007 a total of nearly 130 million websites at: http://news.netcraft.com/archives/2007/08/06/august_2007_web_server_survey.html.

[725] www.wikipedia.org

[726] In the future development of the Internet, information provided by users will become even more important. "User generated content" is a key trend among the latest developments shaping the Internet. For more information, see: *O'Reilly*, What Is Web 2.0 – Design Patterns and Business Models for the Next Generation of Software, 2005, available at: www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

[727] For more information, see: *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, 2006.

[728] See *Nogguchi*, Search engines lift cover of privacy, The Washington Post, 09.02.2004, available at: www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

[729] One example is the "Terrorist Handbook" – a pdf-document that contains detailed information how to build explosives, rockets and other weapons.

[730] See *Thomas*, Al Qaeda and the Internet: The Danger of 'Cyberplanning' Parameters 2003, page 112 *et seq.*, available at: www.iwar.org.uk/cyberterror/resources/cyberplanning/thomas.pdf; *Brown/Carlyle/Salmerón/Wood*, "Defending Critical Infrastructure", Interfaces, Vol. 36, No. 6, page 530, available at: www.nps.navy.mil/orfacpag/resumePages/Wood-pubs/defending_critical_infrastructure.pdf.

[731] "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 per cent of all information required about the enemy". Reports vary as to the source of the quotation: The British High Commissioner Paul Boateng mentioned in a speech in 2007 that the quote was "contained in the Al Qaeda training manual that was recovered from a safe house in Manchester" (see: *Boateng*, The role of the media in multicultural and multifaith societies, 2007, available at: www.britishhighcommission.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1125560437610&a=KArticle&aid=1171452755624. The United States Department of Defence reported that the quote was taken from an Al Qaeda Training Manual recovered in Afghanistan (see: www.defenselink.mil/webmasters/policy/rumsfeld_memo_to_DOD_webmasters.html). Regarding the availability of sensitive information on websites, see: *Knezo*, "Sensitive but Unclassified" Information and Other Controls: Policy & Options for Scientific and Technical Information, 2006, page 24, available at: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-8704:1.

[732] See Telegraph.co.uk, news from 13 January 2007.

[733] See for example, *Sadowsky/Zambrano/Dandjinou*, Internet Governance: A Discussion Document, 2004, available at: www.internetpolicy.net/governance/20040315paper.pdf;

[734] For a brief history of the Internet, including its military origins, see: *Leiner, Cerf, Clark, Kahn, Kleinrock; Lynch, Postel, Roberts, Wolff*, A Brief History of the Internet, available at: www.isoc.org/internet/history/brief.shtml.

[735] *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

[736] Regarding filter obligations/approaches, see: *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/ *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et. seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965; Regarding the discussion on filtering in different countries, see: *Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at:

http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

737 For more information regarding anonymous communications, see below: § 3.2.l2.

738 Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

739 The first and still most important communication protocols are: Transmission Control Protocol (TCP) and Internet Protocol (IP). For further information, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

740 See *Kahn/Lukasik*, Fighting Cyber Crime and Terrorism: The Role of Technology, presentation at the Stanford Conference, December 1999, page 6 *et seq.*; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 6, available at: http://media.hoover.org/documents/0817999825_1.pdf.

741 One example of the international cooperation of companies and delegation within international companies is the Compuserve case. The head of the German daughter company (Compuserve Germany) was prosecuted for making child pornography available that was accessible through the computer system of the mother company in the United States connected to the German company. See *Amtsgericht Muenchen*, Multimedia und Recht 1998, page 429 *et seq.* (with notes *Sieber*).

742 See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management.

743 Regarding the need for international cooperation in the fight against Cybercrime, see: *Putnam/Elliott,* International Responses to Cyber Crime, in Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism" 2001, page 35 *et seq.*, available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

744 National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

745 See *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, page 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

746 See below: § 3.2.10.

747 See *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142.

748 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA).

749 Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, page 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: http://.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

750 See: *Lewis*, Computer Espionage, Titan Rain and China, page 1, available at: www.csis.org/media/csis/pubs/051214_china_titan_rain.pdf.

751 Regarding the extend of cross-border cases related to computer fraud, see: *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 9, available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

[752] See below: § 6.6.12.

[753] See below: § 6.6.

[754] One example is phishing. Although most sites are still stored in the United States (32%), which has strong legislation in place, countries such as China (13%), Russia (7%) and the Republic of Korea (6%), which may have less effective instruments in the field of international cooperation in place, are playing a more important role. Apart from the United States, none of them has yet signed and ratified cybercrime specific international agreements that would enable and oblige them to effectively participate in international investigations.

[755] This issue was addressed by a number of international organizations. UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies". See below: § 5.1.

[756] For more information, see http://en.wikipedia.org/wiki/ILOVEYOU. Regarding the effect of the worm on critical information infrastructure protection, see: *Brock*, ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000, available at: www.gao.gov/archive/2000/ai00181t.pdf.

[757] BBC News, Police close in on Love Bug culprit, 06.05.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/738537.stm. Regarding the technology used, see: http://radsoft.net/news/roundups/luv/20000504,00.html.

[758] See for example: CNN, Love Bug virus raises spectre of cyberterrorism, 08.05.2000, http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; *Chawki*, A Critical Look at the Regulation of Cybercrime, www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 10, available at: http://media.hoover.org/documents/0817999825_1.pdf; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[759] One example of low-cost services that are automated is e-mail. The automation of registration allows providers to offer e-mail addresses free of charge. For more information on the difficulties of prosecuting cybercrime involving e-mail addresses, see: § 3.2.l2.

[760] The term "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[761] For more details on the automation of spam mails and the challenges for law-enforcement agencies, see: *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law enforcement agencies, Michigan Law Journal 2007, page 21, available at: www.michbar.org/journal/pdf/pdf4article1163.pdf.

[762] *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf.

[763] The Online-Community HackerWatch publishes regular reports on hacking attacks. Based on their sources, more than 250 million incidents were reported in only one month (August 2007). Source: www.hackerwatch.org.

[764] Regarding the distribution of hacking tools, see: CC Cert, Overview of Attack Trends, 2002, page 1, available at: www.cert.org/archive/pdf/attack_trends.pdf.

[765] See CC Cert, Overview of Attack Trends, 2002, page 1, available at: www.cert.org/archive/pdf/attack_trends.pdf.

[766] Nearly 50 per cent of all fraud complains reported to the United States Federal Trade Commission are related to an amount paid between USD 0 and 25. See Consumer Fraud and Identity Theft Complain Data – January – December 2006, Federal Trade Commission, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

[767] See Spam Issue in Developing Countries, Page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[768] Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law).

[769] Regarding the attacks, see: Lewis, Cyber Attacks Explained, 2007, available at: www.csis.org/media/csis/pubs/070615_cyber_attacks.pdf; A cyber-riot, The Economist, 10.05.2007, available at: www.economist.com/world/europe/PrinterFriendly.cfm?story_id=9163598; Digital Fears Emerge After Data Siege in

Estonia, The New York Times, 29.05.2007, available at: www.nytimes.com/2007/05/29/technology/29estonia.html?ei=5070&en=2e77eb21a1ab42ac&ex=1188360000&pagewanted=print.

[770] See: *Toth*, Estonia under cyber attack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

[771] See: *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, page 3, available at: www.cert.org/archive/pdf/Botnets.pdf.

[772] See: *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, available at: www.cert.org/archive/pdf/Botnets.pdf; *Barford/Yegneswaran*, An Inside Look at Botnets, available at: http://pages.cs.wisc.edu/~pb/botnets_final.pdf; *Jones*, BotNets: Detection and Mitigation.

[773] See Emerging Cybersecurity Issues Threaten Federal Information Systems, GAO, 2005, available at: www.gao.gov/new.items/d05231.pdf.

[774] *Keizer*, Dutch Botnet Suspects Ran 1.5 Million Machines, TechWeb, 21.10.2005, available at: www.techweb.com/wire/172303160

[775] See *Weber*, Criminals may overwhelm the web, BBC News, 25.01.2007, available at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6298641.stm.

[776] E.g. Botnets were used for the DoS attacks against computer systems in Estonia. See: *Toth*, Estonia under cyber attack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

[777] "Over one million potential victims of botnet cyber crime", United States Department of Justice, 2007, available at: www.ic3.gov/media/initiatives/BotRoast.pdf.

[778] *Staniford/Paxson/Weaver*, How to Own the Internet in Your Space Time, 2002, available at: www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf.

[779] *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International, 2006, page 142.

[780] *Gercke*, Use of Traffic Data to trace Cybercrime offenders, DUD 2002, page 477 *et seq.*; *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

[781] Regarding the necessary instruments, see below: § 6.5. One solution that is currently being discussed is data retention. Regarding the possibilities and risks of data retention, see: *Allitsch*, Data Retention on the Internet – A measure with one foot offside?, Computer Law Review International 2002, page 161 *et seq.*

[782] The term "quick freeze" is used to describe the immediate preservation of data on request of law-enforcement agencies. For more information, see below: § 6.5.4.

[783] The 24/7 network point pursuant to Art. 35 Convention on Cybercrime is a contact point appointed to reply to requests from law enforcement agencies outside the country. For more information, see below: § 6.6.8.

[784] The graphical user interface called World Wide Web (WWW) was created in 1989.

[785] The development of the graphical user interface supported content-related offences in particular. For more information, see above: § 2.6.

[786] For more information see above: § 2.6.5.

[787] Regarding the interception of VoIP by law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[788] With regard to the interception of peer-to-peer based VoIP communications, law-enforcement agencies need to concentrate on carrying out the interception by involving the access provider.

[789] Regarding the implications of the use of cell phones as storage media for computer forensics, see: *Al-Zarouni*, Mobile Handset Forensic Evidence: a challenge for Law Enforcement, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Al-Zarouni%20-%20Mobile%20Handset%20Forensic%20Evidence%20-%20a%20challenge%20for%20Law%20Enforcement.pdf.

[790] On the advantages of wireless networks for the development of an IT infrastructure in developing countries, see: "The Wireless Internet Opportunity for Developing Countries", 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

[791] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[792] Regarding the challenges related to anonymous communication, see: *Sobel*, The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity, Virginia Journal of Law and Technology, Symposium, Vol. 5, 2000, available at: www.vjolt.net/vol5/symposium/v5i1a3-Sobel.html.

[793] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[794] Regarding legislative approaches requiring identification prior to the use of public terminals, see Art. 7 of the Italian Decree-Law No. 144. For more information, see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.* and below: § 6.5.14.

[795] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[796] Regarding the difficulties that are caused if offenders use open wireless networks, see above: § 3.2.3.

[797] Regarding technical approaches in tracing back users of anonymous communication servers based on the TOR structure, see: *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

[798] See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[799] Regarding the possibilities of tracing offenders using e-mail headers, see: *Al-Zarouni*, Tracing Email Headers, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Al-Zarouni.pdf.

[800] *Donath*, Sociable Media, 2004, available at: http://smg.media.mit.edu/papers/Donath/SociableMedia.encyclopedia.pdf.

[801] Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. Regarding the benefits of anonymous communication see: *Du Pont*, The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

[802] "(33) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services [...]". Source: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[803] Article 37 – Traffic and billing data "1. Without prejudice to the provisions of paragraphs 2, 3 and 4, traffic data relating to users which are processed and stored to establish calls and other connections over the telecommunications network shall be erased or made anonymous upon termination of the call or other connection". – Regulation (EC) no 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[804] See below: § 6.5.13.

[805] Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For further information on the Decree-Law, see, for example, the article "Privacy and data retention policies in selected countries", available at: www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[806] Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

[807] This was also highlighted by the drafters of the Council of Europe Convention on Cybercrime, which contains a set of essential investigation instruments. The drafters of the report point out: "Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132.

[808] Regarding user-based approaches in the fight against cybercrime, see: *Goerling*, The Myth Of User Education, 2006 at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See also the comment made by *Jean-Pierre Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

[809] The term "voice over Internet protocol" (VoIP) is use to describe the transmission technology for delivering voice communication using packet-switched networks and related protocols. For more information, see: *Swale*, Voice Over IP: Systems and Solutions, 2001; *Black*, Voice Over IP, 2001.

[810] Regarding the importance of interception and the technical solutions, see: *Karpagavinayagam/State/Festor*, Monitoring Architecture for Lawful Interception in VoIP Networks, in Second International Conference on Internet Monitoring and Protection – ICIMP 2007. Regarding the challenges related to interception of data communication, see*: Swale/Chochliouros/Spiliopoulou/Chochliouros*, Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism – The European Response, in *Janczewski/Colarik*, Cyber Warfare and Cyber Terrorism, 2007, page 424.

[811] Regarding the differences between PSTN and VoIP communication, see: *Seedorf*, Lawful Interception in P2P-Based VoIP Systems, in *Schulzrinne/State/Niccolini*, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, page 217 *et seq.*

[812] Regarding the interception of VoIP by law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006; *Seedorf*, Lawful Interception in P2P-Based VoIP Systems, in *Schulzrinne/State/Niccolini*, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, page 217 *et seq*.

[813] Regarding the impact on computer forensic and criminal investigations, see: See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the mathematical background, see: *Menezes*, Handbook of Applied Cryptography, 1996, page 49 *et seq.*

[814] 74 per cent of respondents of the 2006 E-Crime Watch Survey mentioned encryption technology as one of the most efficient e-crime fight technologies. For more information, see: 2006 E-Crime Watch Survey, page 1, available at: www.cert.org/archive/pdf/ecrimesurvey06.pdf.

[815] *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

[816] *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

[817] *Kahn*, Cryptology goes Public, Foreign Affairs, 1979, Vol. 58, page 143.

[818] *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

[819] Regarding the consequences for the law enforcement, Denning observed: "The widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception and documents from lawful search and seizure, and where all electronic transactions are beyond the reach of any government regulation or oversight. The consequences of this to public safety and social and economic stability could be devastating". Excerpt from a presentation given by Denning, "The Future of Cryptography", to the joint Australian/OECD conference on Security, February, 1996. Regarding practical approaches to recover encrypted evidence see: *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of

Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

820 Examples include the software Pretty Good Privacy (see www.pgp.com) or True Crypt (see www.truecrypt.org).

821 Regarding the use of cryptography by terrorists, see: *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf. *Flamm*, Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography, available at: www.terrorismcentral.com/Library/Teasers/Flamm.html; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

822 See: *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

823 *Denning/Baugh*, Encryption and Evolving Technologies as Tolls of Organised Crime and Terrorism, 1997, available at: www.cs.georgetown.edu/~denning/crypto/oc-rpt.txt.

824 Regarding the most popular tools, see: *Frichot*, An Analysis and Comparison of Clustered Password Crackers, 2004, page 3, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Frichot-1.pdf. Regarding practical approaches in responding to the challenge of encryption see: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf.

825 See: Data Encryption, Parliament Office for Science and Technology No. 270, UK, 2006, page 3, available at: www.parliament.uk/documents/upload/postpn270.pdf.

826 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

827 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

828 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

829 *Schneier*, Applied Cryptography, page 185; *Bellare/Rogaway*, Introduction to Modern Cryptography, 2005, page 36, available at: www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

830 1 099 512 seconds.

831 *Usborne*, Has an old computer revealed that Reid toured world searching out new targets for al-Qaida?, The Independent, 18.01.2002, available at: www.independent.co.uk/news/world/americas/has-an-old-computer-revealed-that-reid-toured-world-searching-out-new-targets-for-alqaida-663609.html; *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf. With further reference to the case: *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

832 Equivalent to 10790283070806000000 years.

833 This technology is called BitLocker. For more information, see: "Windows Vista Security and Data Protection Improvements", 2005, available at: http://technet.microsoft.com/en-us/windowsvista/aa905073.aspx.

834 See *Leyden*, Vista encryption 'no threat' to computer forensics, The Register, 02.02.2007, available at: www.theregister.co.uk/2007/02/02/computer_forensics_vista/.

835 Regarding the encryption technology used by Skype (www.skype.com), see: *Berson*, Skype Security Evaluation, 2005, available at: www.skype.com/security/files/2005-031%20security%20evaluation.pdf.

[836] Phil Zimmermann, the developer of the encryption software PGP, developed a plug-in for VoIP software that can be used to install added encryption, in addition to the encryption provided by the operator of the communication services. The difficulty arising from the use of additional encryption methods is the fact that, even if the law-enforcement agencies intercept the communications between two suspects, the additional encryption will hinder the analysis. For more information on the software, see: *Markoff*, "Voice Encryption may draw US Scrutiny", New York Times, 22.05.2006, available at: www.nytimes.com/2006/05/22/technology/22privacy.html?ex=1305950400&en=ee5ceb136748c9a1&ei=5088. Regarding the related challenges for law-enforcement agencies, see: *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[837] *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[838] For further information, see: *Provos/Honeyman*, Hide and Seek: An Introduction to Steganography, available at: http://niels.xtdnet.nl/papers/practical.pdf; *Kharrazi/Sencar/Memon*, Image Steganography: Concepts and Practice, available at: http://isis.poly.edu/~steganography/pubs/ims04.pdf; *Labs*, Developments in Steganography, available at: http://web.media.mit.edu/~jrs/jrs_hiding99.pdf; *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.

[839] For practical detection approaches, see: *Jackson/Grunsch/Claypoole/Lamont*, Blind Steganography Detection Using a Computational Immune: A Work in Progress, International Journal of Digital Evidence, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04D31C4-A8D2-ADFD-E80423612B6AF885.pdf; *Farid*, Detecting Steganographic Messages in Digital Images, Technical Report TR2001-412, 2001; *Friedrich/Goljan*, Practical Steganalysis of Digital Images, Proceedings of SPIE Photonic West 2002: Electronic Imaging, Security and Watermarking of Multimedia Content IV, 4675, page 1 *et seq.*; *Johnson/Duric/Jajodia*, Information Hiding: Steganography and Watermarking, Attacks and Countermeasures, 2001.

[840] See below: § 6.5.11.

[841] See below: § 6.5.11.

[842] See above: § 3.2.8.

[843] See BBC News, Hacking: A history, 27.10.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/994700.stm.

[844] An example of the integration of digital sources is Section 11, Subsection 3 of the German Penal Code: "Audio & visual recording media, data storage media, illustrations and other images shall be the equivalent of writings in those provisions which refer to this subsection."

[845] Within this process, the case-law based Anglo-American law system has advantages in terms of reaction time.

[846] Computer Emergency Response Team. The CERT Coordination Center was founded in 1988 after the Morris worm incident, which brought 10 per cent of Internet systems to a halt in November 1988. For more information on the history of the CERT CC, see: www.cert.org/meet_cert/; *Goodman*, Why the Police don't Care about Computer Crime, Harvard Journal of Law and Technology, Vol. 10, Issue 3, page 475.

[847] Examples of international cooperation in the fight against cybercrime include the Council of Europe Convention on Cybercrime and UN Resolution 55/63.

[848] See below: § 5.

[849] See above: § 2.8.1.

[850] Regarding the offences recognized in relation to online games, see above: § 2.6.5.

[851] Regarding the trade of child pornography in Second Life, see for example BBC, Second Life "child abuse" claim, 09.05.2007, at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/6638331.stm; Reuters, Virtual Child Pornography illegal in Italy, 23.02.2007, at: http://secondlife.reuters.com/stories/2007/02/23/virtual-child-porn-illegal-in-italy/.

[852] *Gercke*, Zeitschrift fuer Urheber- und Medienrecht 2007, 289 *et seq.*

[853] *Reuters*, UK panel urges real-life treatment for virtual cash, 14.05.2007, available at: http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/.

[854] Regarding the use of ICTs by terrorist groups, see: *Conway*, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006, page 16; *Hutchinson*, "Information terrorism: networked influence", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Hutchinson%20-%20Information%20terrorism_%20networked%20influence.pdf; *Gercke*, Cyberterrorism, Computer Law Review International 2007, page 64.

[855] Data retention describes the collection of certain data (such as traffic data) through obliged institutions, e.g. access providers. For more details, see below: § 6.5.5.

[856] Relating to these concerns, see: Advocate General Opinion, 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top.

[857] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

[858] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

[859] *Casey*, Digital Evidence and Computer Crime, 2004, page 11; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1.

[860] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historic development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol.1, No.1.

[861] *Casey*, Digital Evidence and Computer Crime, 2004, page 12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm.

[862] Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq*.

[863] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1.

[864] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

[865] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[866] See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.

[867] *Casey*, Digital Evidence and Computer Crime, 2004, page 20.

[868] Regarding the different models of cybercrime investigations, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also: *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

[869] This includes the development of investigation strategies.

[870] The second phase covers especially the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[871] See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, No. 2, page 3.

[872] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 532.

[873] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

[874] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

[875] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

[876] This includes for example the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

[877] This includes for example the identification of storage locations. See *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

[878] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

[879] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process within forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

[880] Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

# 4. Anti-cybercrime strategies

**Bibliography (selected):** *Garcia-Murillo*, Regulatory responses to convergence: experiences from four countries, Info, 2005, Volume 7, Issue 1; *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141*; Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf*; Henten/Samarajiva/Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1; *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1; *Killcrece, et al,* Organizational Models for Computer Security Incident Response Teams (CSIRTs). Handbook, December, 2003*; Lie / Macmilian*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf; *Macmillian.* Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf; *Maggetti*, The Role of Independent Regulatory Agencies in Policy-Making a Comparative Analysis of Six Decision-Making Processes in the Netherlands, Sweden and Switzerland. IEPI, University of Lausanne, available at: http://regulation.upf.edu/ecpr-07-papers/mmaggetti.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, page 245 *et seq.*; *Spyrelli*, Regulating The Regulators? An Assessment of Institutional Structures and Procedural Rules of National Regulatory Authorities, International Journal of Communications Law and Policy, Issue. 8, Winter. 2003/2004; *Stevens*, Consumer Protection: Meeting the expectation of connected Consumer. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Consumer-protection_Stevens.pdf.

The growing number of recognized cybercrimes and technical tools to automate cybercrime offences (including anonymous file-sharing systems[881] and software products designed to develop computer viruses[882]) mean that the fight against cybercrime has become an essential element of law-enforcement activities worldwide. Cybercrime is a challenge to law-enforcement agencies in both developed and developing countries. Since ICTs evolve so rapidly, especially in developing countries, the creation and implementation of an effective anti-cybercrime strategy as part of a national cybersecurity strategy is essential.

## 4.1 Cybercrime legislation as an integral part of a cybersecurity strategy

As pointed out previously, cybersecurity[883] plays an important role in the ongoing development of information technology, as well as Internet services.[884] Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy.[885] Cybersecurity strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime.[886]

An anti-cybercrime strategy should be an integral element of a cybersecurity strategy. The ITU Global Cybersecurity Agenda,[887] as a global framework for dialogue and international cooperation to coordinate the international response to the growing challenges to cybersecurity and to enhance confidence and security in the information society, builds on existing work, initiatives and partnerships with the objective of proposing global strategies to address these related challenges. All the required measures highlighted in the five pillars of Global Cybersecurity Agenda are relevant to any cybersecurity strategy. Furthermore, the ability to effectively fight against cybercrime requires measures to be undertaken within all of the five pillars.[888]

### 4.1.1 Implementation of existing strategies

One possibility is that anti-cybercrime strategies developed in industrialized countries could be introduced in developing countries, offering advantages of reduced cost and time for development. The implementation of existing strategies could enable developing countries to benefit from existing insights and experience.

Nevertheless, the implementation of an existing anti-cybercrime strategy poses a number of difficulties. Although similar challenges confront both developing and developed countries, the optimal solutions that might be adopted depend on the resources and capabilities of each country. Industrialized countries may be able to promote cybersecurity in different and more flexible ways, e.g. by focusing on more cost-intensive technical protection issues.

There are several other issues that need to be taken into account by developing countries adopting existing anti-cybercrime strategies. They include compatibility of respective legal systems, the status of supporting initiatives (e.g. education of the society), the extent of self-protection measures in place as well as the extent of private sector support (e.g. through public-private partnerships).

### 4.1.2 Regional differences

Given the international nature of cybercrime, the harmonization of national laws and techniques is vital in the fight against cybercrime. However, harmonization must take into account regional demand and capacity. The importance of regional aspects in the implementation of anti-cybercrime strategies is underlined by the fact that many legal and technical standards were agreed among industrialized countries and do not include various aspects important for developing countries.[889] Therefore, regional factors and differences need to be included within their implementation elsewhere.

### 4.1.3 Relevance of cybercrime issues within the pillars of cybersecurity

The Global Cybersecurity Agenda has seven main strategic goals, built on five work areas: 1) Legal measures; 2) Technical and procedural measures; 3) Organizational structures; 4) Capacity building; and 5) International cooperation. As pointed out above, issues related to cybercrime play an important role in all five pillars of the Global Cybersecurity Agenda. Among these work areas, the "Legal measures" work areas focuses on how to address the legislative challenges posed by criminal activities committed over ICT networks in an internationally compatible manner.

## 4.2 A cybercrime policy as starting point

Developing legislation to criminalize certain conduct or introduce investigation instruments is a rather unusual process for most countries. The regular procedure is first of all to introduce a policy.[890] A policy is comparable to a strategy that defines the different instruments used to address the issue. Unlike a more general cybercrime strategy that may address various stakeholders, the role of policy is to define the government's public response to a certain issue.[891] This response is not necessarily limited to legislation as governments have various instruments that can be used to achieve policy goals. And even if the decision is made that there is a need to implement legislation, it does not necessarily need to focus on criminal law but could also include legislation more focussed on crime prevention. In this regard, developing a policy enables a government to comprehensively define the government response to a problem. As the fight against cybercrime can never solely be limited to introducing legislation, but contains various strategies with different measures, the policy can ensure that those different measures don't cause conflicts.

Within different approaches to harmonize cybercrime legislation too little priority has been given to not only integrating the legislation in the national legal framework but also including it into an existing policy, or developing such policy for the first time. As a consequence some countries that merely introduced cybercrime legislation without having developed an anti-cybercrime strategy as well as policies on the government level faced severe difficulties. They were mainly a result of a lack of crime prevention measures as well as an overlapping between different measures.

### 4.2.1 Responsibility within the government

The policy enables the adjustment of competences for a topic within the government. Overlapping between different ministries is nothing unusual – with regard to cybercrime it is happening frequently as it is an interdisciplinary subject.[892] Aspects related to the fight against cybercrime may be related to the mandate of the Ministry of Justice, Ministry of Communication or Ministry of National Security to name only three. Within the process of developing a policy, the role of the different government institutions involved can be defined.

This is, for example, expressed in the ICB4PAC[893] Draft Model Policy for Cybercrime:

> *It is in this regard crucial that the responsibilities of the different stakeholders are clearly defined. This is particularly relevant because Cybercrime is a cross-sector topic that might relate to mandates of different institutions such as Attorney General, Ministry of Communication and other.*

### 4.2.2 Defining the different components

As indicated above the policy can be used to define different components of the approach. This could range from strengthening institutional capacities (e.g. police and prosecution) to concrete amendments of legislation (such as the introduction of more advanced legislation).

This is another issue expressed in the ICB4PAC[894] Draft Model Policy for Cybercrime:

> *Addressing the multi-dimensional challenges of fighting Cybercrime requires a comprehensive approach that should include overall policies, legislation, education and awareness raising, capacity building, research as well as technical approaches.*

Ideally the policy should be used to coordinate the various activities – even if they are implemented by different ministries and government bodies. The fact that policies in general require approval by cabinet therefore not only enables the identification of different government bodies and ministries involved with regard to the topic, but also enables the harmonization of their activities.[895]

### 4.2.3 Determination of stakeholders

The policy can not only identify the government institutions involved but also the stakeholders that should be addressed. It may, for example, be necessary to develop guidelines with regard to the involvement of the private sector.

The issue of stakeholders that should be involved and addressed is, for example, expressed in the ICB4PAC[896] Draft Model Policy for Cybercrime:

> *Further more such approach needs to involve various stakeholders such as government, ministries and government agencies, private sector, schools and universities, customary leaders, community, international and regional bodies, law enforcement, judges, customs, prosecutors, lawyers, civil society and NGOs.*

### 4.2.4 Identification of benchmarks

As underlined further below the importance of harmonization of legislation is identified as a key priority by different regional organizations.[897] But the need for harmonization is not limited to legislation – it includes issues like strategy and training of experts.[898] The policy can be used to identify the areas where harmonization should take place as well as to define the regional and/or international standards that should be implemented.

The importance of harmonization is for example expressed in the ICB4PAC[899] Draft Model Policy for Cybercrime.

*With regard to the global dimension of Cybercrime as well as the need to protect the Internet users in the region from becoming victims of Cybercrime, measures to increase the ability to combat Cybercrime should have high priority. Strategies and especially legislation that is developed to address the challenges of Cybercrime should on the one hand side be in line with international standards and on the other hand side reflect the uniqueness of the region.*

Another example is the HIPCAR Model Policy on Cybercrime[900].

*There shall be provisions covering the most common and internationally widely accepted forms of Cybercrime as well as those offences that are of specific interest for the region (such as for example SPAM).*
*To ensure the ability to cooperate with law enforcement agencies from countries in the region as well as outside the region the legislation shall be compatible to both international standards and best practices as well as (up to the largest extent possible) to existing regional standards and best practices.*

### 4.2.5 Defining key topics for legislation

The policy can be used to define key areas that should be addressed by legislation. This could include a list of offences that should be covered, for example. The level of detail could go down to details of provisions that should be included in a cybercrime law.

One example is the HIPCAR Model Policy on Cybercrime[901].

*There should be a provision criminalizing the intentional and illegal production, sale and related acts related to child pornography. Especially in this respect international standards should be taken into consideration. The legislation should in addition cover the criminalization of the possession of child pornography and gaining access to child pornography websites. An exemption that enables law enforcement agencies to carry out investigations should be included.*

### 4.2.6 Defining legal frameworks that require amendments, updates or changes

Introducing cybercrime legislation is not an easy task as there are various areas that require regulation. In addition to substantive criminal law and procedural law, cybercrime legislation may include issues related to international cooperation, electronic evidence and the liability of an Internet Service Provider (ISP). In most countries elements of such legislation may already exist – often in different legal frameworks. Provisions related to cybercrime do not necessarily need to be implemented in one single piece of legislation. With regard to existing structures, it might be necessary to update different pieces of legislation (such as amending an Evidence Act to ensure that it is applicable with regard to the admissibility of electronic evidence in criminal proceedings) or remove provision from an older law (for example in a Telecommunications Act) within the process of introducing new legislation.

This approach of implementing cybercrime legislation by a process of respecting existing structures is certainly more challenging than simply implementing a regional standard or international best practice word by word in a standalone piece of legislation. But with regard to the fact that this process of customizing allows national legal traditions to be kept, many countries favour such an approach.

The policy can be used to define the different components that should be integrated as well as identify existing laws that require updates.

### 4.2.7 Relevance of crime prevention

Despite the fact that threats of punishment potentially prevent crimes, the focus of criminal legislation is not on crime prevention but on sanctioning crime. However, crime prevention is identified as a key component in an effective fight against cybercrime.[902] Measures can range from technical solutions (such as firewalls that prevent illegal access to a computer system and anti-virus software that can hinder the installation of malicious software) to the blocking of access to illegal content.[903]

The importance of crime prevention is for example expressed in the ICB4PAC[904] Draft Model Policy for Cybercrime:

> *In addition to the criminalisation of Cybercrime and the improvement of the ability of law enforcement to combat Cybercrime crime preventions measures need to be developed. Within the process of developing such measures, that can range from technical solutions to increasing user awareness, it is important to identify those groups that require specific attention such as youth, technologically challenged people (such as people from isolated villages that are technologically unaware) and women. However, crime prevention measures should also apply to more advanced users and technology-affiliate players such as critical infrastructure provider (such as the tourism or financial sector). The debate about necessary measures should include the whole range of instruments such as awareness raising, making available and promoting free of charge protection technology (such as anti-virus software) and the implementation of solutions that enable parents to restrict the access to certain content. Such measures should ideally be available at the time of an introduction of a service/technology and maintained through out it's operation. To ensure a wider reach of such measure a broad range of stakeholders should be involved that range from Internet Service Provider to governments and regional bodies and explore various sources for funding.*

## 4.3 The role of regulators in fighting cybercrime

In decades gone by, the focus of solutions discussed to address cybercrime was on legislation. As already pointed out in the chapter dealing with an anti-cybercrime strategy, however, the necessary components of a comprehensive approach to address cybercrime are more complex. Recently, the spotlight has fallen on the role of regulators in the fight of cybercrime.

### *4.3.1 From telecommunication regulation to ICT regulation*

The role of regulators in the context of telecommunications is widely recognized.[905] As Internet has eroded the old models of the division of responsibilities between government and private sector, a transformation of the traditional role of ICT regulators and a change in the focus of ICT regulation can be observed.[906] Already today ICT regulatory authorities find themselves involved in a range of activities linked to addressing cybercrime. This is especially relevant for areas like content regulation, network safety and consumer protection, as users have become vulnerable.[907] The involvement of regulators is therefore the result of the fact that cybercrime undermines the development of the ICT industry and related products and services.

The new duties and responsibilities of the ICT regulator in combating cybercrime can be seen as part of the wider trend towards the conversion of centralized models of cybercrime regulation into flexible structures. In some countries, ICT regulators have already explored the possibility of transferring the scope of regulatory duties from competition and authorization issues within the telecom industry to broader consumer protection, industry development, cybersafety, participation in cybercrime policy-making and implementation, which includes the wider use of ICTs and as a consequence cybercrime-related issues. While some new regulatory authorities have been created with mandates and responsibilities that include cybercrime,[908] older established ICT regulators have extended their existing tasks to include various activities aimed at tackling cyber-related threats.[909] However, the extent and limitations of such involvement are still under discussion.

### *4.3.2 Models for extension of regulator responsibility*

There are two different models for establishing the mandate of regulators in combating cybercrime, namely: extensively interpreting the existing mandate, or creating new mandates.

Two traditional areas of involvement of regulators are consumer protection and network safety. With the shift from telecommunication services to Internet-related services, the focus of consumer protection has changed. In addition to the traditional threats, the impact of Spam, malicious software and botnets need to be taken into consideration. One example of extending a mandate comes from the Dutch Independent Post and Telecommunication Authority (OPTA). The mandate[910] of the regulator includes Spam

prohibition[911] and preventing the dissemination of malware.[912] During the debate on the mandate of OPTA, the organization expressed the view that a bridge should be built between cybersecurity as a traditional field of activity and cybercrime in order to effectively address both issues.[913] If cybercrime is seen as a failure of cybersecurity, the mandate of regulators is consequently automatically expanded.

The possibility of extending the regulator's mandate to include cybercrime issues also depends on the institutional design of the regulator, and whether it is a multisector regulator (like utility commissions), a sector-specific telecom regulator or a converged regulator. While every model of institutional design has its advantages and disadvantages from the perspective of ICT industry regulation[914], the type of institutional design should be taken into account when assessing how and in what areas the ICT regulator should be involved. Converged regulators, with responsibility for media and content as well as ICT services, generally face a challenge in terms of complexity of workloads. However, their comprehensive mandate can constitute an advantage in dealing with content-related issues, such as child pornography or other illegal or harmful content.[915] In a converged environment where traditional telecommunication regulators may struggle to resolve certain issues, such as consolidation between media content and telecommunication service providers, the converged regulator appears to be in a better position to address content-network issues. Furthermore, the converged regulator can help to avoid inconsistency and uncertainty of regulation and unequal regulatory intervention in respect of the different content delivered over various platforms.[916] Nevertheless, the discussion of the advantages of a converged regulator should not undermine the importance of the activities of single-sector regulators. While, for instance, up to the end of 2009 the European Union had only four converged ICT regulators,[917] many more were involved in addressing cybercrime.

When thinking of extending the interpretation of existing mandates, account must be taken of the capacity of the regulator and the need to avoid overlap with the mandates of other organizations. Such potential conflicts can be solved more easily if new mandates are clearly defined.

The second approach is the creation of new mandates. In view of the potential for conflicts, countries such as Malaysia have decided to redefine mandates to avoid confusion and overlap. The Malaysian Communications and Multimedia Commission (MCMC), as a converged regulator, has established a special department[918] dealing with information security and network reliability, the integrity of communications and critical communication infrastructure.[919] A similar approach can be observed in South Korea, where in 2008 the Korea Communications Commission (KCC) was created by consolidating the former Ministry of Information and Communication and the Korean Broadcasting Commission. Among other duties, KCC is responsible for the protection of Internet users from harmful or illegal content.[920]

### 4.3.3 Examples for involvement of regulators in fighting cybercrime

It is not only the model for defining the regulators' mandate, but also the scope of action of ICT regulators in this field that is not yet clearly defined. Only few ICT regulatory bodies have effective powers to go beyond telecommunication regulation and deal with wider ICT sector issues. Operating in a rapidly changing and developing sector exposes ICT regulators to new areas that have traditionally been considered as the domain of other government departments and agencies, or even no-one's domain at all.[921] Even if the regulator possesses *de facto* sufficient competence and industry expertise to be involved in addressing specific cybercrime-related issues, a clear mandate pinpointing the exact areas of involvement is key for regulators to be effective. The potential areas of involvement for regulators are highlighted below:

#### Global policy strategies

The principle of the division of power within the state[922] separates policy-making and policy implementation.[923] Despite the importance of this concept, the complexity of the issue may require regulators to be involved in policy advice.[924] On account of their industry expertise and existing communication channels with other stakeholders, ICT regulators in many countries play an important role in determining policies and strategies for ICT industry development.[925] In some countries, the role of providing inputs to ICT policy-making is therefore considered as one of the main tasks of the ICT

regulator.[926] While this common practice focuses on advice on telecommunication issues, the mandate could be extended to cybercrime. In Finland, the government has set up an Advisory Committee for Information Security (ACIS) under the Finnish Communications Regulatory Authority (FICORA) for the purpose of developing their national information strategy. [927] The proposal released by ACIS in 2002 identifies goals and measures to promote the information-security strategy. Several measures can be considered as cybercrime-related, and highlight the importance of developing and improving appropriate legislation, international cooperation, and increasing information-security awareness among end-users.[928]

### Involvement in the development of cybercrime legislation

The competent body to adopt legislation is the legislator, not a regulatory authority. However, the ICT regulator can play an important role in the process of developing cybercrime legislation. In view of the experience regulators possess in data protection, the confidentiality of data transmission, prevention of the spreading of malicious software, other aspects of consumer protection and ISP responsibilities, their involvement is especially discussed in those fields.[929] In addition, criminal law is not an unknown field for regulators, since in many countries grave violations of obligations in the traditional area of regulatory work may be subject to criminal sanctions. In addition to having an advisory role with regard to overall strategies as highlighted above**,** regulators can be involved in the process of drafting legislation. The Ugandan Communications Commission, for example, was involved as adviser in the process of drafting cybercrime legislation.[930] Moreover, the Ugandan Communications Commission, through the Ugandan National Task Force on cybercrime legislation, is now part of a regional initiative, called the East African Countries' Task Force on Cyber Laws, which is dedicated to an ongoing process of development and harmonization of cybercrime laws in the East African region.[931] In Zambia, the Communications Authority[932] was reported to have assisted in drafting new cybercrime-related legislation,[933] namely the Electronic Communications and Transactions Act 2009.[934] A further example is Belgium, where in 2006 the Belgian ICT regulator (BIPT) assisted in the process of drafting cybercrime legislation. The draft was developed in cooperation with the Federal Public Service of Justice and the Federal Computer Crime Unit.[935]

### Detecting and investigating cybercrime

Computer incident response teams (CIRTs) play an important role in monitoring, detecting, analysing and investigating cyberthreats and cyberincidents.[936] Due to the multisector nature of the cybercrime problem, different CIRTs have been established by a range of stakeholders, including governments, businesses, telecom operators and academia, to fulfil various functions.[937] In some countries, ICT regulators are responsible for creating and running national CIRTs. These CIRTs are usually considered not only as major entities in charge of detecting and investigating cybercrime incidents at the national level, but also as key participants in actions to enhance cybercrime cooperation at the international level. One of the first CIRTs established as an initiative under the ICT regulator is the Finnish national Computer Emergency Response Team, launched in January 2002 within the Finnish Communications Regulatory Authority (FICORA).[938] Other examples may be found in Sweden,[939] United Arab Emirates[940] and Qatar.[941]

### Facilitation of law enforcement

An ICT regulator can only undertake investigations and in this respect act as law enforcement on the basis of an explicit mandate granted to the regulator to exercise and enforce particular legal provisions. Some countries have authorized ICT regulators to act as a law-enforcement agency in cybercrime-related areas such as anti-spam, content regulation or enforcing co-regulatory measures. With regard to Spam, some European ICT regulators are already part of a contact network of anti-spam enforcement authorities established by the European Commission in 2004 to fight spam on a pan-European level.[942] The OECD Task Force on Spam also lists ICT regulators as contact points for enforcement agencies.[943] Cooperation agreements between ICT regulators and cybercrime units at the police level are also known to exist in the Netherlands and Romania.[944]

### 4.3.4 Legal measures

Of the five pillars of the Global Cybersecurity Agenda, legal measures are probably the most relevant with regard to an anti-cybercrime strategy.

#### Substantive criminal law

This requires first of all the necessary substantive criminal-law provisions to criminalize acts such as computer fraud, illegal access, data interference, copyright violations and child pornography.[945] The fact that provisions exist in the criminal code that are applicable to similar acts committed outside the network does not mean that they can be applied to acts committed over the Internet as well.[946] Therefore, a thorough analysis of current national laws is vital to identify any possible gaps.[947]

#### Criminal procedural law

Apart from substantive criminal-law provisions,[948] law-enforcement agencies need the necessary tools and instruments to investigate cybercrime.[949] Such investigations themselves present a number of challenges.[950] Perpetrators can act from nearly any location in the world and take measures to mask their identity.[951] The tools and instruments needed to investigate cybercrime can be quite different from those used to investigate ordinary crimes.[952] Due to the international dimension[953] of cybercrime it is in addition necessary to develop the legal national framework to be able to cooperate with law-enforcement agencies abroad.[954]

#### Electronic evidence

When dealing with cybercrime the competent investigation authorities, as well as courts, need to deal with electronic evidence. Dealing with such evidence presents a number of challenges[955] but also opens up new possibilities for investigation and for the work of forensic experts and courts.[956] In those cases where no other sources of evidence are available, the ability to successfully identify and prosecute an offender may depend upon the correct collection and evaluation of electronic evidence.[957] This influences the way law-enforcement agencies and courts deal with such evidence.[958] While traditional documents are introduced by handing out the original document in court, digital evidence in some cases requires specific procedures that do not allow conversion into traditional evidence, e.g. by presenting a printout of files and other discovered data.[959] Having legislation in place that deals with the admissibility of evidence is therefore seen as vital in the fight against cybercrime.

#### International cooperation

Due to the transnational dimension of the Internet and the globalization of services, an increasing number of cybercrimes have an international dimension.[960] Countries that desire to cooperate with other countries in investigating cross-border crime will need to use instruments of international cooperation.[961] Taking into account the mobility of offenders, the independence from presence of the offender and the impact of the offence shows the challenge and the need for a collaboration of law-enforcement and judicial authorities.[962] Due to differences in national law and limited instruments, international cooperation is considered to be one of the major challenges of a globalization of crime.[963] Within a comprehensive approach to address cybercrime, countries need to consider strengthening their ability to cooperate with other countries and making the procedure more efficient.

#### Liability of service provider

Cybercrime can hardly be committed without the use of the services of an Internet Service Provider (ISP). E-Mails with threatening content are sent by using the service of an e-mail provider and illegal content downloaded from a website involves among others the service of a Hosting Provider and Access Provider. As a consequence, ISPs are often in the centre of criminal investigations involving offenders who use the ISPs' services to commit an offence.[964] Taking into account that on the one hand, cybercrime cannot be committed without the involvement of ISPs but on the other hand, providers often do not have the ability

to prevent these crimes, led to the question of whether the responsibility of Internet providers needs to be limited.[965] This issue may be addressed within a comprehensive legal approach to cybercrime.

### 4.3.5 Technical and procedural measures

Cybercrime-related investigations very often have a strong technical component.[966] In addition, the requirement to maintain the integrity of the evidence during an investigation calls for precise procedures. The development of the necessary capacities as well as procedures is therefore a necessary requirement in the fight against cybercrime.

Another issue is the development of technical protection systems. Well-protected computer systems are more difficult to attack. Improving technical protection by implementing proper security standards is an important first step. For example, changes in the online banking system (e.g. the switch from TAN[967] to ITAN[968]) have eliminated much of the danger posed by current "phishing" attacks, demonstrating the vital importance of technical solutions.[969] Technical protection measures should include all elements of the technical infrastructure – the core network infrastructure, as well as the many individually connected computers worldwide. Two potential target groups can be identified for protecting Internet users and businesses: end users and businesses (direct approach) and service providers and software companies.

Logistically, it can be easier to focus on protection of core infrastructure (e.g. backbone network, routers, essential services), rather than integrating millions of users into an anti-cybercrime strategy. User protection can be achieved indirectly, by securing the services consumers use, such as online banking. This indirect approach to protecting Internet users can reduce the number of people and institutions that need to be included in steps to promote technical protection.

Although limiting the number of people that need to be included in technical protection might seem desirable, computer and Internet users are often the weakest link and the main target of criminals. It is often easier to attack private computers to obtain sensitive information, rather than the well-protected computer systems of a financial institution. Despite the logistical problems, the protection of end-user infrastructure is vital for the technical protection of the whole network.

Internet service providers and product vendors (e.g. software companies) play a vital role in the support of anti-cybercrime strategies. Due to their direct contact with clients, they can operate as a guarantor of security activities (e.g. the distribution of protection tools and information on the current status of most recent scams).[970]

#### Organizational structures

An effective fight against cybercrime requires highly developed organizational structures. Without having the right structures in place, ones that avoid overlapping and are based on clear competences, it will hardly be possible to carry out complex investigations that require the assistance of different legal as well as technical experts.

#### Capacity building and user education

Cybercrime is a global phenomenon. In order to be able to investigate offences effectively, laws need to be harmonized and means of international cooperation need to be developed. In order to ensure global standards in both the developed and the developing countries, capacity building is necessary.[971]

In addition to capacity building, user education is required.[972] Certain cybercrimes – especially those related to fraud, such as "phishing" and "spoofing" – do not generally depend on a lack of technical protection, but rather on a lack of awareness on the part of the victims.[973] There are various software products that can automatically identify fraudulent websites,[974] but until now these products cannot identify all suspicious websites. A user-protection strategy based only on software products has limited ability to protect users.[975] Although technical protection measures continue to develop and available products are updated on a regular basis, such products cannot yet substitute for other approaches.

One of the most important elements in the prevention of cybercrime is user education.[976] For example, if users are aware that their financial institutions will never contact them by e-mail requesting passwords or bank-account details, they cannot fall victim to phishing or identity-fraud attacks. The education of Internet users reduces the number of potential targets. Users can be educated through public campaigns, lessons in schools, libraries, IT centres and universities as well as public private partnerships (PPPs).

One important requirement of an efficient education and information strategy is open communication of the latest cybercrime threats. Some states and/or private businesses refuse to emphasize that citizens and clients respectively are affected by cybercrime threats, in order to avoid them losing trust in online communication services. The United States Federal Bureau of Investigation has explicitly asked companies to overcome their aversion to negative publicity and report cybercrime.[977] In order to determine threat levels, as well as to inform users, it is vital to improve the collection and publication of relevant information.[978]

### *International cooperation*

In many cases, data-transfer processes in the Internet affect more than one country.[979] This is a result of the design of the network, and the fact that the protocols ensure that successful transmissions can be made, even if direct lines are temporarily blocked.[980] In addition, a large number of Internet services (like for example hosting services) are offered by companies that are based abroad.[981]

In those cases where the offender is not based in the same country at the victim, the investigation requires cooperation between law-enforcement agencies in all the countries affected.[982] International and transnational investigations without the consent of the competent authorities in the countries involved are difficult in regard to the principle of national sovereignty. This principle does not in general allow one country to carry out investigations within the territory of another country without the permission of the local authorities.[983] Therefore, investigations need to be carried out with the support of the authorities in all the countries involved. With regard to the fact that in most cases there is only a very short time gap available in which successful investigations can take place, application of the classic mutual legal assistance regimes involves clear difficulties when it comes to cybercrime investigations. This is due to the fact that mutual legal assistance in general requires time-consuming formal procedures. As a result, improvement in terms of enhanced international cooperation plays an important and critical role in the development and implementation of cybersecurity strategies and anti-cybercrime strategies.

881 *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Design, 2005. See also above: § 3.2.l.

882 For an overview of the tools used, see *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf. For more information, see above: § 3.2.8.

883 The term "cybersecurity" is used to summarize various activities ITU-T Recommendation X.1205 "Overview of Cybersecurity" provides a definition, description of technologies, and network protection principles: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyberenvironment. Cybersecurity strives to ensure the attainment and maintenance of the security

properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality." Also see: *ITU*, List of Security-Related Terms and Definitions, available at: www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc.

884 With regard to developments related to developing countries, see: ITU Cybersecurity Work Programme to Assist Developing Countries 2007-2009, 2007, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

885 See for example: ITU WTSA Resolution 50 (Rev. Johannesburg, 2008) on Cybersecurity available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52 (Rev. Johannesburg, 2008), on Countering and combating spam, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45 (Doha, 2006), on Mechanism for enhancing cooperation on cybersecurity, including combating spam available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf; EU Communication towards a general policy on the fight against cyber crime, 2007 available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf; Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, 2005, available at: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

886 For more information, see *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1.

887 For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

888 See below: § 4.4.

889 The negotiations regarding the Convention on Cybercrime took place not only between members of the Council of Europe. Four non-members (the United States, Canada, South Africa and Japan) were involved in the negotiations, but no representatives of countries from the African or Arab regions.

890 This issue was for example taken into consideration within the EU/ITU co-funded projects HIPCAR and ICB4PAC. The model policy, as well as the model legislation, are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

891 See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf.

892 Regarding the need for an interdisciplinary approach see: *Schjolberg/Ghernaouti-Helie*, A Global Treaty on Cybersecurity and Cybercrime, Second Edition, 2011, page 17, available at: www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf.

893 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

894 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

895 See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf.

896 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

897 See below: § 5.

898 The harmonization of training is one of the main objectives for the EU Cybercrime Centers of Excellence Network (2Centre). Information is available at: www.2centre.eu. Other examples are the European Cybercrime Training & Education Group (ECTEG) as well as the Europol Working Group on the Harmonization of Cybercrime Training (EWGHCT).

899 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

900 The text is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

901 The text is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

[902] See for example: *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, 2007, page 5, available at: www.penal.org/IMG/Guadalajara-Vogel.pdf; *Pladna*, The Lack of Attention in the Prevention of Cyber Crime and How to improve it, University of East Carolina, ICTN6883, available at: www.infosecwriters.com/text_resources/pdf/BPladna_Cybercrime.pdf.

[903] Regarding blocking of websites with illegal content see: *Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 *et seq.*; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008.

[904] The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

[905] Trends in Telecommunication Reform 2009. Hands-On or Hands-Off? Stimulating Industry Growth through Effective ICT Regulation. Summary, page 7, available at: www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.11-2009-SUM-PDF-E.pdf; see also ITU, World Summit on Information Society, The Report of the Task Force on Financial Mechanisms for ICT for Development, December, 2004, available at: www.itu.int/wsis/tffm/final-report.pdf; ITU/infoDEV ICT Regulation Toolkit, Chapter 4.1. What is the Role of Regulators?, available at: www.ictregulationtoolkit.org/en/Section.3109.html

[906] See GSR09 – Best Practice Guidelines on innovative regulatory approaches in a converged world to strengthen the foundation of a global information society, available at www.itu.int; *Macmillian.* Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009 // available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf

[907] *Stevens*, Consumer Protection: Meeting the expectation of connected Consumer. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Consumer-protection_Stevens.pdf; *Macmillian*, Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf.

[908] E.g. Korea Communications Commission, established in February 2008 (formed after consolidating the former Ministry of Information and Communication and the Korean Broadcasting Commission), announced among other core regulatory duties protection of Internet users from harmful or illegal content. Korea Communications Commission: http://eng.kcc.go.kr.

[909] E.g. Swedish ICT Regulator PTS addresses cyberthreats and cybercrime under user protection mandate and network security mandate. See: *PTS*. Secure communications, available at www.pts.se/en-gb/About-PTS/Operations/Secure%20communications/.

[910] *OPTA*. Regulatory areas, available at: www.opta.nl/en/about-opta/regulatory-areas/.

[911] The Dutch regulator is granted the mandate to monitor any contravention of the prohibition of unsolicited communication under its duties to provide Internet safety for consumers.

[912] OPTA has the power to take action against anyone contravening the prohibition of spam and unsolicited software by imposing fines.

[913] OPTA Reaction on the Consultation Concerning the Future of ENISA, 14/01/2009, available at: http://ec.europa.eu/information_society/policy/nis/docs/pub_consult_nis_2009/public_bodies/OPTA.pdf.

[914] *Spyrelli*, Regulating The Regulators? An Assessment of Institutional Structures and Procedural Rules of National Regulatory Authorities, International Journal of Communications Law and Policy, Issue. 8, Winter. 2003/2004; *Henten/ Samarajiva/ Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1, page 26-33; infoDev/ITU ICT regulation Toolkit, available at: www.ictregulationtoolkit.org/en/Section.2033.html.

[915] See the discussions on regulation, illegal content and converged regulators: *Van Oranje et al,* Responding to Convergence: Different approaches for Telecommunication regulators TR-700-OPTA, 30 September 2008, available at: www.opta.nl/download/convergence/convergence-rand.pdf; *Millwood Hargrave, et al,* Issues facing broadcast content regulation, Broadcasting Standards Authority, New Zealand, 2006, available at: www.bsa.govt.nz/publications/IssuesBroadcastContent-2.pdf. See also: *ITU*, Case Study: Broadband, the Case of Malaysia, Document 6, April 2001, available at: www.itu.int/osg/spu/ni/broadband/workshop/malaysiafinal.pdf.

[916] See*: infoDev/ITU* ICT Regulation Toolkit, Chapter 2.5. Convergence and Regulators, available at: www.ictregulationtoolkit.org/en/section.3110.html. See also: *Henten/ Samarajiva/Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1, page 26-33; *Singh/Raja*, Convergence in ICT services: Emerging regulatory responses to multiple play, June 2008, available at:

http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/Convergence_in_ICT_services_Emerging_regulatory_responses_to_multiple_play.pdf; *Garcia-Murillo*, Regulatory responses to convergence: experiences from four countries, Info, 2005, Volume 7, Issue 1.

[917] The four states which have regulators that can be regarded as converged regulatory authorities are: Finland, Italy, Slovenia and the United Kingdom. See: infoDev/ITU ICT Regulation Toolkit, Chapter 2.5. Convergence and Regulators, available at: www.ictregulationtoolkit.org/en/section.3110.html.

[918] Information and network security (INS).

[919] See: *MCMC*, What do we Do. Information Network Security, available at: www.skmm.gov.my/what_we_do/ins/feb_06.asp.

[920] Korea Communications Commission: Important Issues, available at: http://eng.kcc.go.kr.

[921] Trends in Telecommunication Reform 2009. Hands-On or Hands-Off? Stimulating Industry Growth through Effective ICT Regulation. Summary. 2009, P. 11, available at: www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.11-2009-SUM-PDF-E.pdf.

[922] See: *Haggard/McCubbins*, Presidents, Parliaments, and Policy. University of California, San Diego, July 1999, available at: http://mmccubbins.ucsd.edu/ppp.pdf. For the discussion with regard to regulatory agencies, see: *Maggetti*, The Role of Independent Regulatory Agencies in Policy-Making: a Comparative Analysis of Six Decision-Making Processes in the Netherlands, Sweden and Switzerland. IEPI, University of Lausanne, available at: http://regulation.upf.edu/ecpr-07-papers/mmaggetti.pdf.

[923] The rationale for separating the ICT regulator from the policy-making body is to have an independent regulator that maintains a distance from the ministry or other government bodies which could remain as the major shareholder of the incumbent. An independent regulator can avoid conflict of interest that can happen if the regulator is also responsible for industry promotion. See: *OECD*, Telecommunications Regulatory Structures and Responsibilities, DSTI/ICCP/TISP(2005)6/FINAL, January, 2006, available at: www.oecd.org/dataoecd/56/11/35954786.pdf.

[924] InfoDev ITU ICT Regulation toolkit. Section 6.3. Separation of Power and Relationship of Regulator with Other Entities, available at: www.ictregulationtoolkit.org/en/Section.1269.html.

[925] Public Consultation Processes. InfoDev ITU ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/En/PracticeNote.756.html; *Labelle*, ICT Policy Formulation and e-strategy development, 2005, available at: www.apdip.net/publications/ict4d/ict4dlabelle.pdf.

[926] One example is the Botswana Telecommunications Authority, which is required to provide the input to government policy-making efforts. See: Case Study Single Sector Regulator: Botswana Telecommunications Authority (BTA). InfoDev ITU ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/en/PracticeNote.2031.html.

[927] International CIIP Handbook 2008/2009, Center for Security Studies, ETH, Zurich, 2009, available at www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663, P. 133.

[928] National Information Security Strategy Proposal, November, 2002 // available at: www.mintc.fi/fileserver/national_information_security_strategy_proposal.pdf.

[929] *Lie / Macmilian*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

[930] See: *Uganda Communications Commission*, Recommendations on Proposed Review of the Telecommunications Sector Policy, 2005, available at: www.ucc.co.ug/UgTelecomsSectorPolicyReview_31_Jan_2005.pdf; *Blythe*, The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control in Repositioning African Business and Development for the 21st Century, Simon Sigué (Ed.), 2009, available at: www.iaabd.org/2009_iaabd_proceedings/track16b.pdf; Uganda Computer Misuse Bill 2004, available at: www.sipilawuganda.com/files/computer%20misuse%20bill.pdf.

[931] See, for example: Report of the Second EAC Regional Taskforce Meeting on Cyber Laws. June 2008, Kampala, Uganda, available at: http://r0.unctad.org/ecommerce/event_docs/kampala_eac_2008_report.pdf.

[932] Now: Zambia Information and Communications Technology Authority.

[933] *Mukelabai*, Cybersecurity Efforts in Zambia. Presentation at ITU Regional Cybersecurity Forum for Africa and Arab States 4th – 5th June 2009 Tunis, Tunisia, available at: www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mukelabai-caz-

zambia-lusaka-aug-08.pdf; *Hatyoka*, ZICTA Corner – Defining ZICTA's new mandate. Times of Zambia, 2009 // available at: www.times.co.zm/news/viewnews.cgi?category=12&id=1262768483.

934 Zambia Electronic Communications and Transactions Act 2009, available at: www.caz.zm/index.php?option=com_docman&Itemid=75. See also ZICTA. Cybercrime Penalties (Part 1), available at: www.caz.zm/index.php?option=com_content&view=article&id=76:cyber-crime-penalties-part-1&catid=34:column&Itemid=38.

935 Annual report 2008 Belgian Institute for postal service and telecommunication, BIPT, 2009, available at: http://bipt.be/GetDocument.aspx?forObjectID=3091&lang=en.

936 See: *Killcrece, et al,* Organizational Models for Computer Security Incident Response Teams (CSIRTs). Handbook, December, 2003, available at: www.cert.org/archive/pdf/03hb001.pdf.

937 *Scarfone/Grance/Masone,* Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-61, 2008, available at: http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf, pp. 2-2.

938 www.ficora.fi/.

939 Sweden's IT Incident Centre (Sitic) is located in the ICT regulator PTS .See: PTS. Secure communications, available at: www.pts.se/en-gb/About-PTS/Operations/Secure%20communications/.

940 aeCERT created as an initiative of the UAE Telecommunications Regulatory Authority to detect, prevent and respond to current and future cybersecurity incidents in the UAE *: Bazargan*, A National Cybersecurity Strategy aeCERT Roadmap. Presentation at Regional Workshop on Frameworks for Cybersecurity and CIIP 18 – 21 Feb 2008 Doha, Qatar, available at: www.itu.int/ITU-D/cyb/events/2008/doha/docs/bazargan-national-strategy-aeCERT-doha-feb-08.pdf.

941 The national CERT (qCERT) was established by the Qatari ICT regulator (ictQatar) and acts on behalf of ictQatar; *Lewis*, Q-CERT. National Cybersecurity Strategy Qatar, available at: www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/lewis-Q-CERT-incid ent-management-brisbane-july-08.pdf.

942 *Time.lex.* Study on activities undertaken to address threats that undermine confidence in the information society, such as spam, spyware and malicious software. SMART 2008/ 0013, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf.

943 E.g. ICT regulators are involved in law-enforcement efforts with regard to combating spam in the following countries: Australia, Finland, Greece, Hungary, Japan, Malaysia, Mexico, Netherlands, Portugal, Turkey. See: *OECD* Task Force on Spam. Enforcement authorities contact list, available at: www.oecd-antispam.org/countrycontacts.php3.

944 *Time.lex.* Study on activities undertaken to address threats that undermine confidence in the information society, such as spam, spyware and malicious software. SMART 2008/ 0013, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf. Page 21.

945 *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141. For an overview of the most important substantive criminal law provisions, see below: § 6.2.

946 See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, page 245 *et. seq*.

947 For an overview of cybercrime-related legislation and its compliance with the standards defined by the Convention on Cybercrime, see the country profiles provided on the Council of Europe website, available at: www.coe.int/cybercrime/. See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No. 3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

948 See below: § 6.2.

949 See below: § 6.2.

950 For an overview of the most relevant challenges in the fight against cybercrime, see above: § 3.1.

951 One possibility to mask identity is the use of anonymous communication services. See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999. Regarding the technical discussion about traceability

and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf. Regarding anonymous file-sharing systems, see: *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Desing, 2005.

952 Regarding legal responses to the challenges of anonymous communication, see below: §§ 6.5.10 and 6.3.11.

953 See above: § 3.2.6.

954 See in this context below: § 6.6.

955 *Casey*, Digital Evidence and Computer Crime, 2004, page 9.

956 *Vaciago*, Digital Evidence, 2012.

957 Regarding the need for formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2.

958 Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq.*

959 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 3. Regarding the early discussion about the use of printouts, see: *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970, page 291 *et seq.*

960 Regarding the transnational dimension of cybercrime, see: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289, available at: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

961 See *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 451 *et seq.*, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page xvii, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

962 See, in this context: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

963 *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2, page 156, available at: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

964 See in this context: *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf.

965 For an introduction to the discussion, see: *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.,* available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

966 *Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4, available at: www.acpr.gov.au/pdf/ACPR_CC3.pdf. Regarding the need for standardization, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Hall/Davis*, Towards Defining the Intersection of Forensic and Information Technology, International Journal of Digital Evidence, Vol. 4, Issue 1; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Forensics, International Journal of Digital Evidence, Vol. 3, Issue 2.

[967] Transaction authentication number – for more information, see: Authentication in an Internet Banking Environment, United States Federal Financial Institutions Examination Council, available at: www.ffiec.gov/pdf/authentication_guidance.pdf.

[968] The ITAN system improves the TAN system. The financial institutions provide the customer with a number of TAN-indexed identity numbers. With regard to each relevant transaction, the online banking system requires a specific ITAN number selected at random from the list of supplied TAN. For more information, see: *Bishop*, Phishing & Pharming: An investigation into online identity theft, 2005, available at: http://richardbishop.net/Final_Handin.pdf.

[969] Regarding various authentication approaches in Internet banking, see: Authentication in an Internet Banking Environment, United States Federal Financial Institutions Examination Council, available at: www.ffiec.gov/pdf/authentication_guidance.pdf.

[970] Regarding approaches to coordinate the cooperation of law-enforcement agencies and Internet service providers in the fight against cybercrime, see the results of the working group established by Council of Europe in 2007. For more information, see: www.coe.int/cybercrime/.

[971] Capacity building is in general defined as the creation of an enabling environment with appropriate policy and legal frameworks, institutional development, including community participation (of women in particular), human resources development and strengthening of managerial systems. In addition, UNDP recognizes that capacity building is a long-term, continuing process, in which all stakeholders participate (ministries, local authorities, non-governmental organizations, user groups, professional associations, academics and others).

[972] At the G8 Conference in Paris in 2000, *Jean-Pierre Chevenement*, the French Minister of Interior, stated: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect". Regarding user-education approaches in the fight against phishing, see: Anti-Phishing Best Practices for ISPs and Mailbox Providers, 2006, page 6, available at: www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, Technical Trends in Phishing Attacks, available at: www.cert.org/archive/pdf/Phishing_trends.pdf. Regarding sceptical views on user education, see: *Görling*, The Myth Of User Education, 2006, available at: www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

[973] Anti-Phishing Best Practices for ISPs and Mailbox Providers, 2006, page 6, available at: www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, "Technical Trends in Phishing Attacks", available at: www.cert.org/archive/pdf/Phishing_trends.pdf.

[974] *Shaw*, Details of anti-phishing detection technology revealed in Microsoft Patent application, 2007, available at: http://blogs.zdnet.com/ip-telephony/?p=2199; Microsoft Enhances Phishing Protection for Windows, MSN and Microsoft Windows Live Customers – Cyota Inc., Internet Identity and MarkMonitor to provide phishing Web site data for Microsoft Phishing Filter and SmartScreen Technology services, 2005, available at: www.microsoft.com/presspass/press/2005/nov05/11-17EnhancesPhishingProtectionPR.mspx.

[975] For a different opinion, see: *Görling*, The Myth Of User Education, 2006, at: www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

[976] At the G8 Conference in Paris in 2000, *Jean-Pierre Chevenement*, the French Minister of Interior, stated: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

[977] "The United States Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack, explained Mark Mershon, acting head of the FBI's New York office." See Heise News, 27.10.2007, available at: www.heise-security.co.uk/news/80152.

[978] Examples of the publication of cybercrime-related data include: Symantec Government Internet Security Threat Report Trends for July–December 06, 2007, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf; Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf.

[979] Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[980] The first defined and still most important communication protocols are: TCP (Transmission Control Protocol) and IP (Internet Protocol). For further information, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

[981] See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the possibilities of network-storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management.

[982] Regarding the need for international cooperation in the fight against cybercrime, see: *Putnam/Elliott*, International Responses to Cyber Crime, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 *et seq.*, available at: http://media.hoover.org/documents/0817999825_35.pdf; Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[983] National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

# 5. Overview of activities of regional and international organizations

**Bibliography (selected):** *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002; *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006; *Callanan/Gercke/De Marco/Dries-Ziekenheiner*, Internet Blocking – Balancing Cybercrime Responses in Democratic Societies, 2009; Committee II Report, 11th UN Congress on Crime Prevention and Criminal Justice, 2005, BKK/CP/19; *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007; *Gercke*, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq; *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010; *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1; *Gercke*, How Terrorist Use the Internet in *Pieth/Thelesklaf/Ivory*, Countering Terrorist Financing, 2009; *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025; *Herlin-Karnell*, Commission v. Council: Some reflections on criminal law in the first pillar, European Public Law, 2007; *Herlin-Karnell,* Recent developments in the area of European criminal law, Maastricht Journal of European and Comparative Law, 2007; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007; *Nilsson* in *Sieber*, Information Technology Crime, page 576; Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace, Tokyo, May 2001; Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.2003/RPM.4/1, No. 14; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009; *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, 2001; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07.

The following chapter will provide an overview of international legislative approaches[984] and the relationship with national approaches.

## 5.1 International approaches

A number of international organizations work constantly to analyse the latest developments in cybercrime and have set up working groups to develop strategies to fight these crimes.

### *5.1.1 The G8*[985]

In 1997, the Group of Eight (G8) established a "Subcommittee[986] on High-tech Crimes", dealing with the fight against cybercrime.[987] During their meeting in Washington DC, United States, the G8 Justice and Home Affairs Ministers adopted ten Principles and a Ten-Point Action Plan to fight high-tech crimes.[988] The Heads of the G8 subsequently endorsed these principles, which include:

- There must be no safe havens for those who abuse information technologies.
- Investigation and prosecution of international high-tech crimes must be coordinated among all concerned states, regardless of where harm has occurred.
- Law-enforcement personnel must be trained and equipped to address high-tech crimes.

In 1999, the G8 specified their plans regarding the fight against high-tech crimes at a Ministerial Conference on Combating Transnational Organized Crimes in Moscow, Russian Federation.[989] They expressed their concerns about crimes (such as child pornography), as well as traceability of transactions and transborder access to stored data. Their communiqué contains a number of principles in the fight against cybercrime that are today found in a number of international strategies.[990]

One of the practical achievements of the work done by expert groups has been the development of an international 24/7-network of contacts requiring participating countries to establish points of contact for transnational investigations that are accessible 24 hours a day, 7 days a week.[991]

At the G8 Conference in Paris, France in 2000, the G8 addressed the topic of cybercrime with a call to prevent lawless digital havens. Already at that time, the G8 connected its attempts for international solutions to the Council of Europe's Convention on Cybercrime (the "Convention on Cybercrime").[992] In 2001, the G8 discussed procedural instruments in the fight against cybercrime at a workshop held in Tokyo,[993] focusing on whether data-retention obligations should be implemented or whether data preservation was an alternative solution.[994]

In 2004, the G8 Justice and Home Affairs Ministers issued a communiqué in which they addressed the need for the creation of global capacities in the fight against criminal uses of the Internet.[995] Again, the G8 took note of the Convention.[996]

During the 2006 meeting in Moscow, the G8 Justice and Home Affairs Ministers discussed issues related to the fight against cybercrime and the issues of cyberspace, and especially the necessity of improving effective counter-measures.[997] The meeting of the G8 Justice and Home Affairs Ministers was followed by the G8 Summit in Moscow, where the issue of cyberterrorism[998] was discussed.[999]

During the 2007 meeting the of the G8 Justice and Interior Ministers in Munich, Germany, the issue of terrorist use of the Internet was further discussed and the participants agreed to criminalize the misuse of the Internet by terrorist groups.[1000] This agreement did not include specific acts that the states should criminalize.

At the 2009 meeting of Justice and Home Affairs Ministers in Rome, Italy, several issues related to cybercrime were discussed. The final declaration states that, in the view of G8, blocking of child pornography websites on the basis of blacklists updated and disseminated by international organizations should be implemented.[1001] With regard to cybercrime in general, the final declaration highlights an increasing threat and points out that closer cooperation between service providers and law enforcement is necessary and that existing forms of cooperation, such as the G8 24/7 High-Tech Crime Points of Contact, need to be strengthened.[1002]

At the G8 Summit in Muskoka, Canada, cybercrime was only briefly discussed. The Muskoka Declaration only states in the context of terrorist activities that the G8 is concerned about the growing threat of cybercrime and will intensify work to weaken terrorist and criminal networks.[1003]

Cybercrime and Cybersecurity were issues that were both discusses at the e-G8 Forum, where delegations discussed Internet-related topics with business leader[1004] as well as the G8 summit in Deauville, France. But although the topic cybercrime received great attention the final declaration of the summit did, unlike in previous years, not contain specific recommendations. The G8 only agreed to general principles such as the importance of security and protection from crime that underpin a strong and flourishing Internet.[1005]

### 5.1.2 United Nations and United Nations Office on Drugs and Crimes[1006]

The United Nations has undertaken several important approaches to address the challenge of cybercrime. While in the beginning its response was limited to general guidelines, the organization has in recent times dealt more intensively with the challenges and legal response.

#### UN Convention on the Rights of the Child

The United Nations Convention on the Rights of the Child, adopted in 1989,[1007] contains several instruments aiming to protect children. It does not define child pornography, nor does it contain

provisions that harmonize the criminalization of the distribution of online child pornography. However, Article 34 calls upon Member States to prevent the exploitative use of children in pornographic performances.

### UN General Assembly Resolution 45/121

After the eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (held in Havana, Cuba, 27 August – 7 September 1990), the UN General Assembly adopted a resolution dealing with computer-crime legislation.[1008] Based on its Resolution 45/121 (1990), the UN published a manual in 1994 on the prevention and control of computer-related crime.[1009]

### Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography

The Optional Protocol not only addresses the issue of child pornography in general, but explicitly refers to the role of the Internet in distributing such material.[1010] Child pornography is defined as any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.[1011] Article 3 requires the parties to criminalize certain conduct – including acts related to child pornography.

> ***Article 3***
> *1. Each State Party shall ensure that, as a minimum, the following acts and activities are fully covered under its criminal or penal law, whether these offences are committed domestically or transnationally or on an individual or organized basis:*
> *[...]*
> *(c) Producing, distributing, disseminating, importing, exporting, offering, selling or possessing for the above purposes child pornography as defined in Article 2.*
> *[...]*

### Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders

During the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in Vienna in 2000, the impact of computer-related crimes was discussed in a specific workshop.[1012] The debate focused especially on the categories of crime and transnational investigation, as well as legal response to the phenomenon.[1013] The conclusions of the workshop contain major elements of the debate that is still ongoing: criminalization is required, legislation needs to include procedural instruments, international cooperation is crucial and public-private partnership should be strengthened.[1014] In addition, the importance of capacity building was highlighted – an issue that was picked up again in subsequent years.[1015] The Vienna Declaration called upon the Commission on Crime Prevention and Criminal Justice to undertake work in this regard:

> *18. We decide to develop action-oriented policy recommendations on the prevention and control of computer- related crime, and we invite the Commission on Crime Prevention and Criminal Justice to undertake work in this regard, taking into account the ongoing work in other forums. We also commit ourselves to working towards enhancing our ability to prevent, investigate and prosecute high-technology and computer-related crime.*

### UN General Assembly Resolution 55/63

In the same year, the UN General Assembly adopted a resolution on combating the criminal misuse of information technologies which displays a number of similarities with the G8's Ten-Point Action Plan from 1997.[1016] In its resolution, the General Assembly identified a number of measures to prevent the misuse of information technology, including:

*States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;*
*Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;*
*Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;*

Resolution 55/63 invites States to take the necessary steps to combat cybercrime on the regional and international stage. This includes the development of domestic legislation to eliminate safe havens for criminal misuse of technologies, improving law-enforcement capacities to cooperate across borders in the investigation and prosecution of international cases of criminal misuse of information technologies, improving information exchange, enhancing the security of data and computer systems, training law enforcement to deal specifically with the challenges associated with cybercrime, building mutual assistance regimes and raising public awareness of the threat of cybercrime.

### UN General Assembly Resolution 56/121

In 2002, the UN General Assembly adopted another resolution on combating the criminal misuse of information technology.[1017] The resolution refers to the existing international approaches in fighting cybercrime and highlights various solutions.

*Noting the work of international and regional organizations in combating high-technology crime, including the work of the Council of Europe in elaborating the Convention on Cybercrime as well as the work of those organizations in promoting dialogue between government and the private sector on safety and confidence in cyberspace,*
*1. Invites Member States, when developing national law, policy and practice to combat the criminal misuse of information technologies, to take into account, as appropriate, the work and achievements of the Commission on Crime Prevention and Criminal Justice and of other international and regional organizations;*
*2. Takes note of the value of the measures set forth in its resolution 55/63, and again invites Member States to take them into account in their efforts to combat the criminal misuse of information technologies;*
*3. Decides to defer consideration of this subject, pending work envisioned in the plan of action against high-technology and computer-related crime of the Commission on Crime Prevention and Criminal Justice*

Resolution 56/121 underlines the need for cooperation among states in combating the criminal misuse of information technologies. It highlights the role that can be played by the United Nations and other international and regional organizations. The resolution further invites states to take into account the direction provided by the Commission on Crime Prevention and Criminal Justice when developing national legislation.

### UN General Assembly Resolutions 57/239 and 58/199

Resolutions 57/239 and 58/199 are the two main UN General Assembly resolutions dealing with cybersecurity. Without going into detail with regard to cybercrime, they recall Resolutions 55/06 and 56/121. Both resolutions furthermore emphasize the need for international cooperation in fighting cybercrime by recognizing that gaps in states' access to and use of information technologies can diminish the effectiveness of international cooperation in combating the criminal misuse of information technology.[1018]

### Eleventh UN Congress on Crime Prevention and Criminal Justice

Cybercrime was discussed during the eleventh UN Congress on Crime Prevention and Criminal Justice (the "UN Crime Congress") in Bangkok, Thailand, in 2005. Several challenges associated with the emerging use of computer systems in committing offences and the transnational dimension were addressed both in the

background paper[1019] and in workshops.[1020] Within the framework of the preparatory meetings in advance of the congress, some member countries such as Egypt called for a new UN convention against cybercrime, and the Western Asian regional preparatory meeting called for the negotiation of such convention.[1021] The possibility of negotiating a convention was included in the discussion guide for the eleventh UN Crime Congress.[1022] However, the Member States could at this time not decide to initiate a harmonization of legislation. The Bangkok Declaration therefore – without mentioning a specific instrument – refers to existing approaches.

> *16. We note that, in the current period of globalization, information technology and the rapid development of new telecommunication and computer network systems have been accompanied by the abuse of those technologies for criminal purposes. We therefore welcome efforts to enhance and supplement existing cooperation to prevent, investigate and prosecute high-technology and computer-related crime, including by developing partnerships with the private sector. We recognize the important contribution of the United Nations to regional and other international forums in the fight against cybercrime and invite the Commission on Crime Prevention and Criminal Justice, taking into account that experience, to examine the feasibility of providing further assistance in that area under the aegis of the United Nations in partnership with other similarly focused organizations.*

### UN General Assembly Resolution 60/177

After the eleventh UN Congress on Crime Prevention and Criminal Justice in Bangkok, Thailand, in 2005, a declaration was adopted that highlighted the need for harmonization in the fight against cybercrime,[1023] addressing, among others, the following issues:

> *We reaffirm the fundamental importance of implementation of existing instruments and the further development of national measures and international cooperation in criminal matters, such as consideration of strengthening and augmenting measures, in particular against cybercrime, money-laundering and trafficking in cultural property, as well as on extradition, mutual legal assistance and the confiscation, recovery and return of proceeds of crime.*
> *We note that, in the current period of globalization, information technology and the rapid development of new telecommunication and computer network systems have been accompanied by the abuse of those technologies for criminal purposes. We therefore welcome efforts to enhance and supplement existing cooperation to prevent investigate and prosecute high-technology and computer-related crime, including by developing partnerships with the private sector. We recognize the important contribution of the United Nations to regional and other international forums in the fight against cybercrime and invite the Commission on Crime Prevention and Criminal Justice, taking into account that experience, to examine the feasibility of providing further assistance in that area under the aegis of the United Nations in partnership with other similarly focused organizations.*

UN General Assembly Resolution 60/177 endorsed the 2005 Bangkok Declaration, wherein the international community's efforts to enhance and supplement existing cooperation to prevent computer-related crime were encouraged, inviting further exploration of the feasibility of providing assistance to Member States in addressing computer-related crime under the aegis of the United Nations, and in partnership with other similarly focused organizations.

### Twelfth UN Congress on Crime Prevention and Criminal Justice

The topic of cybercrime was also discussed at the twelfth UN Congress on Crime Prevention and Criminal Justice held in Brazil in 2010.[1024] Within the four regional preparatory meetings for the congress, for Latin America and Caribbean,[1025] Western Asia,[1026] Asia and the Pacific[1027] and Africa,[1028] the countries called for the development of an international convention on cybercrime. Similar calls were raised within academia.[1029]

At the congress itself, Member States took a major step toward more active involvement of the United Nations in the debate on the issue of computer crime and cybercrime. The fact that the delegations discussed the topics for two days and that additional side events were organized highlights the

importance of the topic, which was more intensively discussed than during the previous crime congresses.[1030] The deliberations focused on two main issues: how can harmonization of legal standards be achieved, and how can developing countries be supported in fighting cybercrime? The first point is especially relevant if the UN develops comprehensive legal standards or suggests that Member States implement the Council of Europe Convention on Cybercrime. In preparation of the UN Crime Congress, the Council of Europe had expressed concerns regarding a UN approach[1031] and had called for support for its Convention on Cybercrime. After an intensive debate, where the limited reach of the Convention on Cybercrime was discussed in particular, the Member States decided not to suggest to ratify the Convention on Cybercrime but to strengthen the UN's role in two important areas, which are reflected in the Salvador Declaration:

> *41. We recommend that the United Nations Office on Drugs and Crime, upon request, provide, in cooperation with Member States, relevant international organizations and the private sector, technical assistance and training to States to improve national legislation and build the capacity of national authorities, in order to deal with cybercrime, including the prevention, detection, investigation and prosecution of such crime in all its forms, and to enhance the security of computer networks.*
> *42. We invite the Commission on Crime Prevention and Criminal Justice to consider convening an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.*

The Member States thus recommended a strong mandate for the United Nations Office on Drugs and Crimes (UNODC) to provide global capacity building upon request. Taking into account UNODC's experience in capacity building related to criminal legislation and the fact that, unlike the Council of Europe, UNODC provides a global network of regional offices, it is likely that UN through UNODC will play a more important role in this field in the future.

The second recommendation highlights that, at the time of the UN Crime Congress, Member States were unable to decide whether to develop a legal text or not. This reflects the controversial discussion during the congress, where those European countries that have already ratified the Convention on Cybercrime, in particular, expressed their support for that instrument while a number of developing countries called for a UN convention. However, the Member States did respond differently than at the eleventh Crime Congress, where they had referred to existing instruments. This time they did not refer to existing instruments and, even more importantly, they did not decide to recommend the Convention on Cybercrime as a global standard. Instead, the Member States recommended to invite the Commission on Crime Prevention and Criminal Justice to conduct a comprehensive study, which should, *inter alia*, examine options for strengthening existing and proposing new national and international legal or other responses to cybercrime.

### UN General Assembly Resolution 64/211

In March 2010, the UN General Assembly passed a new resolution[1032] as part of the "Creation of a global culture of cybersecurity" initiative. Resolution 64/211 refers to the two major resolutions on cybercrime[1033] as well as the two main resolutions on cybersecurity.[1034] The voluntary self-assessment tool for national efforts to protect critical information infrastructures provided as an annex to the resolution calls for countries to review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of, and dependence upon, new information and communication technologies. The resolution further calls on states to use regional international conventions, arrangements and precedents in these reviews.

*13. Review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communications technologies, and use regional and international conventions, arrangements and precedents in these reviews. Ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, General Assembly resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies, and regional initiatives, including the Council of Europe Convention on Cybercrime.*
*14. Determine the current status of national cybercrime authorities and procedures, including legal authorities and national cybercrime units, and the level of understanding among prosecutors, judges and legislators of cybercrime issues.*
*15. Assess the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and of cyberspace more generally.*
*16. Examine national participation in international efforts to combat cybercrime, such as the round-the-clock Cybercrime Point of Contact Network.*
*17. Determine the requirements for national law enforcement agencies to cooperate with international counterparts to investigate transnational cybercrime in those instances in which infrastructure is situated or perpetrators reside in national territory, but victims reside elsewhere.*

The fact that four out of 18 subjects of the self-assessment tool are related to cybercrime highlights the importance of the ability of law enforcement to combat cybercrime effectively for maintaining cybersecurity.

### Intergovernmental Expert Group on Cybercrime

Following the decision of the Member States to call upon UNODC to set up an intergovernmental working group, the first meeting of the group was held in Vienna in January 2011.[1035] The expert group included representatives of Member States, intergovernmental and international organizations, specialized agencies, private sector and academia. During the meeting the members of the expert group discussed a draft structure for a comprehensive study analysing the issue of cybercrime, as well as the response.[1036] With regard to the legal response, a number of members underline the usefulness of existing international legal instruments, including the United Nations Convention against Transnational Organized Crime (UNTOC) and the Council of Europe Convention on Cybercrime, and the desirability of elaborating a global legal instrument to address specifically the problem of cybercrime. It was agreed that the decision on whether a global instrument should be developed will be made after the study was conducted.

### Other resolutions and activities

In addition, a number of United Nations system decisions, resolutions and recommendations address issues related to cybercrime, the most important being the following: the United Nations Office for Drugs and Crime (UNODC) and the Commission on Crime Prevention and Criminal Justice[1037] adopted a resolution on effective crime prevention and criminal justice responses to combat sexual exploitation of children.[1038] In 2004, the United Nations Economic and Social Council[1039] adopted a resolution on international cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.[1040] A working group was established in 2005.[1041] A core group of experts on identity-related crime was created to undertake a comprehensive study on the issue. In 2007, the ECOSOC adopted a resolution on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.[1042] Neither of these two resolutions explicitly addresses the challenges of Internet-related crimes,[1043] but they are applicable to those offences as well. Based on ECOSOC Resolution 2004/26[1044] and ECOSOC Resolution 2007/20,[1045] UNODC in 2007 established a core group of experts to exchange views on the best course of action.[1046] The core group has undertaken several studies that included aspects of Internet-related crimes.[1047] In 2004, ECOSOC had adopted a resolution on the sale of licit drugs via the Internet that explicitly took account of a phenomenon related to a computer crime.[1048]

### UNODC/ITU Memorandum of Understanding

In 2011 UNODC and the International Telecommunication Union (ITU) signed a memorandum of understanding related to cybercrime.[1049] The MoU covers cooperation (especially capacity building and technical assistance for developing countries), training and joint workshops. With regard to the capacity building activities the two organizations can refer to a wide network of field offices in all continents. Further more the organizations agreed to a joined dissemination of information and knowledge and data analysis.

## 5.1.3 International Telecommunication Union[1050]

The International Telecommunication Union (ITU), as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications as well as cybersecurity issues.

### World Summit on the Information Society

Among other activities, ITU was the lead agency of the World Summit on the Information Society (WSIS) that took place in two phases in Geneva, Switzerland (2003) and in Tunis, Tunisia (2005). Governments, policy-makers and experts from around the world shared ideas and experiences about how best to address the emerging issues associated with of the development of a global information society, including the development of compatible standards and laws. The outputs of the Summit are contained in the *Geneva Declaration of Principles*, the *Geneva Plan of Action*; the *Tunis Commitment* and the *Tunis Agenda for the Information Society*.

The Geneva Plan of Action highlights the importance of measures in the fight against cybercrime:[1051]

> ***C5.Building confidence and security in the use of ICTs***
> *12. Confidence and security are among the main pillars of the Information Society.*
> *[…]*
> *b. Governments, in cooperation with the private sector, should prevent, detect and respond to cyber-crime and misuse of ICTs by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of misuse; promoting effective mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness.*
> *[…]*

Cybercrime was also addressed at the second phase of WSIS in Tunis in 2005. The Tunis Agenda for the Information Society[1052] highlights the need for international cooperation in the fight against cybercrime and refers to the existing legislative approaches such as the UN General Assembly resolutions and the Council of Europe Convention on Cybercrime:

> *40. We underline the importance of the prosecution of cybercrime, including cybercrime committed in one jurisdiction, but having effects in another. We further underline the necessity of effective and efficient tools and actions, at national and international levels, to promote international cooperation among, inter alia, law-enforcement agencies on cybercrime. We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime.*

### Global Cybersecurity Agenda

As an outcome of WSIS, ITU was nominated as the sole facilitator for Action Line C5 dedicated to building of confidence and security in the use of information and communication technology.[1053] At the second Facilitation Meeting for WSIS Action Line C5 in 2007, the ITU Secretary-General highlighted the importance of international cooperation in the fight against cybercrime and announced the launch of the *ITU Global Cybersecurity Agenda*.[1054] The Global Cybersecurity Agenda is made up of seven key goals,[1055] and built upon five strategic pillars[1056], including the elaboration of strategies for the development of model cybercrime legislation. The seven goals are the following:

*1 Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures.*
*2 Elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime.*
*3 Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for software applications and systems.*
*4 Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives.*
*5 Development of strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries.*
*6 Development of a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and in all the above-mentioned areas.*
*7 Advice on potential framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.*

In order to analyse and develop measure and strategies with regard to the seven goals of the GCA, the ITU Secretary-General created a high-level expert group (HLEG) bringing together representatives from Member States, industry as well as the scientific field.[1057] In 2008, the expert group concluded negotiations and published the "Global Strategic Report".[1058] Most relevant with regard to cybercrime are the legal measures contained in Chapter 1. In addition to an overview of different regional and international approaches in fighting cybercrime,[1059] the chapter provides an overview of criminal law provisions,[1060] procedural instruments,[1061] regulations governing the responsibility of Internet service providers[1062] and safeguards to protect fundamental rights of Internet users.[1063]

### Capacity building

Under the umbrella of the ITU GCA, ITU-D works to assist countries in implementing harmonized cybersecurity-related activities at the national, regional and international level. ITU's mandate in capacity building was emphasized by Resolution 130 (Rev. Guadalajara, 2010) of the ITU Plenipotentiary Conference. Based on the resolution, ITU has the mandate to assist Member States, in particular developing countries, in the elaboration of appropriate and workable legal measures relating to protection against cyberthreats.

This includes capacity-building activities in the development of national strategies, legislation and enforcement, organizational structures (e.g. watch, warning and incident response), among other areas. ITU has organized several regional conferences which have specifically addressed, *inter alia*, the issue of cybercrime.[1064] Together with partners from the public and private sectors, ITU-D has developed cybersecurity/CIIP tools to assist Member States in raising national awareness, conducting national cybersecurity self-assessments, revising legislation and expanding watch, warning and incident-response capabilities. These tools include Understanding Cybercrime: A Guide for Developing Countries, the ITU National Cybersecurity/CIIP Self-Assessment Tool and the ITU Botnet Mitigation Toolkit.

#### Resolutions

ITU has adopted several cybersecurity-related resolutions that are relevant to cybercrime, while not directly addressing the issue with specific criminal law provisions.

- ITU Plenipotentiary Conference Resolution 130 (Rev. Guadalajara, 2010), on Strengthening the role of ITU in building confidence and security in the use of information and communication technologies.
- ITU Plenipotentiary Conference Resolution 149 (Antalya, 2006), on Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies.
- Resolution 45 (Doha, 2006) of the World Telecommunication Development Conference (WTDC), on Mechanisms for enhancing cooperation on cybersecurity, including combating spam and the report from *Meeting on Mechanisms for Cooperation on Cybersecurity and Combating Spam* (31 August – 1 September 2006).
- Resolution 50 (Rev. Johannesburg, 2008) of the World Telecommunication Standardization Assembly (WTSA), on Cybersecurity.
- Resolution 52 (Rev. Johannesburg, 2008) of the World Telecommunication Standardization Assembly (WTSA), on Countering and combating spam.
- Resolution 58 (Johannesburg, 2008) of the World Telecommunication Standardization Assembly (WTSA), on Encouraging the creation of national computer incident response teams, particularly for developing countries.

## 5.2 Regional approaches

In addition to the international organizations that are globally active, a number of international organizations that focus of specific regions have move forward on activities that deal with issues related to cybercrime.

### *5.2.1 Council of Europe*[1065]

The Council of Europe is playing an active role in addressing the challenges of cybercrime.

#### Activities until 1995

In 1976, the Council of Europe highlighted the international nature of computer-related crimes and discussed the topic at a conference dealing with aspects of economic crimes. This topic has since remained on its agenda.[1066] In 1985, the Council of Europe appointed an Expert Committee[1067] to discuss the legal aspects of computer crimes.[1068] In 1989, the European Committee on Crime Problems adopted the "Expert Report on Computer-Related Crime",[1069] analysing the substantive criminal legal provisions necessary to fight new forms of electronic crimes, including computer fraud and forgery. The Committee of Ministers in 1989 adopted a recommendation[1070] that specifically highlighted the international nature of computer crime:

> *The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe, Considering that the aim of the Council of Europe is to achieve a greater unity between its members; Recognising the importance of an adequate and quick response to the new challenge of computer-related crime; Considering that computer-related crime often has a transfrontier character; Aware of the resulting need for further harmonisation of the law and practice, and for improving international legal co-operation, Recommends the governments of member states to :*
>
> *1. Take into account, when reviewing their legislation or initiating new legislation, the report on computer-related crime elaborated by the European Committee on Crime Problems, and in particular the guidelines for the national legislatures;*

> *2. Report to the Secretary General of the Council of Europe during 1993 on any developments in their legislation, judicial practice and experiences of international legal co-operation in respect of computer-related crime.*

In 1995, the Committee of Ministers adopted another recommendation dealing with the problems arising from transnational computer crimes.[1071] Guidelines for the drafting of adequate legislation were summarized in the Appendix to the Recommendation.[1072]

### Council of Europe Convention on Cybercrime and the Additional Protocol

The European Committee on Crime Problems (CDPC) decided in 1996 to set up a committee of experts to deal with cybercrime.[1073] The idea of going beyond principles for another recommendation and drafting a convention was present at the time of the establishment of the Committee of Experts.[1074] Between 1997 and 2000, the committee held ten meetings in plenary and fifteen meetings of its open-ended Drafting Group. The Assembly adopted the draft Convention on Cybercrime in the second part of its plenary session in April 2001.[1075] The finalized draft Convention was submitted for approval to CDPC and to the Committee of Ministers for adoption and opening for signature.[1076] The Convention on Cybercrime was opened for signature at a signing ceremony in Budapest on 23 November 2001, during which 30 countries signed the Convention on Cybercrime (including four non-members of the Council of Europe – Canada, United States, Japan and South Africa – that participated in the negotiations). By April 2012, 47 states[1077] have signed and 33 states[1078] have ratified[1079] the Council of Europe Convention on Cybercrime. In the meantime seven states were invited to accede to the Convention on Cybercrime, but have not done so.[1080] The Convention on Cybercrime is today recognized as an important regional instrument in the fight against cybercrime and is supported by different international organizations.[1081]

The Convention on Cybercrime was followed by the First Additional Protocol to the Convention on Cybercrime.[1082] During the negotiations on the text of the Convention on Cybercrime, it turned out that the criminalization of racism and the distribution of xenophobic material were particularly controversial matters.[1083] Some countries in which the principle of freedom of expression[1084] was strongly protected expressed their concern that if provisions are included in the Convention on Cybercrime that violate freedom of expression they would be unable to sign the Convention.[1085] In the fourth draft version from 1998, the Convention still included a provision that required the parties to criminalize illegal content "concerning in particular matters such as child pornography and racial hatred".[1086] To avoid a situation where countries would not be able to sign the Convention because of freedom of expression concerns, those issues were removed from the Convention on Cybercrime during the drafting process and integrated into a separate protocol. By January 2012, 35 states[1087] have signed and 20 states[1088] have ratified the Additional Protocol.

### Debate about the Council of Europe Convention on Cybercrime

Currently, the Council of Europe Convention on Cybercrime is still the instrument with the broadest reach supported by different international organizations.[1089] However, the debate in the twelfth Crime Congress highlighted that ten years after its opening for signature, the impact of the Convention is limited.[1090]

### Limitation of reach of the Council of Europe Convention on Cybercrime

As of Januar 2011, the United States is the only country outside Europe that has ratified the instrument. It is true that the impact of the Convention cannot be measured solely by the number of signatures or ratifications, since countries such as Argentina,[1091] Pakistan,[1092] Philippines,[1093] Egypt,[1094] Botswana[1095] and Nigeria[1096] have used the Convention as a model and drafted parts of their legislation in accordance with the Convention on Cybercrime without formally acceding to it. Even in the case of those countries, however, it is uncertain to what extent they have used the Convention on Cybercrime as a model. Some of them have also used other law texts, such as the EU Directive on Attacks against Information Systems and the Commonwealth Model Law. Since those laws display a number of similarities to the Convention on Cybercrime and, in addition, provisions have very rarely been reproduced word for word, but have

been adjusted to the countries' requirements, this makes it nearly impossible to determine if and to what extent a country has used the Convention as a guideline. Despite this, the Council of Europe claims that more than 100 countries have either signed, ratified or used the Convention when drafting domestic legislation.[1097] However, this number could not be verified. The Council of Europe does not disclose the names of the countries concerned, and only refers to an "internal list". Not even the precise number of countries is disclosed. Even if it were possible to prove that 100 countries have used the Convention on Cybercrime, this does not necessarily mean that they have harmonized their legislation in line with the Convention. The rather vague information published by the Council of Europe also leaves open the question of whether all provisions from the Convention on Cybercrime have been implemented, or only one.

### Speed of the ratification process

The limited territorial reach was not the only concern discussed at the twelfth UN Crime Congress. The speed of signature and ratification certainly remains an issue. Nine years after the initial signature by 30 states on 23 November 2001, only 17 further states have signed the Convention on Cybercrime. In this time, no non-member of the Council of Europe has acceded to the Convention, although eight countries were invited.[1098] The number of ratifications has evolved as follows: 2002 ($2^{1099}$), 2003 ($2^{1100}$), 2004 ($4^{1101}$), 2005 ($3^{1102}$), 2006 ($7^{1103}$), 2007 ($3^{1104}$), 2008 ($2^{1105}$), 2009 ($3^{1106}$), 2010 ($4^{1107}$) and in 2011 ($2^{1108}$). As slow as the ratification process is the implementation process. In average it takes a country more than five years between signature and ratification of the Convention. The differences between the countries are significant. While it took Albania only a bit more than half a year to ratify the convention Germany needed almost ten years.

### No evaluation of the ratification

The Council of Europe has so far never evaluated whether those countries that have submitted their ratification instrument have actually implemented the Convention on Cybercrime in accordance with the requirements. Especially in the case of the first countries that ratified the Convention, there are serious concerns with regard to its full implementation. Even in large countries such as Germany and the United States, it is unlikely that the Convention has been fully implemented. Germany, for example, contrary to the intent of Article 2 of the Convention on Cybercrime, does not criminalize illegal access to computer systems, but only illegal access to computer data.[1109] The country profile of the US cybercrime legislation posted on the Council of Europe website indicates that 18 USC. § 1030(a)(1) – (5) corresponds to Article 2.[1110] Unlike Article 2 of the Convention on Cybercrime, however, 18 USC § 1030(a) does not criminalize mere access to a computer system. In addition to "access" to a computer system, the provision requires further acts (like for example "obtaining" information).[1111]

### Global debate

One frequently criticized aspect of the Convention on Cybercrime is the inadequate representation of developing countries in the drafting process.[1112] Despite the transnational dimension of cybercrime, its impact in the different regions of the world is different. This is especially relevant for developing countries.[1113] Not only was the Convention on Cybercrime negotiated without any broad involvement of developing countries in Asia, Africa and Latin America, but it also places restrictive conditions on the participation of non-members of the Council of Europe, even though it was designed to be open to non-members. Based on Article 37 thereof, accession to the Convention on Cybercrime requires consulting with and obtaining the unanimous consent of the contracting states to the Convention on Cybercrime. In addition, participation in the deliberations on possible future amendments is restricted to parties to the Convention.[1114] The debate within the framework of preparation of the twelfth UN Crime Congress showed that developing countries in particular are interested in an international approach rather than joining regional initiatives. During the regional preparatory meetings for the twelfth United Nations Congress on Crime Prevention and Criminal Justice for Latin America and Caribbean[1115], Western Asia[1116], Asia and Pacific[1117] and Africa,[1118] countries called for the development of an international convention on cybercrime. Similar calls were raised within academia.[1119]

### Lack of response to recent trends

Cybercrime is an area of crime that is constantly changing.[1120] In the 1990s, when the Convention on Cybercrime was developed, terrorist use of the Internet[1121], botnet attacks[1122] and phishing[1123] either were not known or did not play as important a role as they do today,[1124] and could therefore not be addressed with specific solutions. Even the Council of Europe has recognized that the Convention on Cybercrime is partly out of date. This can be demonstrated by comparing the provisions relating to child pornography in the 2001 Convention on Cybercrime and the 2007 Convention on the Protection of Children. Article 20 (1)(f) of the Convention on the Protection of Children criminalizes "knowingly obtaining access, through information and communication technologies, to child pornography". This act is not criminalized by the Convention on Cybercrime, although the reference to ICTs underlines that it is a crime that can be characterized as cybercrime. Based on the motivation provided in the Explanatory Report, the drafters decided to include this provision to cover cases where offenders view child images online by accessing child-pornography sites but without downloading material. This means, as a consequence, that the Convention on Cybercrime does not cover such acts and therefore in this regard does not even meet the Council of Europe's own current standards.

The same is true with regard to procedural instruments. Interception of voice-over-IP (VoIP) communication, the admissibility of digital evidence and procedures to deal with the emerging use of encryption technology and means of anonymous communication are issues that are of great relevance to, but not addressed by, the Convention on Cybercrime. In its ten years of existence, the Convention has never been amended and, apart from the Additional Protocol on xenophobic material, no additional provisions or instruments have been added.

With changing technologies and criminal behaviour, criminal law needs to be adjusted. As pointed out before, requirements in terms of cybercrime legislation have changed in the last ten years. An update of the Convention on Cybercrime would therefore be highly necessary. Other regional organizations, such as the European Union, have just reviewed their legal instruments addressing cybercrime, which were introduced more recently, around five years ago. Despite the urgency of an update, it is unlikely that such a process will take place. The European Union, a strong supporter of the Convention on Cybercrime, declared recently that in its view "updating of the Convention [on Cybercrime] [...] cannot be considered a feasible option".[1125]

### Focus on accession of countries that provide infrastructure instead of developing countries

Within the last ten years that Council of Europe did not succeed to get accessions by small and developing countries. One of the reasons is the fact that the Convention was negotiated with an inadequate representation of developing countries.[1126] Especially Asia and Africa were underrepresented and Latin America was not represented at all. Although the Council of Europe invites representatives from developing countries to it's main Cybercrime conference those countries are not allowed to participate in in the deliberations on possible future amendments as those meetings are restricted to parties to the Convention.[1127]

Differences compared to truly international instruments such as UN conventions can also be observed when it comes to the accession process. Although the process of becoming part of the Convention – that was designed as open to non-members – restrictive conditions apply. Unlike a UN Convention, the accession to the Convention on Cybercrime requires consultation with and the unanimous consent of the contracting states to the Convention.[1128] Consequently especially the developing countries have started to call for a (more) international approach during the preparation of the 12th UN Crime Congress. Within the regional preparatory meetings for the Congress for Latin America and Caribbean[1129], Western Asia[1130], Asia and Pacific[1131] and Africa,[1132] the participating countries called for the development of such international instrument.

Although the strategy of the Council of Europe to focus on western countries seem logical as they host the infrastructure, the involvement of developing countries is crucial if focus should include potential victims. In 2005, the number of Internet users in developing countries surpassed the number in industrial nations.[1133] By excluding developing countries and focussing instead on developed countries that

(currently) provide most of the infrastructure and services, two crucial aspects are ignored: the importance of protecting the (majority) of users of Internet services, and, secondly, the strongly increasing influence of emerging countries like India, China and Brazil. Without supporting developing countries in establishing legislation that enables them to investigate cases in which their nationals are affected and in addition also to cooperate internationally with other law enforcement units regarding identification of offenders, Cybercrime investigations will be more difficult if they involve those countries. The fact that in the last 10 years no developing country has acceded to the Convention or has ratified it, shows the limitations of a regional approach. Taking further into account that in the last decade the Council of Europe has only invited eight countries (out of 146 UN Member States that have not sign the Convention) to accede to the Convention, highlights the limited energy invested in this regard. This is certainly related to the fact that the needs of developing countries with regard to legislation as well as capacity building and technical assistance in general go beyond the mechanisms of the Convention. Until today the Council of Europe focuses on assisting countries in bringing their legislation in line with the Convention, but does not provide any assistance in drafting legislation that goes beyond the Convention (e.g. to close the above mentioned gaps). Further more the countries might already require help with drafting of national legislation because the provisions contained in the Convention require an adjustment process during the implementation. Countries for example need to determine who is authorized to order a certain investigation (magistrate/prosecutor/police office) and on what basis (sworn evidence/affidavit/information).

This issue was discussed in detail during the 12th UN Crime Congress and led the UN Member States deciding upon strengthening the capacity building mandate of the United Nations Office on Drugs and Crimes (UNODC) in the area of Cybercrime.[1134] Other UN organizations like the International Telecommunications Union (ITU) have recently received similar mandates.[1135]

### Not designed for small and developing countries

Small and developing countries face difficulties in implementing the standards of the Convention. The fact that the smallest Council of Europe Member States did not ratified[1136] the Convention in the last ten years clearly underlines that it is not only challenging for small countries outside of Europe but also small European countries.

One of the provisions that causes difficulties when it comes to the implementation in small countries is the need to establish a 24/7 point of contact. Such contact point can have a highly positive impact on the speed of investigations and Article 35 is consequently one of the most important instruments provided by the Convention.[1137] However, it should be mentioned that recently the Council of Europe has published a study analysing the effectiveness of international cooperation against cybercrime[1138] and a study on the functioning of 24/7 points of contact against cybercrime[1139] and the result of these two studies is that not all countries which have ratified the Convention have established such a contact point even countries which have provided such a contact point often only use it for limited purposes.

The main problem for developing countries is the fact that the establishment of such contact point is mandatory. While for developed countries establishing and maintaining such a contact point will most likely not be challenging utilising a specialized police force dealing with cybercrime in night and day shifts, is however a challenge for countries where the specialized police force dealing with cybercrime consists of only one single police man. In those cases the obligation will require significant investments. That the accession to and implementation of the Convention does not have associated costs for the countries, as was recently stated by a Council of Europe representative at a conference in the Pacific[1140] is therefore only accurate if indirect costs, e.g. for maintaining a 24/7 contact point or for implementing technology to record traffic data in real time, are excluded.

### No comprehensive approach

It was one of the key intentions of the Convention to provide a comprehensive legal approach that addresses all relevant areas of cybercrime.[1141] But comparing the Convention with other approaches – especially the Commonwealth Model Law on Computer and Computer-related Crime[1142] as well as the EU instruments such as the E-Commerce Directive[1143], shows that important aspects are missing. Examples

are provisions dealing with the admissibility of electronic evidence[1144] or with the liability of Internet Service Providers (ISPs). Especially the missing provision of an, at least, basic regulatory framework related to the admissibility of electronic evidence has significant consequences as electronic evidence is widely characterized as a new category of evidence.[1145] And unless a country has other instruments in place or its courts hold such evidence admissible, the country might not be able to sentence any offenders despite having fully implemented the Convention.

#### Convention on the Protection of Children

Within its approach to improve the protection of minors against sexual exploitation, the Council of Europe introduced a new Convention in 2007.[1146] On the first day the Convention on the Protection of Children opened for signature 23 states signed the Convention. By April 2012, it had 42 signatory states,[1147] of which 18 have ratified the Convention.[1148] One of the key aims of the Convention on the Protection of Children is the harmonization of criminal law provisions aimed at protecting children from sexual exploitation.[1149] To achieve this aim, the Convention contains a set of criminal law provisions. Apart from criminalization of the sexual abuse of children (Article 18), the Convention contains provisions dealing with the exchange of child pornography (Article 20) and the solicitation of children for sexual purposes (Article 23).

### 5.2.2 European Union[1150]

Over the past decade, the European Union (EU) has developed several legal instruments addressing aspects of cybercrime. While those instruments are in general only binding for the 27 Member States, several countries and regions are using the EU standards as a reference point in their national and regional discussions on harmonization of legislation.[1151]

#### Situation until December 2009

Until 2009, the EU's mandate in regard to criminal law was limited and contested.[1152] In addition to the challenge posed by the fact that the mandate was limited, it was uncertain whether the mandate for any criminal legislation, including cybercrime, lay with the so-called "First Pillar" (European Community) or the "Third Pillar" (European Union).[1153] Since the prevailing opinion was that the third pillar was responsible, harmonization was therefore only possible on the basis of intergovernmental cooperation within the third pillar of the European Union dealing with police and judicial cooperation in criminal matters.[1154] When, in 2005, the Court of Justice declared a third-pillar instrument in the area of criminal law (the Council Framework Decision on the Protection of the Environment through Criminal Law[1155]) to be unlawful[1156], the distribution of power was challenged for the first time. The court decided that the Framework Decision, being indivisible, infringed EU Article 47 as it encroached on the powers which EC Article 175 confers on the Community. This decision had a major influence on the debate on harmonizing criminal law within the European Union. The European Commission (EC), which is responsible for upholding the Union's treaties, pointed out that as a result of the judgement a number of framework decisions dealing with criminal law were entirely or partly incorrect, since all or some of their provisions were adopted on an incorrect legal basis.[1157] Despite the recognition of the new possibilities to evaluate a mandate within the first pillar, however, initiatives from the EC were limited owing to lack of coverage of the subject matter in the first pillar. In 2007, the Court of Justice confirmed the legal practice in a second court decision.[1158]

#### Situation after the ratification of the Treaty of Lisbon

The Treaty of Lisbon (the "Reform Treaty"),[1159] which came into force in December 2009, changed the function of the European Union significantly. In addition to rescinding the distinction between "first pillar" and "third pillar", for the first time it provided the EU with a solid mandate in the field of computer crime. Arts. 82 to 86 of the Treaty on the Functioning of the European Union (TFEU) provide the EU with a mandate for harmonizing criminal law legislation (substantive criminal law and procedural law). Most relevant with regard to cybercrime is TFEU Article 83.[1160] It authorizes the EU to establish minimum rules concerning the definition of criminal offences and sanctions in relation to serious crime with a cross-

border dimension. Computer crime is specifically mentioned as one of the relevant areas of crime in Article 83, paragraph 1. As the term computer crime is broader than cybercrime it authorizes the EU to regulate both areas. Based on Article 4, paragraph 2.j, the development of computer-crime legislation falls under shared competence between the EU and Member States. This enables the EU to adopt legally binding acts (Article 2, paragraph 2) and limits the ability of Member States to exercise their competence to the extent that the EU has not exercised its competence.

In the "Stockholm Programme", adopted by the European Council in 2009, the EU underlined that it will make use of the new mandate.[1161] The programme is a definition of the focus of EU work in the area of justice and home affairs for a period of five years, and follows the Hague Programme which expired in 2009.[1162] It underlines the EU's intention to make use of the mandate by referring to the areas of crime mentioned in TFEU Article 83, paragraph 1, and giving priority to the areas of child pornography and computer crime.[1163]

### Overview of EU instruments and guidelines

Despite the fundamental changes in the structure of the EU, instruments that have been adopted in the past remain in force. Based on Article 9 of the Protocol on Transitional Provisions, the instruments adopted on the basis of the Treaty on European Union prior to the entry into force of the Treaty of Lisbon shall be preserved until those acts are repealed, annulled or amended in implementation of the treaties. The following chapter therefore provides an overview of all relevant EU instruments.

### General policies

Back in 1996 already, the EU addressed risks related to the Internet in a communication dealing with illegal and harmful content on the Internet.[1164] The EU highlighted the importance of cooperation between Member States to combat illegal content online.[1165] In 1999, the European Parliament and the Council adopted an action plan on promoting safer use of the Internet and combating illegal and harmful content on global networks.[1166] The action plan focused on self-regulation rather than criminalization. Also in 1999, the EU launched the initiative "eEurope", by adopting the European Commission's Communication "eEurope – An Information Society for all".[1167] The initiative defines key goals, but does not deal with criminalization of illegal acts committed by using information technology. In 2001, the European Commission (EC) published a Communication titled "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime".[1168] In this communication, the EC analysed and addressed the problem of cybercrime and pointed out the need for effective action to deal with threats to the integrity, availability and dependability of information systems and networks.

*Information and communication infrastructures have become a critical part of our economies. Unfortunately, these infrastructures have their own vulnerabilities and offer new opportunities for criminal conduct. These criminal activities may take a large variety of forms and may cross many borders. Although, for a number of reasons, there are no reliable statistics, there is little doubt that these offences constitute a threat to industry investment and assets, and to safety and confidence in the information society. Some recent examples of denial of service and virus attacks have been reported to have caused extensive financial damage.*

*There is scope for action both in terms of preventing criminal activity by enhancing the security of information infrastructures and by ensuring that the law enforcement authorities have the appropriate means to act, whilst fully respecting the fundamental rights of individuals.*[1169]

*The Commission having participated in both the C.oE. and the G8 discussions, recognises the complexity and difficulties associated with procedural law issues. But effective co-operation within the EU to combat Cybercrime is an essential element of a safer Information Society and the establishment of an Area of Freedom, Security and Justice*[1170].

*The Commission will bring forward legislative proposals under the Title VI of the TEU:*
*[...] to further approximate substantive criminal law in the area of high-tech crime. This will include offences related to hacking and denial of service attacks. The Commission will also examine the scope for action against racism and xenophobia on the Internet with a view to bringing forward a Framework Decision under Title VI of the TEU covering both off-line and on-line racist and xenophobic activity. Finally, the problem of illicit drugs on the Internet will also be examined.*[1171]
*The Commission will continue to play a full role in ensuring co-ordination between Member States in other international for a in which Cybercrime is being discussed such as the Council of Europe and G8. The Commission's initiatives at EU level will take full account of progress in other international fora, while seeking to achieve approximation within the EU.*[1172]

In addition to the communication on computer-related crime the EC published a communication on "Network and Information Security"[1173] in 2001 that analysed the problems in network security and drafted a strategic outline for action in this area.

Both these EC communications emphasized the need for approximation of substantive criminal law within the European Union – especially with regard to attacks against information systems. Harmonization of substantive criminal law within the European Union in the fight against cybercrime is recognized as a key element of all initiatives at the EU level.[1174]

In 2007, the EC published a communication towards a general policy on the fight against cybercrime.[1175] The communication summarizes the current situation and emphasizes the importance of the Council of Europe Convention on Cybercrime as the predominant international instrument in the fight against cybercrime. In addition, the communication points out the issues that the EC will focus on with regard to its future activities. These include:

- strengthening international cooperation in the fight against cybercrime;
- better coordinated financial support for training activities;
- the organization of a meeting of law-enforcement experts;
- strengthening the dialogue with industry;
- monitoring the evolving threats of cybercrime to evaluate the need for further legislation.

### E-Commerce Directive (2000)

The EU Directive on Electronic Commerce[1176] addresses, among other issues, the liability of Internet service provider (ISP) for acts committed by third parties (Article 12 *et seq.*). Taking into account the challenges stemming from the international dimension of the network, the drafters decided to develop legal standards to provide a framework for the overall development of the information society and to support overall economic development as well as the work of law-enforcement agencies.[1177] It is based on the consideration that development of information-society services is hampered by a number of legal obstacles to the proper functioning of the internal market, which gives the European Community its mandate.[1178] The regulation of liability is based on the principle of graduated responsibility.[1179] Although the Directive highlights that there is no intention to harmonize the field of criminal law as such, it does also regulate liability under criminal law.[1180]

### Council Decision to combat child pornography on the Internet (1999)

In 2000, the Council of the European Union undertook an approach to address child pornography on the Internet. The Decision that was adopted is a follow-up to the 1996 communication on illegal and harmful content on the Internet[1181] and the related 1999 action plan on promoting safer use of the Internet and combating illegal and harmful content on global networks.[1182] However, the Decision does not contain obligations with regard to the adoption of specific criminal law provisions.

### European Union Council Framework Decision on combating fraud (2001)

In 2001, the EU adopted the first legal framework directly addressing aspects of cybercrime. The EU Framework Decision on combating fraud and counterfeiting of non-cash means of payment[1183] contains obligations to harmonize criminal law legislation with regard to specific aspects of computer-related fraud and the production of instruments, such as computer programs, that are specifically adopted for the purpose of committing an offence mentioned in the Framework Decision.[1184]

> ***Article 3 – Offences related to computers***
> *Each Member State shall take the necessary measures to ensure that the following conduct is a criminal offence when committed intentionally: performing or causing a transfer of money or monetary value and thereby causing an unauthorised loss of property for another person, with the intention of procuring an unauthorised economic benefit for the person committing the offence or for a third party, by:*
> *— without right introducing, altering, deleting or suppressing computer data, in particular identification data, or*
> *— without right interfering with the functioning of a computer programme or system.*

In line with the prevailing opinion at that time and as a consequence of the lack of a mandate in the first pillar, the instrument was developed under the third pillar, thereby highlighting that in view of the international dimension of the phenomena involved, such issues cannot be adequately addressed by the Member States themselves.

### European Union Council Framework Decision on attacks against information systems (2005)

After the publication of the general policy in 2001, the EC presented a proposal for a framework decision on attacks against information systems.[1185] It was modified and adopted by the Council in 2005.[1186] Although it takes note of the Council of Europe Convention on Cybercrime,[1187] it concentrates on the harmonization of substantive criminal law provisions that are designed to protect infrastructure elements. Aspects of criminal procedural law (especially the harmonization of the instruments necessary to investigate and prosecute cybercrime) and instruments related to the international cooperation were not integrated into the framework decision. It highlights the gaps and differences in the legal frameworks of the Member States and effective police and judicial cooperation in the area of attacks against information systems.[1188]

> ***Article 2 – Illegal access to information systems***
> *1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.*
> *2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure. punishable by effective, proportional and dissuasive criminal penalties.*
> ***Article 3 – Illegal system interference***
> *Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor.*
> ***Article 4 – Illegal data interference***
> *Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor.*

### Data Retention Directive (2005)

In 2005, the Council adopted the EU Data Retention Directive.[1189] It contains an obligation for ISPs to store certain traffic data that are necessary for the identification of criminal offenders in cyberspace.

> ***Article 3 – Obligation to retain data***
> *1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.*
> *2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the pro- cess of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.*

The fact that key information about any communication on the Internet will be covered by the Directive led to intensive criticism from human rights organizations and could lead to a review of the Directive and its implementation by constitutional courts.[1190] In the conclusion of the case *Productores de Música de España (Promusicae)* v. *Telefónica de España*,[1191] the adviser to the European Court of Justice, Advocate General Juliane Kokott, pointed out that it is questionable whether the data retention obligation can be implemented without a violation of fundamental rights.[1192] Potential difficulties concerning the implementation of such regulations were already highlighted by the G8 in 2001.[1193]

The Directive was based on the European Community's mandate for the internal market (Article 95).[1194] The drafters highlighted that differing legal and technical standards related to the retention of data for the purpose of investigating cybercrime present obstacles to the internal market for electronic communications, insofar as service providers face different requirements entailing different financial investments.[1195] Ireland, supported by Slovakia, asked the European Court of Justice to annul the Directive because it had not been adopted on an appropriate legal basis. Both countries argued that Article 95 was not a sufficient basis, since the focus of the instrument was not on the functioning of the internal market but rather the investigation, detection and prosecution of crime. The European Court of Justice dismissed the action as unfounded, pointing out that differences with regard to obligations to retain data would have a direct impact on the functioning of the internal market.[1196] It furthermore highlighted that such a situation justified the Community legislature in pursuing the objective of safeguarding the proper functioning of the internal market through the adoption of harmonized rules.

### Amendment of the European Union Council Framework Decision on combating terrorism (2007)

In 2007, the European Union started discussion on a draft amendment of the Framework Decision on combating terrorism.[1197] In the introduction to the draft amendment, the EU highlights that the existing legal framework criminalizes aiding or abetting and inciting but does not criminalize the dissemination of terrorist expertise through the Internet.[1198] With the amendment, the EU is aiming to take measures to close the gap and bring the legislation throughout the EU closer to the Council of Europe Convention on the Prevention of Terrorism.

> ***Article 3 – Offences linked to terrorist activities***
> *1. For the purposes of this Framework Decision:*
> *(a) "public provocation to commit a terrorist offence" means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of one of the acts listed in Article 1(1)(a) to (h), where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed;*

*(b) "recruitment for terrorism" means to solicit another person to commit one of the acts listed in Article 1(1), or in Article 2(2);*
*(c) "training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing one of the acts listed in Article 1(1), knowing that the skills provided are intended to be used for this purpose.*
*2. Each Member State shall take the necessary measures to ensure that terrorist-linked offences include the following intentional acts:*
*(a) public provocation to commit a terrorist offence;*
*(b) recruitment for terrorism;*
*(c) training for terrorism;*
*(d) aggravated theft with a view to committing one of the acts listed in Article 1(1);*
*(e) extortion with a view to the perpetration of one of the acts listed in Article 1(1);*
*(f) drawing up false administrative documents with a view to committing one of the acts listed in Article 1(1)(a) to (h) and Article 2(2)(b).*
*3. For an act to be punishable as set forth in paragraph 2, it shall not be necessary that a terrorist offence be actually committed."*

Based on Article 3(1)(c)[1199] of the Framework Decision, the Member States are, for example, obliged to criminalize the publication of instructions on how to use explosives, knowing that this information is intended to be used for terrorist-related purposes. The need for evidence that the information is intended to be used for terrorist-related purposes very likely limits the application of the provision with regard to the majority of instructions on how to use weapons that are available online, as their publication does not directly link them to terrorist attacks. As most of the weapons and explosives can be used to commit "regular" crimes as well as terrorist-related offences (dual use), the information itself can hardly be used to prove that the person who published them had knowledge about the way such information is used afterwards. Therefore the context of the publication (e.g. on a website operated by a terrorist organization) needs to be taken into consideration.

### Directive on child pornography

The first cybercrime-related draft legal framework presented after the ratification of the Treaty of Lisbon was the proposal for a Directive on combating the sexual abuse and sexual exploitation of children and child pornography[1200] that was adopted in 2011.[1201] The drafters pointed out that information technology enables offenders to produce and distribute child pornography more easily[1202] and emphasizes the importance of addressing the resulting challenges with specific provisions. It implements international standards, such as the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.[1203]

***Article 5 – Offences concerning child pornography***
*1. Member States shall take the necessary measures to ensure that the intentional conduct, when committed without right, referred to in paragraphs 2 to 6 is punishable.*
*2. Acquisition or possession of child pornography shall be punishable by a maximum term of imprisonment of at least 1 year.*
*3. Knowingly obtaining access, by means of information and communication technology, to child pornography shall be punishable by a maximum term of imprisonment of at least 1 year.*
*4. Distribution, dissemination or transmission of child pornography shall be punishable by a maximum term of imprisonment of at least 2 years.*
*5. Offering, supplying or making available child pornography shall be punishable by a maximum term of imprisonment of at least 2 years.*
*6. Production of child pornography shall be punishable by a maximum term of imprisonment of at least 3 years.*

*7. It shall be within the discretion of Member States to decide whether this Article applies to cases involving child pornography as referred to in Article 2(c)(iii), where the person appearing to be a child was in fact 18 years of age or older at the time of depiction.*
*8. It shall be within the discretion of Member States to decide whether paragraphs 2 and 6 of this Article apply to cases where it is established that pornographic material as referred to in Article 2(c)(iv) is produced and possessed by the producer solely for his or her private use in so far as no pornographic material as referred to in Article 2(c)(i), (ii) or (iii) has been used for the purpose of its production and provided that the act involves no risk of dissemination of the material.*

Like the Convention, the Directive proposes the criminalization of obtaining access to child pornography by means of information and communication technology.[1204] This enables law-enforcement agencies to prosecute offenders in cases where they are able to prove that the offender opened websites with child pornography, but are unable to prove that the offender downloaded material. Such difficulties in collecting evidence arise, for example, if the offender is using encryption technology to protect downloaded files on his storage media.[1205] The Explanatory Report to the Convention on the Protection of Children points out that the provision should also be applicable in cases where the offender only views child pornography pictures online without downloading them.[1206] In general, opening a website does automatically initiate a download process – often without the knowledge of the user.[1207] As a consequence, the provision is mainly relevant in cases where consumption of child pornography can take place without download of material. This can, for example, be the case if the website enables streaming videos and, due to the technical configuration of the streaming process, does not buffer the received information but discards it straight after transmission.[1208]

***Article 25 – Measures against websites containing or disseminating child pornography***
*1. Member States shall take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory.*
*2. Member States may take measures to block access to web pages containing or disseminating child pornography towards the Internet users within their territory. These measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress.*

In addition to the criminalization of acts related to child pornography, the initiation draft contained a provision that obliges Member States to implement the process of blocking websites containing child pornography.[1209] Several European countries,[1210] as well as non-European countries like China,[1211] Iran[1212] and Thailand,[1213] use such an approach. Concerns relate to the fact that none of the technical concepts has proven to be effective,[1214] and the approach entails a concomitant risk of over-blocking.[1215] As a consequence the mandatory blocking was changed and it was left to Member States to decide if blocking obligations should be implemented on the national level.

### Draft Directive on attacks against information systems (not adopted by end of 2011)

In September 2010, the European Union presented a proposal for a Directive on attacks against information systems.[1216] As described in more detail above, the EU adopted a Council Framework Decision on attacks against information systems in 2005.[1217] The Explanatory Memorandum to the proposal highlights that the intention of the drafters was to update and strengthen the legal framework to fight cybercrime in the European Union by responding to new methods of committing crimes.[1218] In addition to the criminalization of illegal access (Article 3), illegal system interference (Article 4) and illegal data interference (Article 5) already introduced by the 2005 Framework Decision, the 2010 draft Directive contains two additional offences.

***Draft Article 6 – Illegal interception***
*Member States shall take the necessary measures to ensure that the intentional interception by technical means, of non-public transmissions of computer data to, from or within a information system, including electromagnetic emissions from an information system carrying such computer data, is punishable as a criminal offence when committed without right.*
***Draft Article 7 – Tools used for committing offences***
*Member States shall take the necessary measure to ensure that the production, sale, procurement for use, import, possession, distribution or otherwise making available of the following is punishable as a criminal offence when committed intentionally and without right for the purpose of committing any of the offences referred to in Articles 3 to 6:*
*(a) device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;*
*(b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.*

Both provisions are largely in line with the corresponding provisions in the Convention on Cybercrime.

#### Relationship with the Council of Europe Convention on Cybercrime

As pointed out above, the Council of Europe Convention on Cybercrime was negotiated between 1997 and 2000. In 1999, the European Union expressed its perspective on the Convention on Cybercrime in a common position.[1219] It called for Member States to support the drawing up of the Council of Europe's draft Convention on Cybercrime.[1220] At that time, the EU itself had no mandate to develop a similar legal framework. The ratification of the Lisbon Treaty changed the situation. However, the EU has so far not decided to change its position with regard to the Convention on Cybercrime. In the Stockholm Programme, it highlighted that the EU not only calls upon Member States to ratify the Convention on Cybercrime, but also states that, in the view of the EU, it should become the legal framework of reference for fighting cybercrime at global level.[1221] However, this does not imply that the EU will not come up with a comprehensive approach to cybercrime, since EU approaches offer two major advantages. First, EU directives have to be implemented within a short, specified time-frame, whereas the Council of Europe has no means of enforcing the signature and ratification of conventions apart from political pressure.[1222] Secondly, the EU has a practice of constantly updating its instruments, whereas the Council of Europe Convention on Cybercrime has not been updated in the last ten years.

### 5.2.3 Organisation for Economic Co-operation and Development[1223]

In 1983, the Organisation for Economic Co-operation and Development (OECD) initiated a study on the possibility of international harmonization of criminal law in order to address the problem of computer crime.[1224] In 1985, it published a report that analysed the current legislation and made proposals for the fight against cybercrime.[1225] It recommended a minimum list of offences that countries should consider criminalizing, e.g. computer-related fraud, computer-related forgery, the alteration of computer programs and data, and the interception of the communications. In 1990, the Information, Computer and Communications Policy (ICCP) Committee created an Expert Group to develop a set of guidelines for information security, which was drafted by 1992 and then adopted by the OECD Council.[1226] The guidelines include, among other aspects, the issues of sanctions:

*Sanctions for misuse of information systems are an important means in the protection of the interests of those relying on information systems from harm resulting from attacks to the availability, confidentiality and integrity of information systems and their components. Examples of such attacks include damaging or disrupting information systems by inserting viruses and worms, alteration of data, illegal access to data, computer fraud or forgery, and unauthorised reproduction of computer programs. In combating such dangers, countries have chosen to describe and respond to the offending acts in a variety of ways. There is growing international agreement on the core of computer-related offences that should be covered by national penal laws. This is reflected in the development of computer crime and data protection legislation in OECD Member countries during the last two decades and in the work of the OECD and other international bodies on legislation to combat computer-related crime […]. National legislation should be reviewed periodically to ensure that it adequately meets the dangers arising from the misuse of information systems.*

After reviewing the guidelines in 1997, the ICCP created a second Expert Group in 2001 that updated the guidelines. In 2002, a new version of the guidelines "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" was adopted as a Recommendation of the OECD Council.[1227] The guidelines contain nine complementary principles:

*1) Awareness*
*Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.*
*2) Responsibility*
*All participants are responsible for the security of information systems and networks.*
*3) Response*
*Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.*
*4) Ethics*
*Participants should respect the legitimate interests of others.*
*5) Democracy*
*The security of information systems and networks should be compatible with essential values of a democratic society.*
*6) Risk assessment*
*Participants should conduct risk assessments.*
*7) Security design and implementation*
*Participants should incorporate security as an essential element of information systems and networks.*
*8) Security management*
*Participants should adopt a comprehensive approach to security management.*
*9) Reassessment*
*Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.*

In 2005, OECD published a report that analysed the impact of spam on developing countries.[1228] The report showed that, on account of their more limited and more expensive resources, spam is a much more serious issue in developing countries than in developed countries such as the OECD Member States.[1229] After receiving a request from the Strategic Planning Unit of the Executive Office of the Secretary General of the United Nations to produce a comparative outline of domestic legislative solutions regarding the use of the Internet for terrorist purposes, in 2007 OECD published a report on the legislative treatment of "cyberterror" in the domestic law of individual states.[1230] In 2008, OECD published a Scoping Paper on online identity theft.[1231] The paper provides an overview of the characteristics of identity theft, the different forms of identity theft, victim-related issues as well as law-enforcement schemes. The paper highlights that most OECD countries do not address the issue *per se* by means of specific provisions, and that the question whether ID theft should be criminalized as a standalone offence needs to be considered.[1232] In 2009, OECD published a report on malicious software.[1233] Although the

report briefly addresses aspects of criminalization, the focus is on the scope of malware and its economic impact.

### 5.2.4 Asia-Pacific Economic Cooperation[1234]

The Asia-Pacific Economic Cooperation (APEC) has identified cybercrime as an important field of activity, and APEC leaders have called for closer cooperation among officials involved in the fight against cybercrime.[1235] The Declaration of the 2008 meeting of the APEC Telecommunication and Information Ministers in Bangkok, Thailand, highlighted the importance of continuing collaboration to combat cybercrime.[1236] Until now, APEC has not provided a legal framework on cybercrime, but has referred to international standards such as the Budapest Convention on Cybercrime. In addition, APEC has closely studied the national cybercrime legislation in various countries[1237] under a cybercrime legislation survey, and has developed a database of approaches to assist economies in developing and reviewing legislation.[1238] The questionnaire used for the survey was based on the legal framework provided by the Budapest Convention on Cybercrime.

#### Statement on fighting terrorism (2002)

In 2002, APEC leaders released a Statement on Fighting Terrorism and Promoting Growth to enact comprehensive laws relating to cybercrime and develop national cybercrime investigating capabilities.[1239] They committed to endeavouring to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 and the Council of Europe Convention on Cybercrime, by October 2003. In addition, they committed to identifying national cybercrime units and international high-technology assistance points of contact and creating such capabilities, to the extent they do not already exist, by October 2003, and establishing institutions that exchange threat and vulnerability assessment (such as computer emergency response teams), by October 2003.

#### Conference on cybercrime legislation (2005)

APEC has organized various conferences[1240] and called for closer cooperation among officials involved in the fight against cybercrime.[1241] In 2005, APEC organized a Conference on Cybercrime Legislation. [1242] The primary objectives of the conference were to promote the development of comprehensive legal frameworks to combat cybercrime and promote cybersecurity; assist law-enforcement authorities to respond to cutting-edge issues and the challenges raised by advances in technology; promote cooperation between cybercrime investigators across the region.

#### Telecommunications and Information Working Group

The APEC Telecommunications and Information Working Group[1243] actively participated in APEC's approaches to increase cybersecurity.[1244] In 2002, it adopted the APEC Cybersecurity Strategy.[1245] The Working Group expressed their position regarding cybercrime legislation by referring to existing international approaches from the UN and the Council of Europe.[1246] Experiences with drafting cybercrime legislation were discussed within the context of the e-Security Task Group of the Telecommunications and Information Working Group during two conferences[1247] in Thailand in 2003.[1248]

### 5.2.5 The Commonwealth

Cybercrime is among the issues addressed by the Commonwealth. The activities concentrate in particular on harmonization of legislation. This approach to harmonize legislation within the Commonwealth and enable international cooperation was influenced, among other things, by the fact that, without such an approach, it would require no fewer than 1 272 bilateral treaties within the Commonwealth to deal with international cooperation in this matter.[1249]

Taking into account the rising importance of cybercrime, the Law Ministers of the Commonwealth decided to order an expert group to develop a legal framework for combating cybercrime on the basis of the Council of Europe Convention on Cybercrime.[1250] The Expert Group presented its report and

recommendations in March 2002.[1251] Later in 2002, the draft Model Law on Computer and Computer Related Crime was presented.[1252] Due to the clear instruction as well as the recognition of the Council of Europe Convention on Cybercrime as an international standard by the expert group, the model law largely corresponds to the standards defined by that Convention. However, there are differences that will be discussed further in Chapter 6.

At the 2000 meeting, the Law Ministers and Attorney-Generals of small Commonwealth jurisdictions decided to set up an expert group to develop model legislation on digital evidence. The model law was presented in 2002.[1253]

In addition to providing legislation, the Commonwealth has organized several training activities. The Commonwealth Network of IT and Development (COMNET-IT) co-organized training on cybercrime in April 2007.

In 2009, the Commonwealth Third Country Training Programme on legal framework for ICT was held in Malta, with the support of the Commonwealth Fund for Technical Co-operation (CFTC). Another training was organized in 2011.

In 2011 the Commonwealth presented "The Commonwealth Cybercrime Initiative". The main objective of the initiative is to assist Commonwealth countries in building their institutional, human and technical capacities with respect to policy, legislation, regulation, investigation and law enforcement.[1254] It aims to enable all Commonwealth countries to effectively cooperate in the global combat of cybercrime.

### 5.2.6 African Union

During the extra-ordinary conference of the African Union Ministers in charge of Communcation and Information Technologies, which was held in Johannesburg in 2009, the minsters addressed various topics related to the increasing use of ICT in the African country. It was decided that African Union Commission should – jointly with the UN Economic Commission for Africa – develop a legal framework for African countries that addresses issues like electronic transactions, cyber security and data protection.[1255]

In 2011 the African Union presented the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa.[1256] The intention of the drafters is to strengthen existing legislation in Member States regarding Information and Communication Technologies. With regard to the mandate, that was not limited to cybercrime, but also included other information society issues such as data protection and electronic transactions- The Convention is more comprehensive than most other regional approaches. It contains four parts. Part one is related to electronic commerce. It addresses various aspects such as contractual responsibility of an electronic provider of goods and services[1257], treaty obligations in electronic form[1258] and security of electronic transactions.[1259] The second part deals with data protection issues.[1260] The third part is related to combating cybercrime. Section 1 contains five chapters. This includes a set of six definitions (electronic communication, computerized data, racism and xenophobia in ICTs, minor, child pornography and computer system).[1261]

***Article III – 1:***
*For the purpose of this Convention:*
*1) Electronic communication means any transmission to the public or a section of the public by electronic or magnetic means of communication, signs, signals, written matter, pictures, sounds or messages of whatsoever nature;*
*2) Computerized data means any representation of facts, information or concepts in any form that lends itself to computer processing;*
*3) Racism and xenophobia in ICTs means any written matter, picture or any other representation of ideas or theories which advocates or encourages hatred, discrimination or violence against a person or group of persons for reasons of race, color, ancestry or national or ethnic origin or religion, where these serve as pretext for either racism and xenophobia or as motivation thereof;*
*4) Minor means any person aged less than eighteen (18) years in terms of the United Nations Convention on the Rights of the Child;*

*5) Child pornography means any data, regardless of the nature or form, which visually represents a minor lending him/herself to explicit sexual act, or realistic images representing a minor lending himself/herself to explicit sexual behavior;*
*6) Computer system means any device, be it isolated or otherwise, and a range of interconnected devices used in part or in whole for automated processing of data for the purpose of executing a programme.*

In addition the third part addresses the need of a national cybersecurity policy and a related strategy.[1262] The second chapter deals with general aspects related to legal measures. This includes standards related to statuatory authorities, democratic principles, protection of essential information infrastructure, harmonization, double criminality and international cooperation.[1263] The third chapter addresses issues related to a national cyber security system. This includes a culture of security, the role of the government, public-private partnership, education and training and public awareness-raising.[1264] Chapter 4 is dedicated to national cyber security monitoring structures. The fifth chapter deals with international cooperation. The main difference to comparable regional frameworks such as the Council of Europe Convention on Cybercrime is the fact that the Draft African Union Convention– if no other instrument for international cooperation is in place – cannot be used for such purpose. The different conception is especially expressed by Articles 21 and 25.

***Article III – 1 – 21: International cooperation***
*Each Member State shall adopt such measures as it deems necessary to foster exchange of information and the sharing of quick, expeditious and reciprocal data by Member States' organizations and similar organizations of other Member States with responsibility to cause the law to be applied in the territory on bilateral or multilateral basis.*

***Article III – 1 – 25: Model of international cooperation***
*Each Member State shall adopt such measures and strategies as it deems necessary to participate in regional and international cooperation in cyber security. The Resolutions geared to promoting Member States' participation within this framework of relations have been adopted by a large number of international governmental bodies including the United Nations, the African Union, the European Union, the G8, etc. Organizations like the International Telecommunication Union, the Council of Europe, the Commonwealth of Nations and others, have established model frameworks for international cooperation which Member States may adopt as a guide.*

Section II of the third part deals with substantive penal law. Section 1 includes a criminalization of illegal access to a computer system[1265], illegal remaining in a computer system[1266], illegal system interference[1267], illegal data input[1268], illegal data interception[1269] and illegal data interference.[1270] The provisions show a lot of similarities with best practices from other regions – including standards introduced within Africa. One example is the criminalization of illegal remaining in a computer system that was introduced by the Draft ECOWAS Directive.[1271]

***Article III – 3:***
*Each Member State of the African Unions shall take the legislative measures required to set up as a penal offense the fact of retaining oneself or attempting to retain oneself fraudulently in a part or the whole of a computer system.*

One new concept – however, not criminal law provision but a side measure – that was in this regard not introduced by other regional frameworks is the introduction of an obligation of businesses to to submit their products fro vulnerability testing.

***Article III-7:***
*[...]*
*2) The Member States shall adopt rules to compel ICT product vendors to submit their products for vulnerability and guarantee tests to be conducted by independent experts and to divulge to the public any form of vulnerability found in the said products and the measures recommended for a solution thereto.*

Section 2 includes the criminalization of aspects of computer-related forgery[1272], illegal use of data[1273], illegal system interference with the intent to obtain an advantage[1274], data protection violations[1275], illegal devices[1276] and participation in a criminal organization.[1277]

***Article III – 9:***
*Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of using the data obtained with a full knowledge of a case.*

Especially the criminalization of an illegal use of computer data is going beyond the standards defined by most other regional instruments.

Section 3 deals with the criminalization of illegal content. The Draft African Convention introduces a criminalization of producing and disseminating child pornography[1278], procuring and importing child pornography[1279], possessing child pornography[1280], facilitating the access of minors to pornography[1281], dissemination of racist or xenophobic material[1282], racist attacks perpetrated through computer systems[1283], racist abuse through computer systems[1284] and denying or approving genocide or crimes against humanity.[1285]

The last section of Chapter 1 contains provisions that deal in a broader manner with legislation related to Cybercrime and the admissibility of electronic evidence ("written electronic matter").

***Article III – 23 – 1: Laws against cyber crime***
*Each Member State shall adopt such legislative measures as it deems effective, to define material criminal offenses as acts which affect the confidentiality, integrity, availability and survivability of ICT systems and related infrastructure networks; as well as procedural measures deemed effective for the arrest and prosecution of offenders. Member States shall be called upon to take on board, where necessary, the approved language choice in international cyber crime legislation models such as the language choice adopted by the Council of Europe and the Commonwealth of Nations.*

***Article III – 23 – 2:***
*Each Member State of the African Union shall take the legislative measures required to ensure that written electronic matter in respect of criminal matters are admissible to establish offenses under criminal law, provided such written matter has been presented during debate and discussed before the judge, that the person from which the written material emanates can be duly identified and the said material has been prepared and conserved under conditions likely to guarantee their integrity.*

Especially with regard to Article III-23-1 the intention of the drafters is not fully accessible as the crimes contained in previous parts of Chapter 1 define crimes as crimes against the integrity and availability of computer systems. It is therefore uncertain how far Article III-23-1– with regard to the criminalization – requires countries to go beyond the crimes already established in more detail by the Draft African Convention.

Chapter two contains provisions that intend to update traditional provisions to ensure an applicability when it comes to the involvement of computer systems and data. It requires countries to set up an aggravation of penalty if traditional crimes are committed by using information and communication technology[1286], the criminalization violation of property by offences such as theft, abuse of trust or

blackmail involving computer data[1287], update provisions that include dissemination facilities to ensure that the use of means of digital electronic communication is covered[1288] and ensure that provisions that protect secrecy in the interest of national security are applicable with regard to computer data.[1289] Such provisions are not included in other regional frameworks. With regard to Article III-24 it is uncertain why the mere fact that a computer system was used at one stage during the commission of a traditional offence (eg. the offenders send an email prior to breaking into a bank instead of making a phone call) shall lead to an aggravated sentence.

***Article III – 24:***
*Each Member State of the African Union shall take the legislative measures required to set up as an aggravating circumstance the use of ICT to commit common law offenses such as theft, fraud, possession of stolen goods, abuse of trust, extortion of money, terrorism, money laundering, etc.*

Article III-28 – Article III- 35 deal with liability and sanctions.

Section III deals with procedural law. It requires that Member States enable the conservation of computer data[1290], the seizure of computer data[1291], expedited preservation[1292] and interception of data communication.[1293]

### 5.2.7 Arab League and Gulf Cooperation Council[1294]

A number of countries in the Arabic region have already undertaken national measures and adopted approaches to combat cybercrime, or are in the process of drafting legislation.[1295] Examples of such countries include Pakistan,[1296] Egypt[1297] and the United Arabic Emirates (UAE).[1298] In order to harmonize legislation in the region, UAE submitted model legislation to the Arab League (Guiding Law to Fight IT Crime).[1299] In 2003, the Arab Interior Ministers Council and the Arab Justice Ministers Council adopted the law.[1300] The Gulf Cooperation Council (GCC)[1301] recommended at a conference in 2007 that the GCC countries seek a joint approach that takes into consideration international standards.[1302]

### 5.2.8 Organization of American States[1303]

Since 1999, the Organization of American States (OAS) has actively been addressing the issue of cybercrime within the region. Among others, the organization has held a number of meetings within the mandate and scope of REMJA, the Ministers of Justice or Ministers or Attorneys General of the Americas.[1304]

#### Intergovernmental expert group on cybercrime

In 1999, REMJA recommended the establishment of an intergovernmental expert group on cybercrime. The expert group was mandated to complete a diagnosis of criminal activity which targets computers and information, or which uses computers as the means of committing an offence; complete a diagnosis of national legislation, policies and practices regarding such activity; identify national and international entities with relevant expertise; and finally identify mechanisms of cooperation within the inter-American system to combat cybercrime.

#### Recommendations of the Ministers of Justice

REMJA has held eight meetings until 2010.[1305] At the third meeting, in 2000, the Ministers of Justice or Ministers or Attorneys General of the Americas addressed the topic of cybercrime and agreed on a number of recommendations.[1306] These recommendations included to support consideration of the recommendations made by the Group of Governmental Experts at its initial meeting as the REMJA contribution to the development of the Inter-American Strategy to Combat Threats to Cybersecurity, referred to in OAS General Assembly Resolution AG/RES. 1939 /XXXIII-O/03), and to ask the group, through its chair, to continue to support the preparation of the strategy. The meeting further recommended that Member States should review mechanisms to facilitate broad and efficient cooperation among themselves to combat cybercrime and study, where possible, the development of

technical and legal capacity to join the 24/7 Network established by the G8 to assist in cybercrime investigations. Member States were asked to evaluate the advisability of implementing the principles of the Council of Europe Convention on Cybercrime and consider the possibility of acceding to that Convention. In addition to the United States and Canada, which signed the Convention on Cybercrime in 2001, Chile, Costa Rica, Dominican Republic and Mexico have in the meantime been invited by the Council of Europe to accede to the Convention. Finally, the recommendations called for OAS Member States to review and, if appropriate, update the structure and work of domestic bodies, or agencies in charge of enforcing the laws so as to adapt to the shifting nature of cybercrime, including by reviewing the relationship between agencies that combat cybercrime and those that provide traditional police or mutual legal assistance.

The fourth meeting of Ministers of Justice or Ministers or Attorneys General of the Americas in 2002 recommended that, in the framework of the activities of the OAS working group to follow up on the REMJA recommendations, the Group of Governmental Experts[1307] on cybercrime be reconvened and mandated to follow up on implementation of the recommendations prepared by that group and adopted by REMJA-III, and consider the preparation of pertinent inter-American legal instruments and model legislation for the purpose of strengthening hemispheric cooperation in combating cybercrime and considering standards relating to privacy, the protection of information, procedural aspects, and crime prevention.

The recommendations of the sixth meeting of Ministers of Justice[1308] included a call to continue to strengthen cooperation with the Council of Europe so that the OAS Member States can give consideration to applying the principles of the Convention on Cybercrime[1309] and to adhering thereto, and to adopting the legal and other measures required for its implementation. Similarly, the meeting recommended that efforts should continue to strengthen mechanisms for exchange of information and cooperation with other international organizations and agencies in the area of cybercrime, such as the UN, the EU, APEC, OECD, the G8, the Commonwealth and Interpol, in order for the OAS Member States to take advantage of progress in those forums. Furthermore, Member States were asked to establish specialized units to investigate cybercrime, identify the authorities who will serve as the points of contact in this matter and expedite the exchange of information and obtaining of evidence, and in addition, to foster cooperation in efforts to combat cybercrime among government authorities and Internet service providers and other private-sector enterprises providing data transmission services.

These recommendations were reiterated at the 2008 meeting,[1310] which further recommended that, bearing in mind the recommendations adopted by the Group of Governmental Experts and by the previous REMJA meetings, the states consider applying the principles of the Council of Europe's Convention on Cybercrime, acceding thereto, and adopting the legal and other measures required for its implementation. Similarly, the meeting recommended that technical cooperation activities continue to be held under the auspices of the OAS General Secretariat, through the Secretariat for Legal Affairs, and the Council of Europe, and that efforts be continued to strengthen exchange of information and cooperation with other international organizations and agencies in the area of cybercrime, so that the OAS Member States may take advantage of progress in those forums. Finally, the secretariats of the Inter-American Committee against Terrorism (CICTE) and the Inter-American Telecommunication Commission (CITEL) and the Working Group on Cybercrime were requested to continue developing permanent coordination and cooperation actions to ensure the implementation of the Comprehensive Inter-American Cybersecurity Strategy adopted through OAS General Assembly Resolution AG/RES. 2004 (XXXIV-O/04).

In 2010, REMJA addressed the issue of cybercrime at their eighth meeting.[1311] They briefly discussed the importance of continuing to consolidate and update the Inter-American Portal for Cooperation in Cybercrime through the OAS Internet page, and strengthening states' capacity to develop legislation and procedural measures related to cybercrime and electronic evidence. In addition, the meeting's recommendations highlighted the desire to strengthen mechanisms that allow for the exchange of information and cooperation with other international organizations and agencies in the area of cybercrime, such as the Council of Europe, the UN, the EU, APEC, OECD, the G8, the Commonwealth and Interpol, so that OAS Member States can take advantage of developments in those entities.

### 5.2.9 Caribbean

In December 2008, ITU and the EU launched the project "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures" (HIPCAR) to promote the ICT sector in the Caribbean region.[1312] The project forms part of the programme "ACP-Information and Communication Technologies" and the ninth European Development Fund. Beneficiary countries are 15 Caribbean countries.[1313] The aim of the project is to assist CARIFORUM[1314] countries to harmonize their ICT policies and legal frameworks.

Under this project, nine work areas have been identified[1315] in which model policies and model legislative texts were developed to facilitate the development and harmonization of legislation in the region. Cybercrime was one of the nine work areas. The development of the model legislative text took place in three phases. In the first phase, existing legislation in the beneficiary countries was collected and reviewed. In parallel, regional and international best practices were identified. Priority was given to standards that are directly applicable in at least some of the beneficiary countries (e.g. the Commonwealth Model Law from 2002). However, the review also included best practices from other regions, such as the EU and Africa. The assessment report[1316] contained an overview of the existing legislation, as well as a comparative law analysis that compared the existing legislation with regional and international best practices. In order to prepare a gap analysis, the assessment report in addition identified special needs in the region (such as legislation on spam) that are not necessarily addressed by international best practices. In a workshop in 2010, the assessment report was discussed with stakeholders from the beneficiary countries.[1317] On the basis of the assessment report and gap analysis, the stakeholders drafted model policy guidelines.

In the second phase, a model legislative text was developed taking into account the policy guidelines. At a second workshop, policy experts, law drafters and other stakeholders from the beneficiary countries discussed and amended the draft model legislative text that was prepared for the meeting, and adopted it. The model legislative text has three key aims: it provides specific sample language that is in line with international best practices, it reflects the special demands of the region and it is developed with law-drafting practices in the region in mind, so as to ensure smooth implementation. The model legislative text contains a complex set of definitions, and substantive criminal law provisions, including provisions dealing with issues like SPAM that have a high priority for the region but are not necessarily contained in regional frameworks such as the Council of Europe Convention on Cybercrime.

> *15. (1) A person who, intentionally without lawful excuse or justification:*
>
> *a) intentionally initiates the transmission of multiple electronic mail messages from or through such computer system; or*
>
> *b) uses a protected computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead users, or any electronic mail or Internet service provider, as to the origin of such messages, or*
>
> *c) materially falsifies header information in multiple electronic mail messages and intentionally initiates the transmission of such messages,*
>
> *commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*
>
> *(2) A country may restrict the criminalization with regard to the transmission of multiple electronic messages within customer or business relationships. A country may decide not to criminalize the conduct in section 15 (1) (a) provided that other effective remedies are available.*

Furthermore, the text contains procedural law provisions (including advanced investigation instruments such as the use of remote forensic tools) and provisions on the liability of Internet service providers (ISPs).

### 5.2.10 Pacific

In parallel to the ITU and EU co-funded project in the Caribbean the same organizations launched a project in the Pacific (ICB4PAC).[1318] The project aims – based on a request by the the Pacific Island

countries – to provide capacity building related to ICT policies and regulations. In this regard it focuses on building human and institutional capacity in the field of ICT through training, education and knowledge sharing measures. Beneficiary countries are 15 Pacific Island countries.[1319] In March 2011 a workshop dealing with the current cybercrime legislation in the Pacific region was hosted in Vanuatu.[1320] During the workshop a comprehensive comparative legal analysis was presented that provided an overview about existing legislation in the region as well as a comparison with best practices from other regions.[1321] As a follow up to this workshop a conference dealing with techniques of developing cybercrime policies and legislation was organized in August 2011 in Samoa.[1322] During the conference best practices from other regions were presented and structures for a harmonized policy and legislation were developed. They addressed substantive criminal law, procedural law, international cooperation, liability of Internet Service Provider (ISP), electronic evidence and crime prevention measures.

In April 2011 the Secretariat of the Pacific Community organized a conference related to the Fight against Cybercrime in the Pacific.[1323] The event was co-organized by the Council of Europe. During the conference aspects related to substantive criminal law, procedural law and international cooperation were discussed.[1324]

## 5.3 Scientific and independent approaches

### *5.3.1 Stanford Draft International Convention*

A well-known example of a scientific approach to developing a legal framework for addressing cybercrime at the global level is the Stanford Draft International Convention (the "Stanford Draft").[1325] The Stanford Draft was developed as a follow-up to a conference hosted by Stanford University in the United States in 1999.[1326] Comparison with the Council of Europe Convention on Cybercrime[1327] that was drafted around the same time shows a number of similarities. Both cover aspects of substantive criminal law, procedural law and international cooperation. The most important difference is the fact that the offences and procedural instruments developed by the Stanford Draft are only applicable with regard to attacks on information infrastructure and terrorist attacks, while the instruments related to procedural law and international cooperation mentioned in the Council of Europe Convention on Cybercrime can also be applied with regard to traditional offences as well.[1328]

### *5.3.2 Global Protocol on Cybersecurity and Cybercrime*

During the Internet Governance Forum in Egypt in 2009, *Scholberg* and *Ghernaouti-Helie* presented a proposal for a Global Protocol on Cybersecurity and Cybercrime.[1329] Article 1-5 relate to cybercrime and recommend the implementation of substantive criminal law provisions, procedural law provisions, measures against terrorist misuse of the Internet, measures for global cooperation and exchange of information and measures on privacy and human rights.[1330] The model legislation provided in appendix to the protocol is to a large degree (Articles 1-25) exactly based on the wording of the provisions provided by the Council of Europe Convention on Cybercrime.

## 5.4 The relationship between regional and international legislative approaches

The success of single standards with regard to technical protocols leads to the question of how conflicts between different international approaches can be avoided.[1331] The Council of Europe Convention on Cybercrime and the Commonwealth Model Law on Cybercrime are the frameworks that follow the most comprehensive approach, as they cover substantive criminal law, procedural law and international cooperation. But none of the instruments have so far been amended to address developments that have taken place in recent years. In addition, the scope of both instruments is limited. The debate at the last UN Crime Congress highlighted the interest of countries in international instruments.[1332] This raises questions in respect of the relationship between existing regional approaches and possible international action. There are three possible scenarios.

If a new legal approach defines standards that are not in accordance with the consistent existing approaches at the regional and national level, this could, at least initially, have a negative effect on the

necessary harmonization process. It is therefore likely that any new approach will carefully analyse existing standards to ensure consistency. One example is the criminalization of illegal access which is defined in a similar manner by Section 5 of the Commonwealth Model Law on Cybercrime and Article 2 of the Council of Europe Convention on Cybercrime.

In addition, a new approach will be able to avoid including provisions that have led to difficulties in implementation or even stopped countries from acceding to an instrument. One example is the controversially discussed regulation in Article 32b of the Council of Europe Convention on Cybercrime. This provision was criticized by the Russian Delegation at the 2007 meeting of the Cybercrime Committee.[1333]

Finally, a new international approach could – in addition to including basic standards that are similar in the different legal approaches – focus on a gap analysis to identify areas that are not yet sufficiently addressed, and thus criminalize certain cybercrime-related acts and define procedural instruments that are not yet covered by existing instruments. Since 2001, a number of important developments have taken place. When the Council of Europe Convention on Cybercrime was drafted, "phishing",[1334] "identity theft"[1335] and offences related to online games and social networks were not as relevant as they have since become. A new international approach could continue the harmonization process by including further offences with a transnational dimension.[1336]

## 5.5 The relationship between international and national legislative approaches

As pointed out previously, cybercrime is a truly transnational crime.[1337] Having regard to the fact that offenders can, in general, target users in any country in the world, international cooperation of law-enforcement agencies is an essential requirement for international cybercrime investigations.[1338] Investigations require means of cooperation and depend on the harmonization of laws. Due to the common principle of dual criminality,[1339] effective cooperation first requires harmonization of substantive criminal law provisions in order to prevent safe havens.[1340] In addition, it is necessary to harmonize investigation instruments, in order to ensure that all countries involved in an international investigation have the necessary investigative instruments in place to carry out investigations. Finally, effective cooperation of law-enforcement agencies requires effective procedures on practical aspects.[1341] The importance of harmonization triggers the need for participation in the global harmonization process, which is therefore at least a tendency, if not a necessity, for any national anti-cybercrime strategy.

### *5.5.1 Reasons for the popularity of national approaches*

Despite the widely recognized importance of harmonization, the process of implementing international legal standards is far from being completed.[1342] One of the reasons why national approaches play an important role in the fight against cybercrime is that the impact of the crimes is not the same everywhere. One example is the approach taken to combat spam.[1343] Spam-related e-mails especially affect developing countries. This issue was analysed in an OECD report.[1344] Due to scarcer and more expensive resources, spam turns out to be a much more serious problem in developing countries than in western countries.[1345] The different impacts of cybercrime, together with existing legal structures and traditions, are the main reasons for a significant number of legislative initiatives at the national level which are not, or only partly, dedicated to the implementation of international standards.

### *5.5.2 International vs. national solutions*

In times of technical globalization this may seem like a slightly surprising discussion, as anybody wishing to connect to the Internet needs to make use of the (technical) standard protocols in place.[1346] Single standards are an essential requirement for the operation of the networks. However, unlike technical standards, the legal standards still differ.[1347] It must be questioned whether national approaches can still work, given the international dimension of cybercrime.[1348] The question is relevant for all national and regional approaches that implement legislation which is not in line with existing international standards. A lack of harmonization can seriously hinder international investigations, whereas national and regional

approaches which go beyond international standards avoid problems and difficulties in conducting international investigations.[1349]

There are two main reasons for a growing number of regional and national approaches. The first is legislative speed. Neither the Commonwealth nor the Council of Europe can force any of their Member States to use their instruments. In particular, the Council of Europe has no instrument to instruct a signatory of the Convention on Cybercrime to ratify it. The harmonization process is therefore often considered to be slow compared to national and regional legislative approaches.[1350] Unlike the Council of Europe, the European Union has means to force Member States to implement framework decisions and directives. This is the reason why a number of European Union countries which signed the Convention on Cybercrime in 2001, but have not yet ratified it, have nevertheless implemented the 2005 EU Council Framework Decision on attacks against information systems.

The second reason is related to national and regional differences. Some offences are only criminalized in certain countries in a region. Examples are religious offences.[1351] Although it is unlikely that an international harmonization of criminal law provisions related to offences against religious symbols would be possible, a national approach can in this regard ensure that legal standards in one country can be maintained.

### 5.5.3 Difficulties of national approaches

National approaches face a number of problems. In regard to traditional crimes, the decision by one country, or a few countries, to criminalize certain behaviours can influence the ability of offenders to act in those countries. However, when it comes to Internet-related offences, the ability of a single country to influence the offender is much smaller as the offender can, in general, act from any place with a connection to the network.[1352] If they act from a country that does not criminalize the certain behaviour, international investigations as well as extradition requests will very often fail. One of the key aims of international legal approaches is therefore to prevent the creation of such safe havens by providing and applying global standards.[1353] As a result, national approaches in general require additional side measures to be able to work.[1354] The most popular side measures are criminalization of the user in addition to the supplier of illegal content, and of services used in the committing a crime.

#### Criminalization of the user in addition to the supplier of illegal content

One approach is criminalization of the use of illegal services in addition to the sole criminalization of offering such services. The criminalization of users who are located inside the jurisdiction is an approach to compensate for the lack of influence on providers of the services who act from abroad.

#### Criminalization of services used in the committing a crime

A second approach is the regulation and even criminalization of offering certain services within the jurisdiction that are used for criminal purposes. This solution goes beyond the first approach, as it concerns businesses and organizations which offer neutral services that are used for legal as well as illegal activities. An example of such an approach is the United States Unlawful Internet Gambling Enforcement Act of 2006.[1355]

Closely related to this measure is the establishment of obligations to filter certain content available on the Internet.[1356] Such an approach was discussed under the famous Yahoo-decision[1357] and is currently being discussed in Israel, where access providers may be obliged to restrict access to certain adult-content websites. Attempts to control Internet content are not limited to adult content; some countries use filter technology to restrict access to websites that address political topics. OpenNet Initiative[1358] reports that censorship is practised by about two dozen countries.[1359]

[984] This includes regional approaches.

[985] The Group of Eight (G8) consists of eight countries: Canada, France, Germany, Italy, Japan, United Kingdom, United States and the Russian Federation. The presidency of the group, which represents more than 60 per cent of the world economy (source: http://undp.org), rotates every year.

[986] The idea of the creation of five subgroups – among them, one on high-tech crimes – was to improve implementation of the 40 recommendations adopted by G8 Heads of State in 1996.

[987] The establishment of the subgroup (also described as the subgroup to the "Lyon Group") continued the efforts of the G8 (at that time still G7) in the fight against organized crime, which started with the launch of the Senior Experts Group on Organized Crimes (the "Lyon Group") in 1995. At the Halifax summit in 1995, the G8 stated: "We recognize that ultimate success requires all Governments to provide for effective measures to prevent the laundering of proceeds from drug trafficking and other serious crimes. To implement our commitments in the fight against transnational organized crime, we have established a group of senior experts with a temporary mandate to look at existing arrangements for cooperation both bilateral and multilateral, to identify significant gaps and options for improved coordination and to propose practical action to fill such gaps". See: Chairman's Statement, Halifax G7 Summit, June 17 1995. For more information, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[988] Regarding the G8 activities in the fight against cybercrime, see also: United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[989] "Communiqué of the Ministerial Conference of the G8 Countries on Combating Transnational Organized Crime", Moscow, 19-20 October 1999.

[990] 14. As the use of the Internet and other new technologies increase, more criminals are provided with opportunities to commit crimes remotely, via telephone lines and data networks. Presently, malicious programming code and harmful communications (such as child pornography) may pass through several carriers located in different countries. And infrastructures such as banking and finance increasingly are becoming networked and thereby vulnerable to cyber-attack from distant locations. We convene today to provide additional personal attention to and direction for our joint action against this transnational criminality.

15. Our goals are to ensure that our people are protected from those who use new technologies for criminal purposes, such as child exploitation, financial crime, and attacks on critical infrastructures, and to ensure that no criminal receives safe haven anywhere in the world. We are determined that our law enforcement authorities have the technical ability and legal processes to find criminals who abuse technologies and bring them to justice. The safety of our people and their economic prosperity depend upon our leadership and determination and our ability to take coordinated action. We direct our experts to continue their work, particularly, on problems which arise for our law enforcement authorities from new developments in information technology and their use by criminals.

16. Strength of G-8 Legal Systems. Our experts have completed a comprehensive review of G-8 legal systems to assess whether those systems appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes. While, over the past decade, our governments have acted to see that their legal systems account for new technologies, there remains room for improvement. Where laws or legal processes require enhancements, we are committed to use best efforts to fill these gaps and, consistent with fundamental national legal principles, to promote new legal mechanisms for law enforcement to facilitate investigations and prosecutions.

17. Principles on Transborder Access to Stored Computer Data. Criminals take advantage of the jurisdictional inability of law enforcement authorities to operate across national borders as easily as criminals can. High-tech crimes may rapidly affect people in many countries, and evidence of these crimes, which may be quickly altered or destroyed, may be located anywhere in the world. Recognizing these facts, and taking into account principles relating to sovereignty and to the protection of human rights, democratic freedoms and privacy, our law enforcement authorities conducting criminal investigations should in some circumstances be able to pursue investigations across territorial borders. We have today adopted certain principles for access to data stored in a foreign state, which are contained in the Annex 1 to this Communique. We are committed to work towards implementation of these principles through international cooperation, including legal instruments, and through national laws and policies, and invite all nations to join in this effort. We note, however, that continued work is required in this area, including on the appropriate collection, preservation and disclosure of traffic data, and we direct our experts to make further progress in consultation with industry.

18. Locating and Identifying High-tech Criminals. To ensure that we can all locate and identify criminals who use networked communications for illegal purposes, we must enhance our ability to trace communications while they are occurring and afterwards, even when those communications pass through multiple countries. Existing processes are often too slow and are designed more to address bilateral cooperation than crimes requiring the immediate assistance of many countries. Faster or novel solutions must be found. We, as Ministers, direct our experts to develop, in consultation with industry, a concrete set of options for tracing networked communications across national borders in criminal investigations and provide those options as soon as possible within one year.

19. International Network of 24-hour Contacts. Our 24-hour points of contact network, which allows us to respond to fast-breaking investigations, has now been expanded from the eight G-8 countries to a number of additional countries around the world. The speed of electronic communications and perishability of electronic evidence requires real-time assistance, and this growing global network has dramatically increased our investigative abilities. We direct our experts to facilitate further growth of this network. G-8 nations and their partners should also use this network proactively to notify other countries when they learn of significant potential threats to our shared networks.

20. Criminality Associated with the 'Millennium Bug'. Our countries have been at the forefront of efforts to successfully tackle the 'Millennium Bug' or 'Y2K Problem', which presents a major threat to the increasingly networked global economy. We are concerned that the Millennium Bug may either provide new opportunities for fraud and financial crimes, or mask ongoing criminality, if systems for accounting and reporting are disrupted. Therefore, as part of our new proactive use of our 24-hour network, we will provide early warning of Y2K-related abuses.

21. Internet Fraud. We recognize that Internet fraud, in all of its forms, poses a significant threat to the growth and development of electronic commerce and to the confidence that consumers place in electronic commercial transactions. To counter this threat, we are undertaking a comprehensive response, including crime prevention, investigation, and prosecution. For example, we are sharing information on international Internet fraud schemes – including information relating to the criminals, their methods and techniques, the victims involved in these schemes, and reports of enforcement actions – so that criminals defrauding people in multiple countries are investigated and prosecuted for the full range of their criminal activities.

[991] The idea of a 24/7 network has been picked up by a number of international approaches in the fight against cybercrime. One example is Article 35 of the Convention on Cybercrime:

> (1) Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:
> a) the provision of technical advice;
> b) the preservation of data pursuant to Articles 29 and 30;
> c) the collection of evidence, the provision of legal information, and locating of suspects. […]

[992] *Jean-Pierre Chevenement*, the French Minister of the Interior, stated: "Now that the G8 has provided the impetus, it's vital that we formalize the new legal rules and procedures for cooperation in a legal instrument applying world-wide. For France, the negotiations under way in the Council of Europe on a Convention on Cyber-Crime are of fundamental importance for several reasons. The draft currently under discussion defines the offences which all States would have to recognize. It goes on to propose ways in which they could cooperate, taking up, for example, the idea of national contact points. It also proposes extradition procedures. In short, this agreement is an essential instrument, which France wants to see concluded within a reasonable period of time. The important thing about these negotiations is that the countries involved include some major countries outside the Council of Europe and that, once signed, this convention will be opened for signature by all States wishing to accede to it. The idea is in fact to get a convention which applies world-wide so that there can be no more "digital havens" or "Internet havens" in which anyone wanting to engage in shady activities can find all the facilities they need, including financial ones, for laundering the product of their crimes. Since we must never lose sight of the fact that the Internet is a global system and that no country can isolate itself from the rules under which it has to operate."

[993] G8 Government-Industry Workshop on Safety And Security In Cyberspace, Tokyo, May 2001.

[994] The experts expressed their concerns regarding implementation of a data-retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible"; Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace, Tokyo, May 2001.

[995] G8 Justice and Home Affairs Communiqué, Washington DC, 11 May 2004.

[996] G8 Justice and Home Affairs Communiqué Washington DC, 11 May 2004:10. "Continuing to Strengthen Domestic Laws: To truly build global capacities to combat terrorist and criminal uses of the Internet, all countries must continue to improve laws that criminalize misuses of computer networks and that allow for faster cooperation on Internet-related investigations. With the Council of Europe Convention on Cybercrime coming into force on July 1, 2004, we should take steps to encourage the adoption of the legal standards it contains on a broad basis."

[997] The participants expressed their intention to strengthen the instruments in the fight against cybercrime: "We discussed the necessity of improving effective countermeasures that will prevent IT terrorism and terrorist acts in this sphere of high technologies. For that, it is necessary to devise a set of measures to prevent such possible criminal acts, including in the sphere of telecommunication. That includes work against the selling of private data, counterfeit information and application of viruses and other harmful computer programs. We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work, and we will apply all of that to prevent terrorists from using computer and Internet sites for hiring new terrorists and the recruitment of other illegal actors". See: www.g7.utoronto.ca/justice/justice2006.htm.

[998] Regarding the topic of cyberterrorism, see above: § 2.9.1. In addition, see: *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis,* Cyber-terrorism and Cybersecurity; www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in *Arquilla/Ronfeldt*, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45 page 1033 *et seq.*; United States Department of State, Pattern of Global Terrorism, 2000, in: Prados, America Confronts Terrorism, 2002, 111 *et seq.*; *Lake*, 6 Nightmares, 2000, page 33 *et seq.*; *Gordon*, Cyberterrorism, available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; United States National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, 2003, page 11 *et seq.*; OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

[999] The summit declaration calls for measures in the fight against cyberterrorism: "Effectively countering attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists". For more information, see: http://en.g8russia.ru/docs/17.html.

[1000] For more information, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1001] Final Declaration of the 2009 G8 ministerial meeting of Justice and Home Affairs, Rome, page 6, available at: www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf.

[1002] Final Declaration of the 2009 G8 ministerial meeting of Justice and Home Affairs, Rome, page 7, available at: www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf.

[1003] G8 Summit 2010 Muskoka Declaration, 2010, available at: www.g7.utoronto.ca/summit/2010muskoka/communique.html.

[1004] See press release from 30.5.2011, available at: www.eg8forum.com/en/documents/news/Final_press_release_May_30th.pdf.

[1005] See G8 Declaration, Renewed Commitment for Freedom and Democracy, available at: www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html.

[1006] The United Nations (UN) is an international organization founded in 1945. It had 192 Member States in 2010.

[1007] A/RES/44/25, adopted by the UN General Assembly on 12 December 1989.

[1008] A/RES/45/121, adopted by the UN General Assembly on 14 December 1990. The full text of the resolution is available at: www.un.org/documents/ga/res/45/a45r121.htm.

[1009] UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5), available at www.uncjin.org/Documents/EighthCongress.html.

[1010] See the preface to the Optional Protocol.

[1011] See Art. 2.

[1012] See especially the background paper: Crimes related to computer networks, A/CONF.187/10.

[1013] Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 165, available at: www.uncjin.org/Documents/congr10/15e.pdf.

[1014] Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 174, available at: www.uncjin.org/Documents/congr10/15e.pdf.

[1015] "The United Nations should take further action with regard to the provision of technical cooperation and assistance concerning crime related to computer networks".

[1016] A/RES/55/63. The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.

[1017] A/RES/56/121. The full text of the resolution is available at: http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf.

[1018] A/RES/57/239, on Creation of a global culture of cybersecurity; A/RES/58/199, on Creation of a global culture of cybersecurity and the protection of critical information infrastructure.

[1019] Measures to Combat Computer-related Crime, eleventh UN Congress on Crime Prevention and Criminal Justice, 2005, A/CONF.203/14.

[1020] Committee II Report, eleventh UN Congress on Crime Prevention and Criminal Justice, 2005, BKK/CP/19.

[1021] Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.2003/RPM.4/1, No. 14.

[1022] 30(d): "Considering the feasibility of negotiation of an international instrument on preventing and combating crimes involving information technologies", see: Discussion guide to the eleventh United Nations Congress on Crime Prevention and Criminal Justice, 2003, A/CONF.203/RM.1.

[1023] Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, available at: www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.

[1024] See in this context especially the background paper prepared by the secretariat.

[1025] "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

[1026] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

[1027] „The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

[1028] "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

[1029] *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009.

[1030] Regarding the focus of the debate, see: Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime, twelfth UN Congress on Crime Prevention and Criminal Justice, A/CONF.213/9.

[1031] Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress on Crime Prevention and Criminal Justice, Information Documents SG/Inf(2010)4, 16.02.2010, page 17 *et seq.*

[1032] Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

[1033] Resolutions 55/63 and 56/121.

[1034] Resolutions 57/239 and 58/199.

[1035] The report on the meeting of the open-ended working group (UNODC/CCPCJ/EG.4/2011/3) is available at: www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_3/UNODC_CCPCJ_EG4_2011_3_E.pdf.

[1036] Draft topics for consideration in a comprehensive study on the impact of and response to cybercrime, UNODC/CCPCJ/EG.4/2011/2. The document is available at: www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_2/UNODC_CCPCJ_EG4_2011_2_E.pdf.

[1037] The Commission on Crime Prevention and Criminal Justice (CCPCJ) was set up in 1991. It is a subsidiary body of the Economic and Social Council.

[1038] CCPCJ Resolution 16/2, on Effective crime prevention and criminal justice responses to combat sexual exploitation of children. Regarding the discussion process in the development of the resolution and for an overview of different existing legal instruments, see: Note by the Secretariat regarding Commission on Crime prevention and criminal justice responses to urban crime, including gang-related activities, and effective crime prevention and criminal justice responses to combat sexual exploitation of children, CN.15/2007/CRP.3, available at: www.unodc.org/pdf/crime/session16th/E_CN15_2007_CRP3_E.pdf. Regarding the initiative relating to the resolution, see: www.america.gov/st/washfile-english/2007/April/20070423135940ajesrom0.709469.html.

[1039] The United Nations Economic and Social Council (ECOSOC) is a principal organ to coordinate economic, social, and related work and serve as a central forum for discussing international economic and social issues. For more information, see: www.un.org/ecosoc/.

[1040] ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, available at: www.un.org/ecosoc/docs/2004/Resolution%202004-26.pdf.

[1041] For more information on the development process and the work of the intergovernmental expert group, see: Results of the second meeting of the Intergovernmental Expert Group to Prepare a study on Fraud and the Criminal Misuse and Falsification of Identity, Commission on Crime Prevention and Criminal Justice, 16th session, 2007, E/CN.15/2007/8, page 2.

[1042] ECOSOC Resolution 2007/20, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime, available at: www.un.org/ecosoc/docs/2007/Resolution%202007-20.pdf.

[1043] Regarding Internet-related ID-theft, see above: § 2.8.3, and below: § 6.2.16.

[1044] ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.

[1045] ECOSOC Resolution 2004/20, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.

[1046] Reports related to the activities of the working group are published. See: First meeting of the Core Group of Experts on Identity-Related Crime, Courmayeur Mont Blanc, Italy, 29-30 November 2007, available at: www.unodc.org/documents/organized-crime/Courmayeur_report.pdf (last visited: October 2008); Second meeting of the Core Group of Experts on Identity-Related Crime, Vienna, Austria, 2-3 June 2008, available at: www.unodc.org/documents/organized-crime/Final_Report_ID_C.pdf (last visited: October 2008).

[1047] See for example: Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, 2009, E/CN.15/2009/CRP.13.

[1048] ECOSOC Resolution 2004/42, on Sale of internationally controlled licit drugs to individuals via the Internet, available at: www.un.org/ecosoc/docs/2004/Resolution%202004-42.pdf.

[1049] For further information see: www.unodc.org/unodc/en/frontpage/2011/May/unodc-and-itu-to-cooperate-more-closely-to-make-the-internet-safer.html.

[1050] The International Telecommunication Union (ITU) with headquarters in Geneva was founded as the International Telegraph Union in 1865. It is a specialized agency of the United Nations. ITU has 192 Member States and more than 700 Sector Members and Associates. For more information, see: www.itu.int.

[1051] WSIS Geneva Plan of Action, 2003, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

[1052] WSIS Tunis Agenda for the Information Society, 2005, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

[1053] For more information on Action Line C5, see: www.itu.int/wsis/c5/, and also the meeting report of the second Facilitation Meeting for WSIS Action Line C5, 2007, page 1, available at: www.itu.int/osg/csd/cybersecurity/pgc/2007/events/docs/meetingreport.pdf and the meeting report of the third Facilitation Meeting for WSIS Action Line C5, 2008, available at: www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf.

[1054] For more information, see www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[1055] www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[1056] The five pillars are: legal measures, technical and procedural measures, organizational structures, capacity building, international cooperation. For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[1057] See: www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.

[1058] www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; See: *Gercke*, Zeitschrift fuer Urheber- und Medienrecht, 2009, Issue 7, page 533.

[1059] See, in this context: *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1, page 7 *et seq.*

[1060] Global Strategic Report, Chapter 1.6.

[1061] Global Strategic Report, Chapter 1.7.

[1062] Global Strategic Report, Chapter 1.10.

[1063] Global Strategic Report, Chapter 1.11.

[1064] 23-25 November 2009 (Santo Domingo, Dominican Republic): www.itu.int/ITU-D/cyb/events/2009/santo-domingo; 23-25 September 2009 (Hyderabad, India): 2009 ITU Regional Cybersecurity Forum for Asia-Pacific; 4-5 June 2009 (Tunis, Tunisia): 2009 ITU Regional Cybersecurity Forum for Africa and Arab States; 18-22 May 2009 (Geneva, Switzerland): WSIS Forum of Events 2009, including Action Line C5 dedicated to building confidence and security in the use of ICTs, and activities for child online protection; 7-9 September 2009 and 6-7 April 2009 (Geneva, Switzerland): ITU-D Rapporteur's Group Meeting on Question 22/1 on Securing Information and Communication Networks; 7-9 October 2008 (Sofia, Bulgaria): ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States (CIS); 25-28 August 2008 (Lusaka, Zambia): ITU Regional Cybersecurity Forum for Eastern and Western Africa; 15-18 July 2008 (Brisbane, Australia): ITU Regional Cybersecurity Forum for Asia Pacific and Seminar on the Economics of Cybersecurity; 18-21 February 2008 (Doha, Qatar): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) and Cybersecurity Forensics Workshop; 27-29 November 2007 (Praia, Cape Verde): ITU West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP, 29-31 October 2007 (Damascus, Syria): ITU Regional Workshop on E-Signatures and Identity Management; 16-18 October 2007 (Buenos Aires, Argentina): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP); 17 September 2007 (Geneva, Switzerland): Workshop on Frameworks for National Action: Cybersecurity and Critical Information Infrastructure Protection (CIIP); 28-31 August 2007 (Hanoi, Vietnam): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP).

[1065] The Council of Europe, based in Strasbourg and founded in 1949, is an international organization representing 47 Member States in the European region. The Council of Europe is not to be confused with the Council of the European Union and the European Council (informally called the European Summit), as the Council of Europe is not part of the European Union, but a separate organization. In the first edition of this guide, the Council of Europe Convention was listed as an international approach. In consistency with the status of the international debate and UNGA Resolution 60/177, it is characterized as a regional approach and has been moved to this section.

[1066] Twelfth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime in Strasbourg, 1976.

[1067] The Expert Committee consisted of 15 experts, as well as observers from Canada, Japan, United States, the EEC, OECD and UN. Source: *Nilsson* in *Sieber*, Information Technology Crime, page 577.

[1068] United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1069] *Nilsson* in Sieber, Information Technology Crime, page 576.

[1070] Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies.

[1071] Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers Deputies.

[1072] The Guidelines deal with investigative instruments (e.g. search and seizure) as well as electronic evidence and international cooperation.

[1073] Decision CDPC/103/211196. CDPC explained its decision by pointing out the international dimension of computer crimes: "By connecting to communication and information services, users create a kind of common space, called "cyber-space", which is used for legitimate purposes, but may also be the subject of misuse. These "cyber-space offences" are either committed against the integrity, availability and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities."

[1074] Explanatory Report of the Convention on Cybercrime (185), No. 10.

[1075] The full text of Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and ratifications are available at: www.coe.int.

[1076] For more details about the offences covered by the Convention, see below: § 6.2.; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*,
The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

[1077] Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Turkey, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

[1078] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Moldova, Montenegro, Netherlands, Norway, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, The Former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, United States.

[1079] The need for a ratification is laid down in Article 36 of the Convention on Cybercrime:

> *Article 36 – Signature and entry into force*
>
> *1) This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.*
>
> *2)This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.*

[1080] Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico and Philippines.

[1081] Interpol highlighted the importance of the Convention on Cybercrime in the resolution of the 6th International Conference on Cyber Crime, Cairo: "That the Convention on Cybercrime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be

encouraged to consider joining it. The Convention on Cybercrime shall be distributed to all Interpol member countries in the four official languages", available at: www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp; The 2005 WSIS Tunis Agenda states: "We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime", available at: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf; APEC called for economies to study the Convention on Cybercrime, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; OAS called for an evaluation of the Convention while designing Cybercrime legislation, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 19, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

[1082] Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

[1083] Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime No. 4: "The committee drafting the Convention on Cybercrime discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention on Cybercrime."

[1084] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1085] United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 234, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1086] See Art. 3 of the Fourth Draft Convention, PC-CY (98) Draft No. 4, 17.04.1998.

[1087] Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Canada, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Italy, Latvia, Lichtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovenia, Sweden, Switzerland, South Africa, The Former Yugoslav Republic of Macedonia, Turkey, Ukraine.

[1088] Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Finland, France, Germany, Latvia, Lithuania, Montenegro, Netherlands, Norway, Portugal, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine.

[1089] Interpol highlighted the importance of the Convention on Cybercrime in the resolution of the 6th International Conference on Cyber Crime, Cairo: "That the Convention on Cybercrime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it. The Convention shall be distributed to all Interpol member countries in the four official languages", available at: www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp. The 2005 WSIS Tunis Agenda states: "We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime", available at: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf.

[1090] For more information on the achievements and shortcomings see: *Gercke*, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq.

[1091] Draft Code of Criminal Procedure, written by the Advisory Committee on the Reform of Criminal Procedural Legislation, set up by Decree No. 115 of the National Executive Power of 13 February 2007 (Boletín Oficial of 16 February 2007).

[1092] Draft Electronic Crime Act 2006.

[1093] Draft Act Defining Cybercrime, providing for Prevention, Suppression and Imposition of Penalties therefore and for other Purposes, House Bill No. 3777.

[1094] Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

[1095] Draft Cybercrime and Computer related Crimes Bill 2007, Bill No. 17 of 2007.

[1096] Draft Computer Security and Critical Information Infrastructure Protection Bill 2005.

[1097] Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress, ID SG/Inf(2010)4, 2010, page 18.

[1098] Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines and Senegal.

[1099] Albania, Croatia,

[1100] Estonia, Hungary.

[1101] Lithuania, Romania, Slovenia, The former Yugoslav Republic of Macedonia.

[1102] Bulgaria, Cyprus, Denmark.

[1103] Armenia, Bosnia and Herzegovina, France, Netherlands, Norway, Ukraine, United States.

[1104] Finland, Iceland, Latvia.

[1105] Italy, Slovakia.

[1106] Germany, Moldova, Serbia.

[1107] Azerbaijan, Montenegro, Portugal, Spain.

[1108] United Kingdom, Switzerland.

[1109] See Sec. 202a of the German Penal Code.

[1110] Country profiles can be downloaded at www.coe.int/cybercrime.

[1111] For details on the requirements, see: *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025, available at: www.fas.org/sgp/crs/misc/97-1025.pdf.

[1112] *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007, page 28, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

[1113] See in this context, for example: *OECD*, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4,

[1114] See Art. 44 Convention on Cybercrime.

[1115] "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

[1116] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

[1117] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

[1118] "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

[1119] *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009.

[1120] Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

[1121] See *Gercke*, How Terrorist Use the Internet in *Pieth/Thelesklaf/Ivory*, Countering Terrorist Financing, 2009, page 127-150.

[1122] Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

[1123] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Criminal Responsibility for Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.8.4. Regarding the legal response to phishing, see: *Lynch*, Identity Theft in Cyberspace: Crime Control, Berkeley Tech. Law Journal, 2005, 259; *Hoffhagle*, Identity Theft: Making the Known Unknowns Known, Harvard Journal of Law & Technology, Vol. 21, No. 1, 2007, page 97 *et seq.*

[1124] Criticism about the lack of coverage of such topics in the existing instruments: *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07, page 7.

[1125] See: Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, COM(2010) 517, page 6.

[1126] *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007, page 28, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

[1127] See Art. 44 Convention on Cybercrime.

[1128] See Art. 37 Convention on Cybercrime.

[1129] "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

[1130] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

[1131] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

[1132] "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

[1133] See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

[1134] See: Art. 41 Salvador Declaration on Comprehensive Strategies for Global Challenges, 2010. Available at: www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf.

[1135] See ITU Resolution 130 (Rev. Guadalajara, 2010).

[1136] Andorra, Monaco and San Marino did not even sign the Convention. Lichtenstein and Malta signed but never ratified the Convention.

[1137] See Explanatory Report to the Convention on Cybercrime, No. 298.

[1138] *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf

[1139] The Functioning of 24/7 points of contact for cybercrime, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf.

[1140] ICB4PAC Workshop on Concepts and Techniques of Developing CyberCrime Policy and Legislation, Apia, Samoa 22-25 August 2011.

[1141] Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress, ID SG/Inf(2010)4, 2010, No. 47.

[1142] Model Law on Computer and Computer Related Crime, LMM(02)17. For more information about the Model Law see:

[1143] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union E-Commerce Regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*

[1144] For further information and references on electronic evidence see blow: § 6.5.

[1145] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historical development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.

[1146] Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

[1147] Austria, Belgium, Bulgaria, Croatia, Cyprus, Finland, France, Germany, Greece, Ireland, Lithuania, Moldova, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovenia, Sweden, The former Yugoslav Republic of Macedonia and Turkey. Albania, Armenia, Azerbaijan, Denmark, Estonia, Georgia, Hungary, Iceland, Italy, Liechtenstein, Luxembourg, Malta, Monaco, Montenegro, Slovakia, Spain, Switzerland, Ukraine and the United Kingdom followed.

[1148] Albania Austria, Denmark, France, Greece, Malta, Montenegro, Netherlands, San Marino, Serbia and Spain.

[1149] For more details, see: *Gercke*, The Development of Cybercrime Law, Zeitschrift fuer Urheber- und Medienrecht 2008, 550ff.

[1150] The European Union is a supranational and intergovernmental union with, as at today, 27 Member States from the European continent.

[1151] One example is the EU funded HIPCAR project on Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures. For more information, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1152] *Herlin-Karnell*, Commission v. Council: Some reflections on criminal law in the first pillar, European Public Law, 2007, page 69 *et seq.*; *Herlin-Karnell,* Recent developments in the area of European criminal law, Maastricht Journal of European and Comparative Law, 2007, page 15 *et seq.*; *Ambos*, Is the development of a common substantive criminal law for Europe possible? Some preliminary reflections, Maastricht Journal of European and Comparative Law, 2005, 173 *et seq.*

[1153] See: *Satzger*, International and European Criminal Law, 2005, page 84 for further reference.

[1154] Title VI, Treaty on European Union.

[1155] Framework Decision 2003/80/JHI, OJ L 29, 5.2.2003.

[1156] Decision of the Court of Justice of the European Communities, 13.09.2005, Case C-176/03. See in this context: *Gercke.*

[1157] Communication from the Commission to the European Parliament and the Council on the implications of the Court's judgement of 13 September 2005 (Case C-176/03 Commission v Council), 24.11.2005, COM(2005) 583.

[1158] Decision of the Court of Justice of the European Communities, 23.10.2007, Case C-440/05; See in this context: *Eisele*, Anmerkung zum Urteil des EuGH C 440/05, JZ 2008, page 251 *et seq.*; *Fromm*, Anmerkung zum Urteil des EuGH C 440/05, ZIS 2008, page 168 *et seq.*

[1159] ABl. 2007 C 306, 1.

[1160] Regarding the impact of the reform on the harmonization of criminal law, see: *Peers*, EU criminal law and the Treaty of Lisbon, European law review 2008, page 507 *et seq.*; *Zeder*, EU-minimum rules in substantive penal law: What will be new with the Lisbon Treaty?, ERA Forum 2008, page 209 *et seq.*

[1161] Stockholm Programme, An open and secure Europe serving and protecting the citizens, 2009.

[1162] Regarding the Hague Programme, see: *Braum*, Das Haager-Programm der Europaeischen Union: falsche und richtige Schwerpunkte europaeischer Strafrechtsentwicklung in *Joerden/Szwarc*, Europaeisierung des Strafrechts in Deutschland und Polen, 2007, page 11 *et seq.*

[1163] See: Stockholm Programme, An open and secure Europe serving and protecting the citizens, 2009, No. 3.3.1.

[1164] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487.

[1165] See: Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487, page 24.

[1166] Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (276/1999/EC).

[1167] Communication of 8 December 1999 on a Commission initiative for The Lisbon Special European Council, 23 and 24 March 2000 – *e*Europe – An information society for all – COM 1999, 687. See in this regard also: *Buono*, Investigating and prosecuting crimes in cyberspace, to be published in ERA Forum 2010.

[1168] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, 26.1.2001, COM(2000) 890.

[1169] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890, page 23.

[1170] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890, page 23.

[1171] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM (2000) 890, page 31.

[1172] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM (2000) 890, page 32.

[1173] Network and Information Security – A European Policy approach – adopted 6 June 2001.

[1174] For example the Council in 1999, available at: http://db.consilium.eu.int/de/Info/eurocouncil/index.htm.

[1175] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM (2007) 267. For more information see: ITU Global

Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1176] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union E-Commerce Regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*

[1177] See *Lindholm/Maennel*, Computer Law Review International 2000, 65.

[1178] See Directive 2000/31/EC, recital 1 *et seq.*

[1179] For more details, see below: § 6.

[1180] *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010, page 75 *et seq.*

[1181] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487.

[1182] Decision No. 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (276/1999/EC).

[1183] Council Framework Decision of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA).

[1184] See Art. 4 of the Framework Decision.

[1185] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. The legal basis for the Framework Decision, indicated in the preamble of the proposal for the Framework Decision is Articles 29, 30(a), 31 and 34(2)(b) of the Treaty on European Union. See: *Gercke*, Framework Decision on Attacks against Information Systems, CR 2005, 468 *et seq.*; *Sensburg*, Schutz vor Angriffen auf Informationssystem: Weiterer Schritt zum europaeischen Strafrecht?, Kriminalistik 2007, page 607ff.

[1186] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[1187] See the explanation of the Framework Decision in the Proposal For A Council Framework Decision on combating serious attacks against information systems, No. 1.6.

[1188] Council Framework Decision 2005/222/JHA of 24.02.2005 on attacks against information systems, recital 5.

[1189] Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communication networks and amending directive 2002/58/EC. Document 2005/0182/COD.

[1190] *Gercke*, The Development of Cybercrime Law in 2005, Zeitschrift fuer Urheber- und Medienrecht 2006, page 286.

[1191] European Court of Justice, Case C-275/06.

[1192] See: Advocate General Opinion – 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top. The court usually but not invariably follows the adviser's conclusion.

[1193] In a G8 meeting in Tokyo, experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding implementation of a data retention obligation. Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001.

[1194] Data Retention Directive, recital 6.

[1195] Data Retention Directive, recital 6.

[1196] Case C-301/06.

[1197] Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

[1198] "Article 4 of the Framework Decision on combating terrorism states that inciting, aiding or abetting terrorist offences should be made punishable by the Member States. Article 2 of the same instrument requires Member States to hold those directing a terrorist group or participating in its activities criminally liable. However, these provisions do not explicitly cover the dissemination of terrorist propaganda and terrorist expertise, in particular through the Internet."

[1199] "Training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing one of the acts listed in Article 1(1), knowing that the skills provided are intended to be used for this purpose.

[1200] Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, COM (2010) 94.

[1201] Directive 2011/92/EU of the European Parliament and of The Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

[1202] See: Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, page 2.

[1203] ETS 201. For more information see: § 5.2.1

[1204] See Art. 5, No. 3, of the Draft Directive.

[1205] Regarding the challenges related to the use of encryption technology, see above: § 3.2.13. One survey on child pornography suggested that only 6 per cent of arrested child pornography possessors used encryption technology. See: *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

[1206] See Explanatory Report to the Convention on the Protection of Children, No. 140.

[1207] The download is in general necessary to enable the display of the information on the website. Depending on the configuration of the browser, the information can be downloaded to cache and temp files or just stored in the RAM memory of the computer. Regarding the forensic aspects of this download, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 180.

[1208] Regarding the underlying technology, see: *Austerberrry*, The Technology of Video & Audio Streaming, 2004, page 130 *et seq.*; *Wu/Hou/Zhu/Zhang/Peha*, Streaming Video over the Internet: Approaches and Directions, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 11, No. 3, 2001, page 282 *et seq.*; *Garfia/Pau/Rico/Gerla*, P2P Streaming Systems: A Survey and Experiments, 2008.

[1209] Regarding filter obligations/approaches, see*: Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 *et seq.*; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008; *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide.

[1210] See *Gercke*, The Role of Internet Service Providers in the Fight against Child Pornography, Computer Law Review International, 2009, page 69 *et seq.*

[1211] *Clayton/Murdoch/Watson*, Ignoring the Great Firewall of China, available at: www.cl.cam.ac.uk/~rnc1/ignoring.pdf; *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 53; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73.

[1212] *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73.

[1213] *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 55.

[1214] *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf.

[1215] *Callanan/Gercke/De Marco/Dries-Ziekenheiner*, Internet Blocking – Balancing Cybercrime Responses in Democratic Societies, 2009, page 131 *et seq.*; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page ix.

[1216] Proposal for a Directive of the European Parliament and the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA.

[1217] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[1218] Proposal for a Directive of the European Parliament and the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, page 3.

[1219] 1999/364/JHA: Common Position of 27 May 1999 adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the draft Convention on Cyber Crime held in the Council of Europe.

[1220] See Art. 1 of the Common Position.

[1221] See in this context: *Buono*, Investigating and prosecuting crimes in cyberspace, to be published in ERA Forum 2010.

[1222] See *Gercke*, The Slow Awake of a Global Approach against Cybercrime, Computer Law Review International, page 145.

[1223] The Organisation for Economic Co-operation and Development was founded 1961. It has 34 member countries and is based in Paris. For more information, see: www.oecd.org.

[1224] *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 8, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1225] OECD, Computer-related Criminality: Analysis of Legal Policy in the OECD Area, OECD, Report DSTI-ICCP 84.22 of 18 April 1986.

[1226] In 1992, the Council of the OECD adopted the Recommendation concerning Guidelines for the Security of Information Systems. The 24 OECD member countries adopted the guidelines later.

[1227] Adopted by the OECD Council at its 1037th session on 25 July 2002. The 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, available at: www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.

[1228] Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1229] See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1230] The report is available at: www.legislationline.org/upload/lawreviews/6c/8b/82fbe0f348b5153338e15b446ae1.pdf.

[1231] Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, 2008, available at: www.oecd.org/dataoecd/35/24/40644196.pdf.

[1232] Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, 2008, page 5, available at: www.oecd.org/dataoecd/35/24/40644196.pdf.

[1233] Computer Viruses and other malicious software: A threat to the internet economy, OECD, 2009.

[1234] The Asia-Pacific Economic Cooperation (APEC) is a group of Pacific Rim countries dealing with the improvement of economic and political ties. It has 21 members.

[1235] "We also call for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime." APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, 26 October 2002.

[1236] The Ministers stated in the declaration "their call for continued collaboration and sharing of information and experience between member economies to support a safe and trusted ICT environment including effective responses to ensure security against cyber threats, malicious attacks and spam." For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html.

[1237] Australia, Brunei Darussalam, Canada, China, Hong Kong, Japan, Korea, Malaysia, New Zealand, Philippines, Singapore, Chinese Taipei, Thailand and United States.

[1238] See: Report to Leaders and Ministers on Actions of the Telecommunications and Information Working Group to Address Cybercrime and Cybersecurity, 2003/AMM/017.

[1239] APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, on 26 October 2002. Regarding national legislation on cybercrime in the Asian-Pacific region, see: *Urbas*, Cybercrime Legislation in the Asia-Pacific Region, 2001, available at: www.aic.gov.au/conferences/other/urbas_gregor/2001-04-cybercrime.pdf. See also

in this regard: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1240] APEC TEL-OECD Malware Workshop (2007); APEC TEL and ASEAN Workshop on Network Security (2007); Workshop on Cyber Security and Critical Information Infrastructure Protection (CIIP); APEC Symposium on Spam and Related Threats (2007); APEC Best Practices In International Investigations Training Sessions (2004); Conference on cybercrime for the APEC region (2005); Conference on cybercrime for the APEC region (2004); Conference on cybercrime for the APEC region (2003); Cybercrime legislation training workshops (several, 2003); Judge and Prosecutor Capacity Building Project.

[1241] "We also call for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime." APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, 26 October 2002.

[1242] Cybercrime Legislation and Enforcement Capacity Building Project – 3rd Conference of Experts and Training Seminar, APEC Telecommunications and Information Working Group, 32nd Meeting, 5-9 September 2005, Seoul, Korea.

[1243] "Economies are currently implementing and enacting cybersecurity laws, consistent with the UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001). The TEL Cybercrime Legislation initiative and Enforcement Capacity Building Project will support institutions to implement new laws."

[1244] The APEC Telecommunications and Information Working Group was founded in 1990. It aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing information policies. For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

[1245] For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/som/mtg/2002/word.Par.0204.File.v1.1

[1246] See: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

[1247] Cybercrime Legislation & Enforcement Capacity Building Workshop, and Electronic Commerce Steering Group Meeting.

[1248] 2003/SOMIII/ECSG/O21.

[1249] *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf.

[1250] See: Model Law on Computer and Computer Related Crime, LMM(02)17, Background information.

[1251] See: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf (Annex 1).

[1252] Model Law on Computer and Computer Related Crime, LMM(02)17; the Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1253] Draft Model Law on Electronic Evidence, LMM(02)12.

[1254] For more information see: www.waigf.org/IMG/pdf/Cybercrime_Initiative_Outline.pdf.

[1255] For more information see: African Union, Oliver Tambo Declaration, Johannesburg 2009, available at: www.uneca.org/aisi/docs/AU/The%20Oliver%20Tambo%20Declaration.pdf.

[1256] The Draft Convention is available for download at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf

[1257] See Part 1, Sec. II, Ch. II.

[1258] See Part 1, Sec. IV.

[1259] See Part 1, Sec. V.

[1260] See Part 2.

[1261] Art. III-1.

[1262] Part 3, Chaptr 1, Art. 1 and Art. 2.

[1263] Art. III-1-1 to Art. III-1-7

[1264] Art. III-1-8 to Art. III-1-12.

[1265] Art. III-2.

[1266] Art. III-3.

[1267] Art. III-4.

[1268] Art. III-5.

[1269] Art. III-6.

[1270] Art. III-7 1).

[1271] For more information see below: § 6.2.2.

[1272] Art. III-8.

[1273] Art. III-9.

[1274] Art. III-10.

[1275] Art. III-11.

[1276] Art. III-12.

[1277] Art. III-13.

[1278] Art. III-14.

[1279] Art. III-15.

[1280] Art. III-16.

[1281] Art. III-17.

[1282] Art. III-19.

[1283] Art. III-20.

[1284] Art. III-21.

[1285] Art. III-22.

[1286] Art. III-24.

[1287] Art. III-25.

[1288] Art. III-26.

[1289] Art. III-27.

[1290] Art. III-36.

[1291] Art. III-37.

[1292] Art. III-39.

[1293] Art. III-41.

[1294] The League of Arab States is a regional organization, with currently 22 members.

[1295] See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 20, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1296] Draft Electronic Crime Act 2006.

[1297] Draft Law on Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

[1298] Law No. 2 of 2006, enacted in February 2006.

[1299] Regional Conference Booklet on: Cybercrime, Morocco, 2007, page 6, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

[1300] Decision of the Arab Justice Ministers Council, 19th session, 495-D19-8/10/2003.

[1301] Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and UAE.

[1302] Non-official translation of the recommendations of the Conference on Combating Cybercrime in the GCC Countries, 18 June 2007, Abu Dhabi:
1) Calling for the adoption of a treaty by the Gulf Cooperation Council (GCC) countries, inspired by the Council of Europe Cybercrime convention, to be expanded later to all Arab countries.
2) Calling all GCC countries to adopt laws combating cybercrime inspired by the model of the UAE cybercrime Law.
3) Calling for the adoption of laws in relation to procedural matters such as seizure, inspection and other investigation procedures for such special type of crimes.
5) Providing trainings to inspection and law enforcement officials on dealing with such crimes.
6) Providing sufficient number of experts highly qualified in new technologies and cybercrime particularly in regard to proof and collecting evidence.
7) Recourse to the Council of Europe's expertise in regard to combating cybercrime particularly in regard to studies and other services which would contribute in the elaboration and development of local countries legislation in GCC countries.
8) Harmonization of the legislations in Arab and particularly GCC countries in regard to basic principles in combating this type of crimes on both procedural and substantive level.
9) Increasing cooperation between public and private sectors in the intent of raising awareness and exchange of information in the cybercrime combating field.

[1303] The Organization of American States is an international organization with 34 active Member States. For more information, see: www.oas.org/documents/eng/memberstates.asp.

[1304] For more information, see: www.oas.org/juridico/english/cyber.htm, and the Final report of the Fifth Meeting of REMJA, which contains the full list of reports, results of the plenary session and conclusions and recommendations, at: www.oas.org/juridico/english/ministry_of_justice_v.htm.

[1305] The conclusions and recommendation of the meetings of Ministers of Justice or of Ministers or Attorneys General of the Americas on Cyber Crime are available at: www.oas.org/juridico/english/cyber_meet.htm.

[1306] The full list of recommendations from the 2000 meeting is available at: www.oas.org/juridico/english/ministry_of_justice_iii_meeting.htm#Cyber. The full list of recommendations from the 2003 meeting is available at: www.oas.org/juridico/english/ministry_of_justice_v.htm.

[1307] The OAS General Secretariat, through the Office of Legal Cooperation of the Department of International Legal Affairs, serves as the technical secretariat to this Group of Experts, pursuant to the resolutions of the OAS General Assembly. More information on the Office of Legal Cooperation is available at: www.oas.org/dil/department_office_legal_cooperation.htm.

[1308] In addition, the Working Group of Governmental Experts on cybercrime recommended that training be provided in the management of electronic evidence and that a training programme be developed to facilitate states link-up to the 24 hour/7 day emergency network established by the G8 to help conduct cybercrime investigations. Pursuant to such recommendation, three OAS regional technical workshops were held during 2006 and 2007, the first being offered by Brazil and the United States, and the second and third by the United States. The list of technical workshops is available at: www.oas.org/juridico/english/cyber_tech_wrkshp.htm.

[1309] In the meantime, OAS has established joint collaboration with the Council of Europe and attended and participated in the 2007 Octopus Interface Conference on Cooperation against cybercrime. See: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/Interface2007_en.asp.

[1310] Conclusions and Recommendations of REMJA-VII, 2008, are available at: www.oas.org/juridico/english/cybVII_CR.pdf.

[1311] Conclusions and Recommendations of REMJA-VIII, 2010, are available at: www.oas.org/en/sla/dlc/remja/recom_VIII_en.pdf.

[1312] For more information about the project, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1313] The beneficiary countries are: Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname and Trinidad and Tobago.

[1314] CARIFORUM is a regional organization of 15 independent countries in the Caribbean region (Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago).

[1315] Electronic transactions, Electronic evidence in e-commerce, Privacy and data protection, Interception of communications, Cybercrime, Access to public information (freedom of information), Universal access and service, Interconnection and access and finally Licensing.

[1316] The assessment report is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1317] The workshop was held in Saint Lucia on 8-12 March 2010. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1318] For further information about the project see: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

[1319] Cook Islands, East Timor, Fiji, Kiribati, Marshall Islands, Federated States of Micronesia, Nauru, Niue, Palau, Papua New Guinea, Samoa, Salomon Islands, Tonga, Tuvalu and Vanuatu.

[1320] More information about the event are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/events/2011/port_vila/port_vila.html.

[1321] The assessment report will be made available through the project website.

[1322] www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/events/2011/samoa/samoa.html.

[1323] More information about the event are available at: www.spc.int/en/component/content/article/704-responding-to-cybercrime-threats-in-the-pacific.html.

[1324] An overview about the output of the conference is available at: and www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_tonga_apr_11/AGREED_Cybercrime_Workshop_Outcomes.pdf.

[1325] *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf.

[1326] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf ; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf. ABA International Guide to Combating Cybercrime, 2002, page 78.

[1327] Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention, see below: § 6.2; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cybercrime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No. 4, 2001, page 889 *et seq*.

[1328] Regarding the application of Art. 23 *et seq.* with regard to traditional crimes, see: Explanatory Report to the Convention on Cybercrime, No. 243.

[1329] *Schjolberg*, A Cyberspace Treaty – A United Nations Convention or Protocol on Cybersecurity and Cybercrime, twelfth UN Crime Congress, 2010, A/CONF.213, page 3, available at: www.cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf.

[1330] *Schjolberg/Ghernaouti-Helie*, A Global Protocol on Cybersecurity and Cybercrime, 2009, available at: www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf.

[1331] For details, see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 *et seq.*

[1332] "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations, No. 41 (page 10); "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations, No. 47 (page 10); "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations, No. 29 (page 7); "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations, No. 40 (page 10).

[1333] Meeting Report, The Cybercrime Convention Committee, 2nd Multilateral Consultation of the Parties, 2007, page 2, available at: www.coe.int/t/e/legal_affairs/legal_co%2Doperation/combating_economic_crime/6_cybercrime/t%2Dcy/FINAL%20T-CY%20_2007_%2003%20-%20e%20-%20Report%20of%20the%20meeting1.pdf.

[1334] The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions, see *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. Regarding the phenomenon of phishing, see *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, available at: www.usdoj.gov/opa/report_on_phishing.pdf.

[1335] For an overview of the different legal approaches, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf. See also: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm. Regarding the economic impact, see for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

[1336] There are two aspects that need to be taken into consideration in this context: To avoid redundancy, a new approach should focus on offences that are not intended to be covered within further amendments of the Convention on Cybercrime. The second aspect is related to the difficulties in finding a common position all countries can agree on. Based on the experiences with the negotiations of the Convention on cybercrime, it is likely that negotiations of criminalization that go beyond the standards of the Convention will run into difficulties.

[1337] Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1338] Regarding the need for international cooperation in the fight against cybercrime, see: *Putnam/Elliott*, International Responses to Cybercrime, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, page 35 *et seq*., available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, page 1 *et seq*., available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1339] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties which the dual criminality principle can cause within international investigations is currently addressed in a number of international conventions and treaties. One example is Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and surrender procedures between Member States (2002/584/JHA).

[1340] Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1341] See Convention on Cybercrime, Articles 23-35.

[1342] See *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141 *et seq.*

[1343] See above: § 2.6.7.

[1344] See Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1345] See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1346] Regarding the network protocols, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

[1347] See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*., available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper, No. 3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

[1348] Regarding the international dimension, see above: § 3.2.6.

[1349] With regard to the Convention on Cybercrime, see: Explanatory Report to the Convention on Cybercrime, No. 33.

[1350] Regarding concerns related to the speed of the ratification process, see *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 144.

[1351] See below: § 6.2.10.

[1352] See above: §§ 3.2.6 and 3.2.7.

[1353] The issue has been addressed by a number of international organizations. UN General Assembly Resolution 55/63 stipulates: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 Ten-Point Action Plan highlights: "There must be no safe havens for those who abuse information technologies".

[1354] For details, see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*

[1355] For an overview of the law, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analysed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm. For more information, see below: § 6.2.11.

[1356] Regarding filter obligations/approaches, see: *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion on filtering in different countries, see: *Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No. 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches,
see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf; *Zittrain*, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.*

[1357] See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: *www.juriscom.net/en/uni/doc/yahoo/poullet.htm*; *Goldsmith/Wu*, Who Controls the Internet?: Illusions of a Borderless World, 2006, page 2 *et seq.*

[1358] The OpenNet Initiative is a transatlantic group of academic institutions that reports about Internet filtering and surveillance. Among others, the Harvard Law School and the University of Oxford participate in the network. For more information, see: www.opennet.net.

[1359] *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

# 6. Legal response

The following chapter will provide an overview of legal response to the phenomenon of cybercrime by explaining legal approaches in criminalizing certain acts.[1360] Wherever possible, international approaches will be presented. In cases where international approaches are lacking, examples of national or regional approaches will be provided.

## 6.1 Definitions

Bibliography (selected): *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 253 et seq; *Lindahl,* Deduction and Justification in the Law. Role of Legal Terms and Conditions, Ratio Juris, Vol. 17, Iss. 2, 2004, page 182 et seq.; *Macagno*, Definitions in Law, Bulletin Suisse de Linguistique Appliquée, Vol. 2, 2010, page 199 et seq, available at: http://ssrn.com/abstract=1742946.

### *6.1.1 The function of definitions*

Definitions are a common element of various national and regional legal frameworks. However it is important to differentiate between different functions that those definitions have. In law it is in general possible to divide into two classes of definitions: descriptive and statutory definitions.[1361] Descriptive definitions are used to explain the meaning of ambiguous words while statutory definitions intend to commit those that are subject to law to a particular definition of a word.[1362] The following overview does not distinguish between those two types of definition.

Regional legal frameworks and model laws do not only follow different concepts with regard to the type of definitions but also when it comes to quantitative aspects. The Convention on Cybercrime, for example, only contains five definitions[1363] while the HIPCAR Model Legislative Text on Cybercrime contains twenty.

### *6.1.2 Access provider*

Access providers play an important role as they enable users to connect to the Internet. In cybercrime law the term access provider is used both with regard to the regulation of liability[1364] as well as the involvement in investigations – especially the lawful interception of communication.[1365] A definition of the term is provided in the HIPCAR Model Legislative Text on Cybercrime.

***Definitions***
***3.*** *(1) Access provider means any natural or legal person providing an electronic data transmission service by transmitting information provided by or to a user of the service in a communication network or providing access to a communication network.*
*[…]*

The provision is broad as it covers commercial providers as well as companies that only provide access for employees and operators of private networks. While this approach is useful when it comes to a wide application of liability regulations, it could lead to challenges if the definition is also applied in procedural law (which was not intended by the drafters of the HIPCAR Model Legislative Text).

### *6.1.3 Caching provider*

Caching providers provide an important service to increase the speed of access to popular content. With regard to the need to regulate the liability[1366] of caching providers, the drafters of the HIPCAR Model Legislative Text on Cybercrime decided to include a definition.

***Definitions***

> ***3.*** *[…]*
> *(2) Caching provider means any natural or legal person providing an electronic data transmission service by automatic, intermediate and temporary storing information, performed for the sole purpose of making more efficient the information's onward transmission to other users of the service upon their request;*
> *[…]*

Just like their definition for access provider, the drafters did not limit the application of the provision to commercial operations. As a consequence the provision also covers companies and private network operators.

### 6.1.4 Child

The term child is especially relevant with regard to the criminalization of child pornography.[1367] It is also used in the context of provisions that criminalize making certain content (for example adult pornography) available to minors.[1368] One of the most frequently used definitions is provided in the UN Convention on the Rights of the Child from 1989.

> *For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.*

Several cybercrime-specific legal frameworks and model laws, such as the 2011 EU Directive on combating child pornography[1369], the 2007 Council of Europe Convention on the Protection of Children[1370] and the 2009 HIPCAR Model Legislative Text on Cybercrime[1371] contain similar definitions. The Council of Europe Convention on Cybercrime does not define child but only child pornography.

### 6.1.5 Child pornography

Child pornography is one of the few offences related to the category of illegal content where most countries in the world agree to a criminalization.[1372] As the differentiation between legal forms of sexual-related material and child pornography can be challenging, some legal frameworks provide a definition of child pornography.

One major challenge for law drafters in this regard is to avoid conflicts between different categories of age in order to avoid a potentially unintended criminalization in cases where the age of marriage or sexual consent and the age-limit within the definition of child pornography differ.[1373] If, for example, child pornography is defined as visual depiction of sexual acts of a person below the age of 18 and at the same time the age of sexual consent and marriage is 16, two 17 year old children can legally get married or have a sexual relationship but will be committing a serious crime (production of child pornography) if they take pictures or movies of this act.[1374]

One definition is provided by Article 2 c) of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

> ***Article 2***
> *For the purpose of the present Protocol:*
> *[…]*
> *(c) Child pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.*

The definition provided in the Optional Protocol does not explicitly cover forms of fictional child pornography such as realistic images. To ensure that such material is also covered some legal frameworks, such as the Council of Europe Convention on Cybercrime, have amended the definition of child pornography.

***Article 9 – Offences related to child pornography***
*[…]*
*(2) For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:*
*a) a minor engaged in sexually explicit conduct;*
*b) a person appearing to be a minor engaged in sexually explicit conduct;*
*c) realistic images representing a minor engaged in sexually explicit conduct.*
*(3) For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.*
*[…]*

Article 9, paragraph 2, provides three subsections on material that visually depicts child pornography: a minor engaged in sexually explicit conduct, a person appearing to be a minor engaged in sexually explicit conduct and realistic images representing a minor engaged in sexually explicit conduct.

While in this regard the Convention on Cybercrime expands the definition provided in the Optional Protocol to the UN Convention, on the other hand it narrows the applicability in two important aspects.

Although the drafters of the Convention on Cybercrime emphasised the importance of a uniform international standard regarding age[1375] the Convention on Cybercrime nevertheless permits parties to require a different age limit of not lower than 16 years.

The second major difference to the definition provided in the Optional Protocol is the fact that the definition in the Council of Europe Convention on Cybercrime focuses on visual depiction. Child pornography is not necessary distributed as pictures or movies, but also as audio files.[1376] Due to the fact that the provision provided in Article 9 refers to "material that visually depicts" a child, the provision does not cover audio files.

As a consequence, more recent approaches such as the HIPCAR[1377] cybercrime legislative text[1378] follow the concept of the Option Protocol to the UN Convention instead of the Council of Europe Convention and avoid the term "visually".

***Definitions***
***3.***
*[…](4) Child pornography means pornographic material that depicts presents or represents:*
*a) a child engaged in sexually explicit conduct;*
*b) a person appearing to be a child engaged in sexually explicit conduct; or*
*c) images representing a child engaged in sexually explicit conduct;*
*this includes, but is not limited to, any audio, visual or text pornographic material.*
*A country may restrict the criminalisation by not implementing (b) and (c).*

Definitions of child pornography are also contained in the 2011 EU Directive on combating child pornography[1379], and the 2007 Council of Europe Convention on the Protection of Children.[1380]

### 6.1.6 Computer data

The increasing use of computer technology as well as the trend to digitalization of data led to an increasing relevance of computer data. As a consequence computer data has become a frequent target of attacks that range from data interference[1381] to data espionage.[1382] Various regional frameworks contain definitions for computer data. One example is section 3 of the Commonwealth Model Law on Computer and Computer-related Crime.

***Definitions***
***3.*** *In this Act, unless the contrary intention appears:*
*"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;*
*[…]*

Similar definitions are contained in the 2001 Council of Europe Convention on Cybercrime[1383], the 2005 EU Council Framework Decision on attacks against information systems[1384], 2008 Draft ECOWAS Directive on Fighting Cyber Crime[1385], and the 2009 HIPCAR Model Legislative Text on Cybercrime[1386].

### 6.1.7 Computer data storage device

Storage devices play an important role with regard to cybercrime – both with regard to possible data interference as well as with regard to the seizure of evidence. One example for a regional framework that contains a definition is section 3 if the Commonwealth Model Law on Computer and Computer-related Crime.

***Definitions***
***3.***
*[…]*
*"computer data storage medium" means any article or material (for example, a disk) from which information is capable of being reproduced, with or without the aid of any other article or device;*
*[…]*

A similar definition is contained in HIPCAR Model Legislative Text.[1387]

### 6.1.8 Computer system

In cybercrime laws the term computer system is used in relation to substantive criminal law as well as procedural law. Computer systems can be the target of an attack; they can be used as a tool when committing a crime and finally can be seized as evidence. Consequently most applicable regional frameworks and model laws contain such a definition. One example is section 3 of the 2002 Commonwealth Model Law on Computer and Computer-related Crime.

***Definitions***
***3.***
*[…]*
*"computer system" means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function;*
*[…]*

One unusual aspect is the fact that the definition mentions "the Internet". The Internet is widely defined as a system of interconnected networks.[1388] From a technical perspective the Internet itself is therefore not a computer system but a network and should consequently not be included in the definition of computer systems but may be included in the definition of computer networks. However, several drafters of legal frameworks followed the example of the Commonwealth Model Law and included the Internet in the definition of computer system.

Definitions are also contained in the 2001 Council of Europe Convention on Cybercrime[1389], the 2005 EU Council Framework Decision on attacks against information systems[1390], 2008 Draft ECOWAS Directive on Fighting Cyber Crime[1391], and the 2009 HIPCAR Model Legislative Text on Cybercrime[1392]

### 6.1.9 Critical infrastructure

As a consequence of an increasing use of computer and network technology in the operation of critical infrastructure, such infrastructure is a possible target for attacks.[1393] Taking into account the potential impact of such attack, some of the more recent frameworks include a specific criminalization/aggravation penalty for certain attacks against critical infrastructure and consequently also a definition. One example is the HIPCAR Model Legislative Text on Cybercrime.

***Definitions***
***3.***
*[…]*
*(8) Critical infrastructure means computer systems, devices, networks, computer programs, computer data, so vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.*
*[…]*

### 6.1.10 Cryptology

The use of encryption technology by offenders can seriously hinder access to relevant evidence.[1394] As a consequence several countries implemented legislation addressing the use of encryption technology and related investigation instruments of law enforcement.[1395] However, out of the different regional frameworks addressing cybercrime only the draft African Union Convention on Cyber Security[1396] provides a definition of cryptology in Article I-1.

*8) Cryptology means the science of protecting and securing information particularly for the purpose of ensuring confidentiality, authentication, integrity and non-repudiation;*

### 6.1.11 Device

The term device is especially used in relation to the criminalization of "illegal devices".[1397] With regard to the potential risk that such devices may be widely spread and used to commit crimes, the drafters of several regional frameworks decided to include a provision criminalizing certain activities related to illegal devices. Unlike the Council of Europe Convention on Cybercrime and the Commonwealth Model Law, that both use the term device, the HIPCAR Model Legislative contains a definition of the term in section 3.

***Definitions***
***3.***
*[…]*
*(9) Device includes but is not limited to*
*a) components of computer systems such as graphic cards, memory, chips;*
*b) storage components such as hard drives, memory cards, compact discs, tapes;*
*c) input devices such as keyboards, mouse, track pad, scanner, digital cameras;*
*d) output devices such as printer, screens.*
*[…]*

It is a typical descriptive definition as the provision explicitly indicates that the definition of device shall not be limited to the components listed ("includes but is not limited to"). With reference to the underlying provision[1398] that criminalizes illegal devices the term also includes computer programs.

### 6.1.12 Hindering

In information societies and economies that include e-commerce the functioning of computer systems is essential. Attacks against computer system that hinder the computer system from carrying out operations can seriously interfere with the society and economy. As a consequence many regional frameworks criminalize hindering a computer system from functioning.[1399] The HIPCAR Model Legislative Text on Cybercrime contains a Cybercrime-specific definition of the term hindering in section 3.

***Definitions***
***3.***
*[…]*
*(10) Hinder in relation to a computer system includes but is not limited to:*
*a) cutting the electricity supply to a computer system; and*
*b) causing electromagnetic interference to a computer system; and*
*c) corrupting a computer system by any means; and*
*d) inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.*
*[…]*

The definition underlines that manipulations include physical interference (such as cutting electrical supply) as well as data related manipulations (such as inputting computer data).

### 6.1.13 Hosting provider

Hosting providers play a crucial role with regard to the fight against cybercrime as their services are, for example, used to store illegal content. Consequently different regional frameworks deal with issues related to ISP liability.[1400] However, the main regional frameworks do not provide a definition of hosting provider. But such a definition is included in the HIPCAR Model Legislative Text on Cybercrime.

***Definitions***
***3.***
*[…]*
*(11) Hosting provider means any natural or legal person providing an electronic data transmission service by storing of information provided by a user of the service.*
*[…]*

The definition does not limit the application of the provision to commercial provider but also includes private operator. As a consequence even the operator of a private website that enables others to store information on the website can be covered by related liability regulations.

### 6.1.14 Hyperlink

While very often only hosting provider, access provider and caching provider are listed as sub-categories to Internet Service Provider (ISP) several legal frameworks provide specific regulations for other service such as search engines[1401] and hyperlinks. In this regard the HIPCAR Model Legislative Text on Cybercrime provides a definition for Hyperlinks.

***Definitions***
***3.***
*[…]*
*(12) Hyperlink means characteristic or property of an element such as symbol, word, phrase, sentence, or image that contains information about another source and points to and causes to display another document when executed.*
*[…]*

The definition is broad and covers various types of hyperlinks such as deep links.

### 6.1.15 Interception

The term interception is frequently used in substantive criminal law with regard to the criminalization of illegal interception[1402] as well as in criminal procedural law with regard to the lawful interception of communication. While regional frameworks like the Council of Europe Convention on Cybercrime and the Commonwealth Model Law contain provisions related to illegal as well as lawful interception, those frameworks do not provide a definition of interception. However, such provision is contained in the HIPCAR Model Legislative Text on Cybercrime.

***Definitions***
***3.***
*[…]*
*(13) Interception includes but is not limited to the acquiring, viewing and capturing of any computer data communication whether by wire, wireless, electronic, optical, magnetic, oral, or other means, during transmission through the use of any technical device.*
*[…]*

### 6.1.16 Interference

Interference is a standard term that is used in several provisions related to Cybercrime. Examples are data interference[1403] as well as system interference.[1404] However, in several regional instruments the term is only used within the headlines of certain provisions but does not describe a criminalized act itself. Consequently most regional frameworks and model laws do not further define the term.

### 6.1.17 Multiple electronic mails

A significant number of all e-mails that are sent out are SPAM. As a consequence a number of countries, as well as recent model laws, have included provisions criminalizing acts related to the distribution of SPAM.[1405] One key term used within such provision is “multiple electronic mail”. The HIPCAR Model Legislative Text on Cybercrime contains a definition for this term.

***Definitions***
***3.***
*[…]*
*(14) Multiple electronic mail messages mean a mail message including E-Mail and instant messaging sent to more that thousand recipients.*
*[…]*

### 6.1.18 Remote forensic software

Some more recent and advanced legal frameworks contain procedural instruments that in certain cases authorize law enforcement agencies to apply advanced forensic tools – such as keylogger.[1406] The HIPCAR Model Legislative Text on Cybercrime contains a definition for the term remote forensic software.

***Definitions***
***3.***
*[…]*
*(15) Remote forensic software means an investigative software installed on a computer system and used to perform tasks that include but are not limited to keystroke logging or transmission of an IP-address.*
*[…]*

Within discussion about the use of the HIPCAR standards, which were developed for the Caribbean, in the Pacific it was pointed out that in order to cover the full range of forensic solutions the term tool (that also covers hardware solutions) is favourable compared to software.

### 6.1.19 Seize

Not only with regard to traditional crimes but also in relation to Cybercrime, seizure remains one of the most important investigation instruments used to collect evidence.[1407] The Commonwealth Model Law on Computer and Computer-related Crime contains a definition of seizure in Part III, Procedural Powers, section 11.

***Definitions for this Part***
*[…]*
***11. In this Part:***
*[…]*
*"seize" includes:*
*(a) make and retain a copy of computer data, including by using onsite equipment; and*
*(b) render inaccessible, or remove, computer data in the accessed computer system; and*
*(c) take a printout of output of computer data.*

This definition that contains three sub-sections was further amended within the development of the HIPCAR Model Legislative Text on Cybercrime. A definition was included in section 3 (16).

***Definitions***
***3.***
*[…]*
*(16) Seize includes:*
*a. activating any onsite computer system and computer data storage media;*
*b. making and retaining a copy of computer data, including by using onsite equipment;*
*c. maintaining the integrity of the relevant stored computer data;*
*d. rendering inaccessible, or removing, computer data in the accessed computer system;*
*e. taking a printout of output of computer data; or*
*f. seize or similarly secure a computer system or part of it or a computer-data storage medium.*
*[…]*

The Council of Europe Convention on Cybercrime followed a different approach and included the different elements of seizure in the provision itself.[1408]

### 6.1.20 Service provider

Service provider is a category used to describe different types of providers offering Internet services. As underlined above different regional frameworks include provisions addressing service provider (such as provisions related to the liability of different types of service provider or procedural instruments that require the support of law enforcement activities by a service provider). Not all of them differentiate between different types of provider. Consequently, especially those regional frameworks that do not differentiate, include a definition of the term service provider. One example is the Council of Europe Convention on Cybercrime.

***Article 1 – Definitions***
*[…]*
*c) "service provider" means:*
*i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and*

*ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.*

*[…]*

The 2002 Commonwealth Model Law on Computer and Computer-related Crime[1409], and the 2009 HIPCAR Model Legislative Text on Cybercrime[1410] also contain similar definitions.

### 6.1.21 Traffic data

Traffic data is a category of data for which some regional legal frameworks and model laws provide specific investigations instruments.[1411] Consequently those regional frameworks and model laws often also provide a definition. One example is section 3 of the 2002 Commonwealth Model Law on Computer and Computer-related Crime.

***Definitions***

***3.***

*[…]*

*"traffic data" means computer data:*

*(a) that relates to a communication by means of a computer system; and*

*(b) is generated by a computer system that is part of the chain of communication; and*

*(c) shows the communication's origin, destination, route, time date, size, duration or the type of underlying services.*

Similar definitions are provided in the 2001 Council of Europe Convention on Cybercrime[1412], and the 2009 HIPCAR Model Legislative Text on Cybercrime.[1413]

## 6.2 Substantive criminal law

**Bibliography (selected):** ABA International Guide to Combating Cybercrime, 2002; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Broadhurst*, Development in the global law enforcement of cybercrime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006; *Brown*, Mass media influence on sexuality, Journal of Sex Research, February 2002; *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81; *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007; *Gercke/Tropina*, from Telecommunication Standardization to Cybercrime Harmonization, Computer Law Review International, 2009, Issue 5; *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010; *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1; *Gercke*, Cybercrime Training for Judges, 2009; *Gercke*, How Terrorist Use the Internet in Pieth/Thelesklaf/Ivory, Countering Terrorist Financing, 2009; *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025; *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; *Hopkins*, Cybercrime Convention: A Positive Beginning to a Long Road Ahead, Journal of High Technology Law, 2003, Vol. II, No. 1; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf; Internet Gambling – An overview of the Issue, GAO-03-89, page 45 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf; *Jonsson/Andren/Nilsson/Svensson/Munck/Kindstedt/Rönnberg*, Gambling addiction in Sweden – the characteristics of problem gamblers, available at: www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Krone*, A

Typology of Online Child Pornography Offending, Trends & Issues in Crime and Criminal Justice, No. 279; *Krotosi,* Identifying and Using Evidence Early To Investigate and Prosecute Trade Secret and Economic Espionage Act Cases, Economic Espionage and Trade Secrets, 2009, Vol. 75, No. 5, page 41 *et seq.*, available at: www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf; *Lavalle*, A Politicized and Poorly Conceived Notion Crying Out for Clarification: The Alleged Need for Universally Agreed Definition of Terrorism, Zeitschrift fuer auslaendisches oeffentliches Recht und Voelkerrecht, 2006, page 89 *et seq.*; *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999; *Liu*, Ashcroft, Virtual Child Pornography and First Amendment Jurisprudence, UC Davis Journal of Juvenile Law & Policy, 2007, Vol. 11; *Mitchell/Finkelhor/Wolak*, The exposure of youth to unwanted sexual material on the Internet – A National Survey of Risk, Impact and Prevention, Youth & Society, Vol. 34, 2003; *Morse*, Extraterritorial Internet Gambling: Legal Challenges and Policy Opinion, page 7, available at: http://law.creighton.edu/pdf/4/morsepublication2.pdf; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf; *Parsonage*, Web Browser Session Restore Forensics, A valuable record of a user's internet activity for computer forensic examinations, 2010, available at: http://computerforensics.parsonage.co.uk/downloads/WebBrowserSessionRestoreForensics.pdf; Preliminary Report On The National Legislation In Europe Concerning Blasphemy, Religious Insults And Inciting Religious Hatred, 2007, available at: www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analysed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009; *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Shaker*, America's Bad Bet: How the Unlawful Internet Gambling Enforcement Act of 2006 will hurt the house, Fordham Journal of Corporate & Financial Law, Vol. XII; *Shaffer*, Internet Gambling & Addiction, 2004, available at: www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Singh*, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cybercrime and Terror, 2001; *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP/e-RIAPL, 2008, C-07; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33; *Walden*, Computer Crimes and Digital Investigations, 2006; *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2; *Wortley/Smallbone*, Child Pornography on the Internet, page 10 *et seq.*, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729; *Wolak/ Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005; *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf.

### 6.2.1 Illegal access (hacking)

Since the development of computer networks, by virtue of their ability to connect computers and offer users access to other computer systems, computers have been used by hackers for criminal purposes.[1414] There is substantial variation in hackers' motivations.[1415] Hackers need not be present at the crime scene;[1416] they just need to circumvent the protection securing the network.[1417] In many cases of illegal access, the security systems protecting the physical location of network hardware are more sophisticated than the security systems protecting sensitive information on networks, even in the same building.[1418]

Illegal access to computer systems hinders computer operators in managing, operating and controlling their systems in an undisturbed and uninhibited manner.[1419] The aim of protection is to maintain the integrity of computer systems.[1420] It is vital to distinguish between illegal access and subsequent offences (such as data espionage[1421]), since legal provisions have a different focus of protection. In most cases,

illegal access (where law seeks to protect the integrity of the computer system itself) is not the end goal, but rather a first step towards further crimes, such as modifying or obtaining stored data (where law seeks to protect the integrity and confidentiality of the data).[1422]

The question is whether the act of illegal access should be criminalized, in addition to subsequent offences.[1423] Analysis of the various approaches to the criminalization of illegal computer access at the national level shows that enacted provisions sometimes confuse illegal access with subsequent offences, or seek to limit the criminalization of illegal access to grave violations only.[1424] Some countries criminalize mere access, while others limit criminalization only to offences where the accessed system is protected by security measures, or where the perpetrator has harmful intentions, or where data were obtained, modified or damaged.[1425] Other countries do not criminalize the access itself, but only subsequent offences.[1426] Opponents to the criminalization of illegal access refer to situations where no dangers were created by mere intrusion, or where acts of "hacking" have led to the detection of loopholes and weaknesses in the security of targeted computer systems.[1427]

### Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime includes a provision on illegal access protecting the integrity of computer systems by criminalizing unauthorized access to a system. Noting inconsistent approaches at the national level,[1428] the Convention on Cybercrime offers the possibility of limitations that – at least in most cases – enable countries without legislation to retain more liberal laws on illegal access.[1429] The provision aims to protect the integrity of computer systems.

### The provision

> ***Article 2 – Illegal access***
> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.*

### The acts covered

The term "access" does not specify a certain means of communication, but is open-ended and open to further technical developments.[1430] It shall include all means of entering another computer system, including Internet attacks,[1431] as well as illegal access to wireless networks. Even unauthorized access to computers that are not connected to any network (e.g. by circumventing password protection) are covered by the provision.[1432] This broad approach means that illegal access not only covers future technical developments, but also covers secret data accessed by insiders and employees.[1433] The second sentence of Article 2 offers the possibility of limiting the criminalization of illegal access to access over a network.[1434]

The illegal acts and protected systems are thus defined in a way that remains open to future developments. The Explanatory Report lists hardware, components, stored data, directories, traffic and content-related data as examples of the parts of computer systems that can be accessed. [1435]

### Mental element

Like all other offences defined by the Council of Europe Convention on Cybercrime, Article 2 requires that the offender is carrying out the offences intentionally.[1436] The Convention on Cybercrime does not contain a definition of the term "intentionally". In the Explanatory Report, the drafters pointed out that "intentionally" should be defined at national level.[1437]

### Without right

Access to a computer can only be prosecuted under Article 2 of the Convention on Cybercrime if it takes place "without right".[1438] Access to a system permitting free and open access by the public or access to a system with the authorization of the owner or other rights-holder is not "without right".[1439] In addition to the subject of free access, the legitimacy of security testing procedures is also addressed.[1440] Network administrators and security companies that test the protection of computer systems in order to identify potential gaps in security measures were wary of the risk of criminalization under illegal access.[1441] Despite the fact that these professionals generally work with the permission of the owner and therefore act legally, the drafters of the Convention on Cybercrime emphasized that "testing or protection of the security of a computer system authorized by the owner or operator, [...] are with right".[1442]

The fact that the victim of the crime has handed out a password or similar access code to the offender does not necessarily mean that the offender then acted with right when accessed the victim's computer system. If the offender has persuaded the victim to disclose a password or access code by means of a successful social-engineering approach,[1443] it is necessary to verify if the authorization given by the victim covers the act carried out by the offender.[1444] In general, this is not the case and the offender therefore acts without right.

### Restrictions and reservations

As an alternative to the broad approach, the Convention on Cybercrime offers the possibility of restricting criminalization with additional elements, listed in the second sentence.[1445] The procedure of how to utilize this reservation is laid down in Article 42 of the Convention on Cybercrime.[1446] Possible reservations relate to security measures,[1447] special intent to obtain computer data,[1448] other dishonest intent that justifies criminal culpability, or requirements that the offence be committed against a computer system through a network.[1449] A similar approach can be found in the EU[1450] Council Framework Decision on attacks against information systems.[1451]

### Commonwealth Model Law on Computer and Computer-related Crime

A similar approach can be found in section 5 of the 2002 Commonwealth Model Law.[1452] As in the Council of Europe Convention on Cybercrime, the provision protects the integrity of computer systems.

> ***Illegal access 5.***
> *A person who intentionally, without lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*

Section 5 follows an approach that is similar to Article 5 of the Council of Europe Convention on Cybercrime. The main difference to the Convention on Cybercrime is that the Commonwealth Model Law, does not contain options to make reservations.

### European Union Council Framework Decision on attacks against iInformation systems

The 2005 EU Council Framework Decision on attacks against information systems contains a provision criminalizing illegal access to information systems in Article 2.

> ***Article 2*** *– Illegal access to information systems*
> *1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.*
> *2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.*

All substantive criminal law provisions of the framework decision were drafted in accordance with the standards defined by the Council of Europe Convention on Cybercrime.[1453] The main difference to the Convention on Cybercrime is the fact that Member States can limit criminalization to cases which are not minor. In this context, the framework decision explicitly points out that minor cases should not be covered by the instrument.[1454]

#### Stanford Draft International Convention

The informal[1455] 1999 Stanford Draft International Convention recognizes illegal access as one of the offences the signatory states should criminalize.

#### The provision

> ***Art. 3*** *– Offences*
> *1. Offenses under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognized authority, permission, or consent:*
> *[...]*
> *(c) enters into a cybersystem for which access is restricted in a conspicuous and unambiguous manner;*
> *[...]*

#### The acts covered

The draft provision displays a number of similarities to Article 2 of the Council of Europe Convention on Cybercrime. Both require an intentional act that is committed without right/without authority. In this context, the requirement of the draft provision ("*without legally recognized authority, permission, or consent* ") is more precise than the term "without right"[1456] used by the Council of Europe Convention on Cybercrime, and explicitly aims to incorporate the concept of self-defence.[1457] Another difference to the regional approaches such as the Convention on Cybercrime is the fact that the draft provision uses the term "cybersystem". The cybersystem is defined in Article 1, paragraph 3 of the Draft Convention. It covers any computer or network of computers used to relay, transmit, coordinate or control communications of data or programs. This definition shows many similarities to the definition of the term "computer system" provided by Article 1 a) of the Council of Europe Convention on Cybercrime.[1458] Although the Draft Convention refers to acts related to the exchange of data and does therefore primarily focus on network-based computer systems, both definitions include interconnected computers as well as standalone machines.[1459]

### *6.2.2 Illegal remaining*

The integrity of computer systems can be violated not only by illegally entering a computer system, but also by continuing to use a computer system after permission has expired. Since in such cases the computer system was not accessed illegally, the application of provisions criminalizing illegal access to computer systems can run into difficulties.

#### Council of Europe

The Council of Europe Convention on Cybercrime criminalizes illegal access to a computer system, but not illegal remaining in a computer system. Nevertheless, illegal remaining was discussed during negotiation of the Convention. In 1998, when the fourth draft version of the Convention on Cybercrime was finished, it still contained this element.

> ***Art. 2*** *– Offences against the confidentiality, integrity and availability of computer data and systems*
> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law [when committed intentionally] the following conduct:*
> *[…]*

*1bis: The intentional failure to exit a computer system, the whole or a part of which has been accessed inadvertently without right by a person, as soon as he becomes aware of this [undue] situation.*
*[…]*

However, the final version of the Convention on Cybercrime that was opened for signature in 2001 no longer contained such a provision.

**Example**

Some of the recent approaches such as the HIPCAR[1460] cybercrime legislative text[1461] include specific provisions to address this issue. Section 5 criminalizes illegal remaining in a computer system. Like the criminalization of illegal access, the protected legal interest is the integrity of computer systems.

***Illegal Remaining***
***5.****(1) A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, remains logged in a computer system or part of a computer system or continues to use a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*
*(2) A country may decide not to criminalize the mere unauthorized remaining provided that other effective remedies are available. Alternatively a country may require that the offence be committed by infringing security measures or with the intent of obtaining computer data or other dishonest intent.*

The provision, which is not contained in similar form in any of the regional approaches, reflects the fact that the integrity of a computer system can be violated not only by entering a computer system without right but also by remaining in the computer system after authorization has expired. Remaining requires that the offender still has access to the computer system. This can be the case, for example, if he/she remains logged on or continues to undertake operations. The fact that he/she has the theoretical possibility to log on to the computer system is not sufficient. Section 54 requires that the offender is carrying out the offences intentionally. Reckless acts are not covered. In addition, Section 54 only criminalizes acts if they are committed "without lawful excuse or justification".

### 6.2.3 Illegal acquisition of computer data

The Council of Europe Convention on Cybercrime as well as the Commonwealth Model Law and the Stanford Draft International Convention provide legal solutions for illegal interception only.[1462] It is questionable whether Article 3 of the Council of Europe Convention on Cybercrime applies to other cases than those where offences are carried out by intercepting data-transfer processes. As noted below,[1463] the question of whether illegal access to information stored on a hard disk is covered by the Convention on Cybercrime was discussed with great interest.[1464] Since a transfer process is needed, it is likely that Article 3 of the Convention on Cybercrime does not cover forms of data espionage other than the interception of transfer processes.[1465] This is in so far interesting as the 9th Draft of the Convention on Cybercrime mentioned the relevance of criminalizing data espionage.

One issue frequently discussed in this context is the question whether the criminalization of illegal accesses renders the criminalization of data espionage unnecessary. In cases where the offender has legitimate access to a computer system (e.g. because he/she is ordered to repair it) and on this occasion (in violation of the limited legitimation) copies files from the system, the act is in general not covered by the provisions criminalizing illegal access.[1466]

Given that much vital data are now stored in computer systems, it is essential to evaluate whether existing mechanisms to protect data are adequate or whether other criminal law provision are necessary to protect the user from data espionage.[1467] Today, computer users can use various hardware devices and software tools in order to protect secret information. They can install firewalls and access-control systems or encrypt stored information and thereby decrease the risk of data espionage.[1468] Although user-friendly

devices are available, requiring only limited knowledge by users, truly effective protection of data on a computer system often requires knowledge that few users have.[1469] Data stored on private computer systems, in particular, are often not adequately protected against data espionage. Criminal law provisions can therefore offer an additional protection.

Some countries have decided to extend the protection that is available through technical measures by criminalizing data espionage. There are two main approaches. Some countries follow a narrow approach and criminalize data espionage only where specific secret information is obtained – an example is 18 USC § 1831, which criminalizes economic espionage. The provision does not only cover data espionage, but other ways of obtaining secret information as well.

### United States Code

***§ 1831 – Economic espionage***
*(a) In General – Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly:*

*(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;*
*(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;*
*(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;*
*(4) attempts to commit any offense described in any of paragraphs (1) through (3); or*
*(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than $500 000 or imprisoned not more than 15 years, or both.*

*(b) Organizations – Any organization that commits any offense described in subsection (a) shall be fined not more than $10 000 000.*

This § 1831 was introduced by the Economic Espionage Act of 1996.[1470] Until 1996, economic espionage was only criminalized under largely inconsistent state laws.[1471] The Economic Espionage Act criminalizes two types of trade secret misappropriation in Title 18 – theft of a trade secret to benefit a foreign government, instrumentality, or agent; and commercial theft of trade secrets carried out for economic advantage, whether or not it benefits a foreign government, instrumentality, or agent.[1472] Although the provision focuses on the protection of content (trade secrets) and does not require a specific format (computer data), it is not only relevant with regard to traditional crime but also computer-related offences.[1473] In general, 18 U.S.C. § 1030(a)(2) is also applicable in such cases.[1474] With regard to computer-related cases, the acts are covered by § 1831(a)(2)-(5).

### HIPCAR Cybercrime Legislative Text

Another example is section 8 of the HIPCAR[1475] cybercrime legislative text.[1476]

***Data Espionage***
***8.*** *(1) A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification obtains, for himself or for another, computer data which are not meant for him and which are specially protected against unauthorized access, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*
*(2) A country may limit the criminalization to certain categories of computer data.*

Section 8 protects the secrecy of stored and protected computer data. The special protection requires that the hoster of the information has implemented protection measures that significantly increase the

difficulty of obtaining access to the data without authorization. Examples are password protection and encryption. The Explanatory Notes to the legislative text point out that it is necessary that the protection measures go beyond standard protection measures that apply to data as well as other property, for example access restrictions to certain parts of government buildings.[1477]

#### German Penal Code

A similar approach can be found in section 202a of the German Penal Code in the version in force until 2007.[1478]

> ***Section 202a.*** *– Data Espionage:*
> *(1) Any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorized access, shall be liable to imprisonment for a term not exceeding three years or to a fine*
> *(2) Data within the meaning of subsection 1 are only such as are stored or transmitted electronically or magnetically or in any form not directly visible.*

This provision covers not only economic secrets, but stored computer data in general.[1479] In terms of its objects of protection, this approach is broader compared to 18 USC § 1831 Economic espionage, but the application of the provision is limited since obtaining data is only criminalized where data are specially protected against unauthorized access.[1480] The protection of stored computer data under German criminal law is thus limited to persons or businesses that have taken measures to avoid falling victim to such offences.[1481]

#### Relevance of such provisions

The implementation of such provision is especially relevant with regard to cases where the offender was authorized to access a computer system (e.g. because he/she was ordered to fix a computer problem) and then abused the authorization to illegally obtain information stored on the computer system.[1482] Having regard to the fact that the permission covers access to the computer system, it is in general not possible to cover such cases with provisions criminalizing the illegal access.

#### Without right

The application of data-espionage provisions generally requires that the data were obtained without the consent of the victim. The success of phishing attacks[1483] clearly demonstrates the success of scams based on the manipulation of users.[1484] Due to the consent of the victim, offenders who succeed in manipulating users to disclose secret information cannot be prosecuted on the basis of the above-mentioned provisions.

### *6.2.4 Illegal interception*

The use of ICTs is accompanied by several risks related to the security of information transfer.[1485] Unlike classic mail-order operations within a country, data-transfer processes over the Internet involve numerous providers and different points where the data transfer process could be intercepted.[1486] The weakest point for intercept remains the user, especially users of private home computers, who are often inadequately protected against external attacks. As offenders generally always aim for the weakest point, the risk of attacks against private users is great, all the more so given:

- the development of vulnerable technologies; and
- the increasing relevance of personal information for offenders.

New network technologies (such as “wireless LAN”) offer several advantages for Internet access.[1487] Setting up a wireless network in a private home, for example, allows families to connect to the Internet from anywhere inside a given radius, without the need for cable connections. But the popularity of this technology and resulting comfort is accompanied by serious risks to network security. If an unprotected

wireless network is available, perpetrators can log on to this network and use it for criminal purposes without the need to get access to a building. They simply need to get inside the radius of the wireless network to launch an attack. Field tests suggest that in some areas as many as 50 per cent of private wireless networks are not protected against unauthorized interception or access.[1488] In most cases, lack of protection arises from a lack of knowledge as to how to configure protection measures.[1489]

In the past, perpetrators concentrated mainly on business networks for illegal interceptions.[1490] Interception of corporate communications was more likely to yield useful information than interception of data transferred within private networks. The rising number of identity thefts of private personal data suggests that the focus of the perpetrators may have changed.[1491] Private data such as credit-card numbers, social-security numbers[1492], passwords and bank account information are now of great interest to offenders.[1493]

### Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime includes a provision protecting the integrity of non-public transmissions by criminalizing their unauthorized interception. This provision aims to equate the protection of electronic transfers with the protection of voice conversations against illegal tapping and/or recording that currently already exists in most legal systems.[1494]

### The provision

> ***Article 3*** *– Illegal interception*
> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.*

### The acts covered

The applicability of Article 3 is limited to the interception of transmissions realized by technical measures.[1495] Interceptions related to electronic data can be defined as any act of acquiring data during a transfer process.[1496]

As mentioned above, the question whether illegal access to information stored on a hard disk is covered by the provision is controversial and much discussed.[1497] In general, the provision only applies to the interception of transmissions – access to stored information is not considered as an interception of a transmission.[1498] The fact that the application of the provision is discussed even in cases where the offender physically accesses a standalone computer system partly arises as a result of the fact that the Convention does not contain a provision related to data espionage,[1499] and the Explanatory Report to the Convention contains two slightly imprecise explanations with regard to the application of Article 3:

The Explanatory Report first of all points out that the provision covers communication processes taking place within a computer system.[1500] However, this still leaves open the question of whether the provision should only apply in cases where victims send data that are then intercepted by offenders or whether it should apply also when the offender operates the computer. The second point is related to the criminalization of illegal acquisition of computer data.

The guide points out that interception can be committed either indirectly through the use of tapping devices or "through access and use of the computer system".[1501] If offenders gain access to a computer system and use it to make unauthorized copies of stored data on an external disc drive, whereby the act leads to a data transfer (sending data from the internal to the external hard disc), this process is not *intercepted*, but rather *initiated*, by offenders. The missing element of technical interception is a strong argument against the application of the provision in cases of illegal access to stored information.[1502]

The term "transmission" covers all data transfers, whether by telephone, fax, e-mail or file transfer.[1503] The offence established under Article 3 applies only to non-public transmissions.[1504] A transmission is "non-public", if the transmission process is confidential.[1505] The vital element to differentiate between public and non-public transmissions is not the nature of the data transmitted, but the nature of the transmission process itself. Even the transfer of publicly available information can be considered criminal, if the parties involved in the transfer intend to keep the content of their communications secret. Use of public networks does not exclude "non-public" communications.

### Mental element

Like all other offences defined by the Council of Europe Convention on Cybercrime, Article 3 requires that the offender is carrying out the offences intentionally.[1506] The Convention on Cybercrime does not contain a definition of the term "intentionally". In the Explanatory Report, the drafters pointed out that "intentionally" should be defined at national level.[1507]

### Without right

The interception of communication can only be prosecuted under Article 3 of the Convention on Cybercrime, if it happens "without right". [1508] The drafters of the Convention on Cybercrime provided a set of examples for interceptions that are not carried out without right. These include action on the basis instructions or by authorization of the participants of the transmission,[1509] authorized testing or protection activities agreed to by the participants[1510] and lawful interception on the basis of criminal law provisions or in the interests of national security.[1511]

Another issue raised within the negotiation of the Convention on Cybercrime was the question whether the use of cookies would lead to criminal sanctions based on Article 3.[1512] The drafters pointed out that common commercial practices (such as cookies) are not considered to be interceptions without right.[1513]

### Restrictions and reservations:

Article 3 offers the option of restricting criminalization by requiring additional elements listed in the second sentence, including a "dishonest intent" or relation to a computer system connected to another computer system.

### Commonwealth Model Law on Computer and Computer related Crime

A similar approach can be found in section 8 of the 2002 Commonwealth Model Law.[1514]

> ***Illegal interception of data etc.***
> ***8.*** *A person who, intentionally without lawful excuse or justification, intercepts by technical means:*
> *(a) any non-public transmission to, from or within a computer system; or*
> *(b) electromagnetic emissions from a computer system that are carrying computer data; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*

Section 8 follows an approach that is similar to Article 3 of the Council of Europe Convention on Cybercrime. Like the Convention on Cybercrime, the provision protects data during non-public transmission processes.

### Stanford Draft International Convention

The informal[1515] 1999 Stanford Draft International Convention (the "Stanford Draft") does not explicitly criminalize the interception of computer data.

### 6.2.5 Data interference

The protection of tangible, or physical, objects against intentional damage is a classic element of national penal legislation. With continuing digitization, more critical business information is stored as data.[1516] Attacks or obtaining of this information can result in financial losses.[1517] Besides deletion, the alteration of such information could also have major consequences.[1518] Previous legislation has in some cases not completely brought the protection of data in line with the protection of tangible objects. This has enabled offenders to design scams that do not lead to criminal sanctions.[1519]

#### Council of Europe Convention on Cybercrime

In Article 4, the Council of Europe Convention on Cybercrime includes a provision that protects the integrity of data against unauthorized interference.[1520] The aim of the provision is to fill existing gaps in some national penal laws and to provide computer data and computer programs with protections similar to those enjoyed by tangible objects against the intentional infliction of damage.[1521]

#### The provision:

> ***Article 4 – Data interference***
> *(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.*
> *(2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.*

#### The acts covered

Article 4 criminalizes five different acts. The terms "damaging" and "deterioration" mean any act related to the negative alteration of the integrity of information content of data and programs.[1522] "Deleting" covers acts where information is removed from storage media and is considered comparable to the destruction of a tangible object. While providing the definition, the drafters of the Convention on Cybercrime did not differentiate between the various ways data can be deleted.[1523] Dropping a file to the virtual trash bin does not remove the file from the hard disk.[1524] Even "emptying" the trash bin does not necessarily remove the file.[1525] It is therefore uncertain if the ability to recover a deleted file hinders the application of the provision.[1526] "Suppression" of computer data denotes an action that affects the availability of data to the person with access to the medium, where the information is stored in a negative way.[1527] The application of the provision is especially discussed with regard to denial-of-service[1528] attacks.[1529] During such an attack, the data provided on the targeted computer system are no longer available to potential users or to the owner of the computer system.[1530] The term "alteration" covers the modification of existing data, without necessarily lowering the serviceability of the data.[1531] This act covers especially the installation of malicious software like spyware, viruses or adware on the victim's computer.[1532]

#### Mental element

Like all other offences defined by the Council of Europe Convention on Cybercrime, Article 4 requires that the offender is carrying out the offences intentionally.[1533] The Convention on Cybercrime does not contain a definition of the term "intentionally". In the Explanatory Report, the drafters pointed out that "intentionally" should be defined at national level.[1534]

#### Without right

Similarly to the provisions discussed above, the acts must be committed "without right".[1535] The right to alter data was discussed, especially in the context of "remailers".[1536] Remailers are used to modify certain data for the purpose of facilitating anonymous communications.[1537] The Explanatory Report mentions

that, in principle, these acts are considered a legitimate protection of privacy and can thus be considered as being undertaken with authorization.[1538]

### Restrictions and reservations

Article 4 offers the option of restricting criminalization by limiting it to cases where serious harm arises, a similar approach to the EU Council Framework Decision on attacks against information systems,[1539] which enables Member States to limit the applicability of the substantive criminal law provision to "cases which are not minor".[1540]

### Commonwealth Computer and Computer related Crimes Model Law

An approach in line with Article 4 of the Council of Europe Convention on Cybercrime can be found in section 8 of the 2002 Commonwealth Model Law.[1541]

### The provision

***Interfering with data***
***6.*** *(1) A person who, intentionally or recklessly, without lawful excuse or justification, does any of the following acts:*
*(a) destroys or alters data; or*
*(b) renders data meaningless, useless or ineffective; or*
*(c) obstructs, interrupts or interferes with the lawful use of data; or*
*(d) obstructs, interrupts or interferes with any person in the lawful use of data; or*
*(e) denies access to data to any person entitled to it;*
*commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*
*(2) Subsection (1) applies whether the person's act is of temporary or permanent effect.*

The first main difference between section 6 and the corresponding provision in the Convention on Cybercrime is the fact that this provision of the Commonwealth Model Law, in addition to intentional acts, even criminalizes reckless acts. Unlike section 6, three other provisions of the Model Law[1542], like the Convention on Cybercrime, limit the criminalization to intentional acts. The coverage of recklessness significantly broadens the approach, since even the unintentional deletion of files from a computer system or damage of a storage device will lead to criminal sanctions.

The second difference is the fact that the acts covered by section 6 vary slightly from the corresponding provision in the Convention on Cybercrime. Finally, the provision contains a clarification in subsection 2 that the acts do not require permanent effect, but even temporary effects are covered.

### Stanford Draft International Convention

The informal[1543] 1999 Stanford Draft International Convention ("Stanford Draft") contains two provisions that criminalize acts related to interference with computer data.

### The provision

***Art. 3***
*1. Offenses under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognized authority, permission, or consent:*
*(a) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data or programs in a cybersystem with the purpose of causing, or knowing that such activities would cause, said cybersystem or another cybersystem to cease functioning as intended, or to perform functions or activities not intended by its owner and considered illegal under this Convention;*

*(b) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data in a cybersystem for the purpose and with the effect of providing false information in order to cause substantial damage to persons or property.*

#### The acts covered

The main difference between the Council of Europe Convention on Cybercrime and the Commonwealth Model Law on the one hand, and the approach of the Stanford Draft on the other, is that the Stanford Draft only criminalizes interference with data if it interferes with the functioning of a computer system (Article 3, paragraph 1a) or if the act is committed with the purpose of providing false information in order to cause damage to a person or property (Article 3, paragraph 1b). Therefore, Therefore, the Stanford Draft does not criminalize the deletion of a regular text document from a data storage device as this neither influences the functioning of a computer nor provides false information. The Council of Europe Convention on Cybercrime and the Commonwealth Model Law both adopt a broader approach, protecting the integrity of computer data without the mandatory requirement of further effects.

### *6.2.6 System interference*

People or businesses offering services based on ICTs depend on the functioning of their computer systems.[1544] The lack of availability of webpages that are victim to denial-of-service (DOS) attacks[1545] demonstrates how serious the threat of attack is.[1546] Attacks like these can cause serious financial losses and affect even powerful systems.[1547] Businesses are not the only targets. Experts around the world are currently discussing possible "cyberterrorism" scenarios that take into account attacks against critical infrastructures such as power supplies and telecommunication services. [1548]

#### Council of Europe Convention on Cybercrime

To protect access of operators and users to ICTs, the Convention on Cybercrime includes a provision in Article 5 that criminalizes the intentional hindering of lawful use of computer systems.[1549]

#### The provision

***Article 5 – System interference***
*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.*

#### The acts covered

The application of the provision requires that the functioning of a computer system has been hindered.[1550] Hindering means any act interfering with the proper functioning of the computer system.[1551] The application of the provision is limited to cases where hindering is carried out by one of the acts mentioned. In addition, the provision requires that the hindering is "serious". It is the parties' responsibility to determine the criteria to be fulfilled in order for the hindering to be considered as serious.[1552] Possible restrictions under national law could include a minimum amount of damage, as well as limitation of criminalization to attacks against important computer systems.[1553]

The list of acts by which the functioning of the computer system is adversely affected is conclusive.[1554]

Inputting is defined neither by the Convention on Cybercrime itself, nor by the drafters of the Convention on Cybercrime. Given that transmitting is mentioned as an additional act in Article 5, the term "inputting" could be defined as any act related to use of physical input interfaces to transfer information to a computer system, whereas the term "transmitting" covers acts that entail the remote input of data.[1555]

The terms "damaging" and "deteriorating" overlap and are defined by the drafters of the Convention on Cybercrime in the Explanatory Report with regard to Article 4 as negative alteration of the integrity of information content of data and programs.[1556]

"Deleting" was also defined by the drafters of the Convention on Cybercrime in the Explanatory Report with regard to Article 4, and covers acts where information is removed from storage media.[1557]

The term "alteration" covers the modification of existing data, without necessarily lowering the serviceability of the data. [1558]

"Suppression" of computer data denotes an action that adversely affects the availability of data to the person with access to the medium where the information is stored.[1559]

### Application of the provision with regard to SPAM

It was discussed whether the problem of SPAM e-mail[1560] could be addressed under Article 5, since spam can overload computer systems.[1561] The drafters stated clearly that spam may not necessarily lead to "serious" hindering and that "conduct should only be criminalized where the communication is intentionally and seriously hindered".[1562] The drafters also noted that parties may have a different approach to hindrance under their own national legislation,[1563] e.g. by making acts of interference administrative offences or subject to sanction.[1564]

### Mental elemen

Like all other offences defined by the Council of Europe Convention on Cybercrime, Article 5 requires that the offender is carrying out the offences intentionally.[1565] This includes the intent to carry out one of listed acts as well as the intention to seriously hinder the functioning of a computer system.

The Convention on Cybercrime does not contain a definition of the term "intentionally". In the Explanatory Report, the drafters pointed out "intentionally" should be defined at national level.[1566]

### Without right

The act needs to be carried out "without right".[1567] As mentioned previously, network administrators and security companies testing the protection of computer systems were afraid of the possible criminalization of their work.[1568] These professionals work with the permission of the owner and therefore act legally. In addition, the drafters of the Convention on Cybercrime explicitly mentioned that testing the security of a computer system based on the authorization of the owner is not without right.[1569]

### Restrictions and reservations

Unlike Article 2-4, Article 5 does not contain an explicit possibility of restricting the application of the provision implementation in national law. Nevertheless, the responsibility of the parties to define the gravity of the offence gives them the possibility to adjust the criminalization during the implementation process. A similar approach can be found in the European Union Framework[1570] Decision on Attacks against Information Systems.[1571]

### Commonwealth Computer and Computer related Crimes Model Law

An approach in line with Article 5 of the Council of Europe Convention on Cybercrime can be found in section 7 of the 2002 Commonwealth Model Law.[1572]

### The provision

***Sec Interfering with computer system***
***7.*** *(1) A person who intentionally or recklessly, without lawful excuse or justification:*
*(a) hinders or interferes with the functioning of a computer system; or*
*(b) hinders or interferes with a person who is lawfully using or operating a computer system;*
*commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*
*In subsection (1) "hinder", in relation to a computer system, includes but is not limited to:*
*(a) cutting the electricity supply to a computer system; and*
*(b) causing electromagnetic interference to a computer system; and*
*(c) corrupting a computer system by any means; and*
*(d) inputting, deleting or altering computer data;*

The main difference with the corresponding provision in the Council of Europe Convention is the fact that, based on section 7 of the Commonwealth Model Law, even reckless acts are criminalized. Even unintentional cutting of electricity supply during construction work can therefore lead to criminal sanctions. With this approach, the Model Law even goes beyond the requirements of the Convention on Cybercrime. Another difference is the fact that the definition of "hindering" in section 7 of the Commonwealth Model Law lists more acts than Article 5 of the Council of Europe Convention on Cybercrime.

### European Union Coucnil Framework Decision on attacks against information systems

The EU Council Framework Decision adopts a similar approach and criminalizes illegal data interference in Article 3.

***Article 3 – Illegal system interference***
*Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor.*

The approach is based on the Council of Europe Convention on Cybercrime. The first main difference is that, in addition to the acts covered by the Convention on Cybercrime (inputting, transmitting, damaging, deleting, deteriorating, altering and suppressing), Article 3 also criminalizes hindering the functioning of an information system by rendering computer data inaccessible. Data are rendered inaccessible if, by committing the act, the offender prevents someone from gaining access to them. Yet despite the more complex list of acts in Article 3, there is no difference with the corresponding article in the Council of Europe Convention on Cybercrime insofar as rendering inaccessible is covered by the act of suppressing computer data. The explanation to the 19th draft version of the Convention on Cybercrime highlights that the expert group which drafted the Convention on Cybercrime agreed that the term suppression of data has two meanings: the deletion of data so they no longer physically exist, and rendering data inaccessible.[1573]

### Stanford Draft International Convention

The informal[1574] 1999 Stanford Draft International Convention ("Stanford Draft") contains a provision that criminalizes acts related to interference with computer systems.

### The provision

***Art.3***
*1. Offenses under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognized authority, permission, or consent:*

*(a) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data or programs in a cyber system with the purpose of causing, or knowing that such activities would cause, said cyber system or another cyber system to cease functioning as intended, or to perform functions or activities not intended by its owner and considered illegal under this Convention;*

**The acts covered**

The main difference between the Council of Europe Convention on Cybercrime and the Commonwealth Model Law and the approach of the Stanford Draft is the fact that Stanford Draft covers any manipulation of computer systems while the Council of Europe Convention on Cybercrime and the Commonwealth Model Law limit criminalization to the hindering of the functioning of a computer system.

### *6.2.7 Erotic or pornographic material*

The criminalization and gravity of criminalization of illegal content and sexually-explicit content varies between countries.[1575] The parties that negotiated the Council of Europe Convention on Cybercrime focused on the harmonization of laws regarding child pornography and excluded the broader criminalization of erotic and pornographic material. Some countries have addressed this problem by implementing provisions that criminalize the exchange of pornographic material through computer systems. However, the lack of standard definitions makes it difficult for law-enforcement agencies to investigate those crimes, if offenders act from countries that have not criminalized the exchange of sexual content.[1576]

**Examples**

One example of the criminalization of the exchange of pornographic material is Section 184 of the German Penal Code.

*Section 184 Dissemination of Pornographic Writings*
*(1) Whoever, in relation to pornographic writings (Section 11 subsection (3)):*

*1. offers, gives or makes them accessible to a person under eighteen years of age;*
*2. displays, posts, presents or otherwise makes them accessible at a place accessible to persons under eighteen years of age, or into which they can see;*
*3. offers or gives them to another in retail trade outside of the business premises, in kiosks or other sales areas which the customer usually does not enter, through a mail-order business or in commercial lending libraries or reading circles;*
*3a. offers or gives them to another by means of commercial rental or comparable commercial furnishing for use, except for shops which are not accessible to persons under eighteen years of age and into which they cannot see;*
*4. undertakes to import them by means of a mail-order business;*
*5. publicly offers, announces, or commends them at a place accessible to persons under eighteen years of age or into which they can see, or through dissemination of writings outside of business transactions through normal trade outlets;*
*6. allows another to obtain them without having been requested to do by him;*
*7. shows them at a public film showing for compensation requested completely or predominantly for this showing;*
*8. produces, obtains, supplies, stocks, or undertakes to import them in order to use them or copies made from them within the meaning of numbers 1 through 7 or to make such use possible by another; or*
*9. undertakes to export them in order to disseminate them or copies made from them abroad in violation of the applicable penal provisions there or to make them publicly accessible or to make such use possible, shall be punished with imprisonment for not more than one year or a fine.*

This provision is based on the concept that trade and other exchange of pornographic writings should not be criminalized, if minors are not involved.[1577] On this basis, the law aims to protect the undisturbed development of minors.[1578] Whether access to pornography has a negative impact on the development of minors is controversial and much discussed.[1579] The exchange of pornographic writings among adults is not criminalized by Section 184. The term "writing" covers not only traditional writings, but also digital storage.[1580] Equally, making them "accessible" not only applies to acts beyond the Internet, but covers cases where offenders make pornographic content available on websites.[1581]

One example of an approach that goes beyond this and criminalizes any sexual content is Section 4.C.1, Philippines draft House Law Bill No. 3777 of 2007.[1582]

> ***Sec. 4.C1.:*** *Offenses Related to Cybersex – Without prejudice to the prosecution under Republic Act No. 9208 and Republic Act No. 7610, any person who in any manner advertises, promotes, or facilitates the commission of cybersex through the use of information and communications technology such as but not limited to computers, computer networks, television, satellite, mobile telephone, […]*
> ***Section 3i.:*** *Cybersex or Virtual Sex – refers to any form of sexual activity or arousal with the aid of computers or communications network*

This provision follows a very broad approach, as it criminalizes any kind of sexual advertisement or facilitation of sexual activity carried out over the Internet. Due to the principle of dual criminality,[1583] international investigations with regard to such broad approaches run into difficulties.[1584]

### 6.2.8 Child pornography

The Internet is becoming the main instrument for the trade and exchange of material containing child pornography.[1585] The major reasons for this development are the speed and efficiency of the Internet for file transfers, its low production and distribution costs and perceived anonymity.[1586] Pictures placed on a webpage can be accessed and downloaded by millions of users worldwide.[1587] One of the most important reasons for the "success" of webpages offering pornography or even child pornography is the fact that Internet users feel less observed while sitting in their home and downloading material from the Internet. Unless the users have used means of anonymous communication, the impression of no traceability is wrong.[1588] Most Internet users are simply unaware of the electronic trail they leave while surfing.[1589]

The provisions criminalizing child pornography are designed in general to protect different legal interests. Criminalization of the production of child pornography seeks to protect children from falling victim to sexual abuse.[1590] With regard to the prohibition of acts related to the exchange of child pornography (offering, distributing) as well as possession, criminalization is intended to destroy the market, insofar as ongoing demand for new material could motivate offenders to continue the abuse of children.[1591] In addition, the prohibition of exchange seeks to make it more difficult for people to gain access to such material and thereby prevent a trigger effect on sexual abuse of children. Finally, criminalization of possession intends to prevent offenders from using child-pornography material to seduce children into getting involved in sexual intercourse.[1592]

#### Council of Europe Convention on Cybercrime

In order to improve and harmonize the protection of children against sexual exploitation,[1593] the Convention on Cybercrime includes an article addressing child pornography.

#### The provision:

> ***Article 9 – Offences related to child pornography***
> *(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:*
> *a) producing child pornography for the purpose of its distribution through a computer system;*
> *b) offering or making available child pornography through a computer system;*

*c) distributing or transmitting child pornography through a computer system;*
*d) procuring child pornography through a computer system for oneself or for another person;*
*e) possessing child pornography in a computer system or on a computer-data storage medium.*
*(2) For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:*
*a) a minor engaged in sexually explicit conduct;*
*b) a person appearing to be a minor engaged in sexually explicit conduct;*
*c) realistic images representing a minor engaged in sexually explicit conduct.*
*(3) For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.*
*4) Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.*

Most countries already criminalize the abuse of children, as well as traditional methods of distribution of child pornography.[1594] The Convention on Cybercrime is thus not limited to closing gaps in national criminal law[1595] – it also seeks to harmonize differing regulation.[1596]

### The acts covered

"Production" describes any process of creating child pornography. There is an ongoing discussion on the interpretation of the term. In the United Kingdom, the download of child pornography images is considered as production ("making") of child pornography.[1597] The distinction between "procuring" and "producing" in Article 9 of the Council of Europe Convention on Cybercrime indicates that the drafter of the Convention did not consider the mere download of child pornography as production. Even on the basis of the distinction drawn in the Convention on Cybercrime, however, further differentiation is required. An offender taking pictures of a child being abused is producing child pornography; but it is uncertain whether a person who uses child-pornography pictures to put them together in an animation is similarly producing child pornography. While he/she is certainly the producer of the animation, it is uncertain whether the term "production" in the Council of Europe Convention on Cybercrime is only applicable if it is documentation of an actual abuse of a child. The fact that the Convention on Cybercrime intends to criminalize the production of fictive child pornography – which does not require the actual abuse of a child – is an argument in favour of a broad interpretation of the term "production". On the other hand, the Explanatory Report to the Convention on Cybercrime indicates that criminalization of production is required to combat the danger "at the source".[1598] While the Council of Europe Convention on Cybercrime does not specify that intention of the drafters, the Explanatory Report to the Council of Europe Convention on the Protection of Children[1599] provides a more specific explanation of the motivation of the drafters with regard to a similar provision.[1600] The drafters of the Convention on the Protection of Children highlighted that criminalization of the production of child pornography is "necessary to combat acts of sexual abuse and exploitation at their source". This can be seen as an argument in favour or a narrower approach.

It is necessary that the production of child pornography be carried out for the purpose of distribution through a computer system. If the offender produces the material for his own use, or intends to distribute it in non-electronic form, Article 9 of the Council of Europe Convention on Cybercrime is not applicable. Another problem discussed in the context of production is coverage of auto-depiction.[1601] If the offender, from a distance, convinces a child to take pornographic pictures of himself/herself this could, depending on the national legislation, lead to criminalization of the victim (the child) and not the offender.

"Offering" covers the act of soliciting others to obtain child pornography. It is not necessary that the material be offered on a commercial basis, but it implies that the offender offering the material is capable of providing it.[1602] "Making available" refers to an act that enables other users to gain access to child pornography. The act can be committed by placing child pornography on websites or connecting to file-sharing systems and enabling others to access such material in unblocked storage capacities or folders.

"Distribution" covers active acts of forwarding child pornography to others. "Transmitting" covers all communication by means of transmitted signals. "Procuring" for oneself or for another covers any act of actively obtaining child pornography.

Article 9 finally criminalizes "possessing" child pornography. The criminalization of possession of child pornography also differs between national legal systems.[1603] Demand for such material could result in its production on an ongoing basis.[1604] Possession of such material could encourage the sexual abuse of children, so drafters suggest that one effective way to curtail the production of child pornography is to make possession illegal.[1605] However, the Convention enables the parties, in paragraph 4, to exclude the criminalization of mere possession, by restricting criminal liability to the production, offer and distribution of child pornography.[1606] Possession involves the control a person intentionally exercises towards child pornography. It requires that the offender have control, which is not only the case with regard to local storage devices but also remote storage devices which he/she can access and control. Furthermore, possession in general requires a mental element as stated in the definition above.

### Child pornography

Article 9, paragraph 2, provides three subsections on material that visually depicts child pornography: a minor engaged in sexually explicit conduct, a person appearing to be a minor engaged in sexually explicit conduct and realistic images representing a minor engaged in sexually explicit conduct. The fact that a visual depiction is required excludes audio files.

Although the drafters sought to improve the protection of children against sexual exploitation, the legal interests covered by paragraph 2 are broader. Paragraph 2(a) focuses directly on protection against child abuse. Paragraphs 2(b) and 2(c) cover images that were produced without violating children's rights, e.g. images that have been created through the use of 3D modelling software.[1607] The reason for the criminalization of fictive child pornography is the fact that these images can, without necessarily creating harm to a "real child", be used to seduce children into participating in such acts.[1608]

One of the main challenges related to the definition is the fact that it focuses on visual depiction. Child pornography is not necessary distributed as pictures or movies, but also as audio files.[1609] Due to the fact that the provision provided in Article 9 refers to "material that visually depicts" a child, the provision does not cover audio files. As a consequence, more recent approaches such as the HIPCAR[1610] cybercrime legislative text[1611] adopt a different approach and avoid the term "visually".

***Definitions***
***3.***
*[…]*
*(4) Child pornography means pornographic material that depicts presents or represents:*
*a) a child engaged in sexually explicit conduct;*
*b) a person appearing to be a child engaged in sexually explicit conduct; or*
*c) images representing a child engaged in sexually explicit conduct;*
*this includes, but is not limited to, any audio, visual or text pornographic material.*
*A country may restrict the criminalisation by not implementing (b) and (c).*

Another broader definition can be found in Article 2 c) of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

*Article 2*
*For the purpose of the present Protocol:*
*[…]*
*(c) Child pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.*

One of the most important differences between national legislation is the age of the person involved. Some states define the term "minor" in relation to child pornography in their national law in accordance with the definition of a "child" in Article 1 of the UN Convention on the Rights of the Child[1612] as all persons less than 18 years old. Other countries define minors as a person under 14 years old.[1613] A similar approach is found in the 2003 EU Council Framework Decision on combating the sexual exploitation of children and child pornography[1614] and the 2007 Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse.[1615] Emphasizing the importance of a uniform international standard regarding age, the Convention on Cybercrime defines the term according to the UN Convention.[1616] However, in recognition of the huge differences in the existing national laws, the Convention on Cybercrime permits parties to require a different age limit of not lower than 16 years. One problem that is more and more frequently debated is potentially unintended criminalization in cases where the age of sexual consent and the age-limit within the definition differ.[1617] If, for example, child pornography is defined as visual depiction of sexual acts of a person below the age of 18 and at the same time the age of sexual consent is 16, two 17 year old children can legally have a sexual relationship but will be committing a serious crime (production of child pornography) if they take pictures or movies of this act.[1618]

### Mental element

Like all other offences defined by the Council of Europe Convention on Cybercrime, Article 9 requires that the offender is carrying out the offences intentionally.[1619] In the Explanatory Report, the drafters explicitly pointed out that interaction with child pornography without any intention is not covered by the Convention on Cybercrime. Lack of intention can be relevant especially if the offender accidentally opened a webpage with child pornography images and despite the fact that he/she immediately closed the website some images were stored in temp-folders or cache-files.

### Without right

The acts related to child pornography can only be prosecuted under Article 9 of the Convention on Cybercrime if they are carried out "without right".[1620] The drafters of the Convention on Cybercrime did not further specify in which cases the user is acting with authorization. In general, the act is not carried out "without right" only if members of law-enforcement agencies are acting within an investigation.

### Council of Europe Convention on the Protection of Children

Another approach to criminalize acts related to child pornography is Article 20 of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.[1621]

### The provision

*Article 20 – Offences concerning child pornography*
*(1) Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalised:*
*a) producing child pornography;*
*b) offering or making available child pornography;*
*c) distributing or transmitting child pornography;*
*d) procuring child pornography for oneself or for another person;*
*e) possessing child pornography;*
*f) knowingly obtaining access, through information and communication technologies, to child pornography.*
*(2) For the purpose of the present article, the term "child pornography" shall mean any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes.*
*(3) Each Party may reserve the right not to apply, in whole or in part, paragraph 1.a and e to the production and possession of pornographic material:*

*– consisting exclusively of simulated representations or realistic images of a non-existent child;*
*– involving children who have reached the age set in application of Article 18, paragraph 2, where these images are produced and possessed by them with their consent and solely for their own private use.*
*(4) Each Party may reserve the right not to apply, in whole or in part, paragraph 1.f*

### The acts covered

The provision is based on Article 9 of the Council of Europe Convention on Cybercrime and therefore to a large degree comparable to this provision.[1622] The main difference is the fact that the Convention on Cybercrime focuses on the criminalization of acts related to information and communication services ("producing child pornography for the purpose of its distribution through a computer system") while the Convention on the Protection of Children mainly takes a broader approach ("producing child pornography") and even covers acts that are not related to computer networks.

Despite the similarities with regard to the acts covered, Article 20 of the Convention on the Protection of Children contains one act that is not covered by the Convention. Based on Article 20, paragraph 1f) of the Convention on the Protection of Children, the act of obtaining access to child pornography through a computer is criminalized. Obtaining access covers any act of initiating the process of displaying information made available through ICTs. This is the case, for example, if the offender enters the domain name of a known child-pornography website and initiates the process of receiving the information from the first page which involves a necessary automated download process. It enables law-enforcement agencies to prosecute offenders in cases where they are able to prove that the offender opened websites with child pornography but are unable to prove that the offender downloaded material. Such difficulties in collecting evidence do, for example, arise if the offender is using encryption technology to protect downloaded files on his storage media.[1623] The Explanatory Report to the Convention on the Protection of children points out that the provision should also be applicable in cases where the offender only watches child pornography pictures online without downloading them.[1624] In general, opening a website automatically initiates a download process – often without the knowledge of the user.[1625] The case mentioned in the Explanatory Report is therefore only relevant in those cases where a download in the background is not taking place. But it is also applicable in cases where consumption of child pornography can take place without download of material. This can, for example, occur if the website enables streaming videos and, due to the technical configuration of the streaming process, does not buffer the received information but discards it straight after transmission (e.g. if the offender is using video streaming).

### Commonwealth Computer and Computer-related Crimes Model Law

An approach in line with Article 9 of the Council of Europe Convention on Cybercrime can be found in section 10 of the 2002 Commonwealth Model Law.[1626]

***Child pornography***
***10*** *(1) A person who, intentionally, does any of the following acts:*
*(a) publishes child pornography through a computer system; or*
*(b) produces child pornography for the purpose of its publication through a computer system; or*
*(c) possesses child pornography in a computer system or on a computer data storage medium; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*[1627]
*(2) It is a defence to a charge of an offence under paragraph (1) (a) or (1)(c) if the person establishes that the child pornography was a bona fide scientific, research, medical or law enforcement purpose.*[1628]
*(3) In this section:*
*"child pornography" includes material that visually depicts:*
*(a) a minor engaged in sexually explicit conduct; or*
*(b) a person who appears to be a minor engaged in sexually explicit conduct; or*
*(c) realistic images representing a minor engaged in sexually explicit conduct.*

> *"minor" means a person under the age of [x] years.*
> *"publish" includes:*
> *(a) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way; or*
> *(b) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a); or*
> *(c) print, photograph, copy or make in any other manner (whether of the same or of a different kind or nature) for the purpose of doing an act referred to in paragraph (a).*

The main differences with the Council of Europe Convention on Cybercrime is the fact that the Commonwealth Model Law does not provide a fixed definition of the term "minor" and leaves it to the Member States to define the age-limit. Like the Council of Europe Convention on Cybercrime, the Commonwealth Model Law does not provide for criminalization of obtaining access to child pornography through information technology.

#### Optional Protocol to the UN Convention on the Rights of the Child

A technology-neutral approach can be found in Article 3 of the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.

> ***Article 3***
> *1 . Each State Party shall ensure that, as a minimum, the following acts and activities are fully covered under its criminal or penal law, whether these offences are committed domestically or transnationally or on an individual or organized basis:*
> *[...]*
> *(c) Producing, distributing, disseminating, importing, exporting, offering, selling or possessing for the above purposes child pornography as defined in Article 2.*
> *[...]*

While the Optional Protocol does explicitly refer to the role of the Internet in distributing such material,[1629] it criminalizes acts related to child pornography in a technology-neutral way. Child pornography is defined as any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities, or any representation of the sexual parts of a child for primarily sexual purposes.[1630] The acts covered are comparable to the acts covered in the Convention on Cybercrime, with the exception that the provision in Article 3 was drafted so as to be technology neutral.

#### Stanford Draft International Convention

The informal[1631] 1999 Stanford Draft International Convention (the "Stanford Draft") does not contain any provision criminalizing the exchange of child pornography through computer systems. The drafters of the Stanford Draft pointed out that in general no type of speech or publication is to be treated as criminal under the Stanford Draft.[1632] Recognizing different national approaches, the drafters of the Stanford Draft left it to the states to decide about this aspect of criminalization.[1633]

### *6.2.9 Solicitation of children*

The Internet offers the possibility of communicating with others without disclosing one's age or gender. This ability can be abused by offenders to solicit children.[1634] The phenomenon is frequently called "grooming".[1635] Some regional legal frameworks contain provisions criminalizing such contact.

#### Council of Europe Convention on the Protection of Children

One example is Article 23 of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.[1636]

***Article 23 – Solicitation of children for sexual purposes***
*Each Party shall take the necessary legislative or other measures to criminalise the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2, for the purpose of committing any of the offences established in accordance with Article 18, paragraph 1.a, or Article 20, paragraph 1.a, against him or her, where this proposal has been followed by material acts leading to such a meeting.*

The solicitation of a child for the purpose of sexually abusing the child is in general not covered by provisions criminalizing the sexual abuse of children, insofar as the solicitation is considered a preparatory act. Having regard to the increasing debate on online grooming, the drafters of the Convention decided to include Article 23 to criminalize already preparatory acts.[1637] To avoid over-criminalization, the drafter of the Convention underlined that simple sexual chatting with a child should not be considered sufficient for committing the act of solicitation, although this can be part of the preparation of a sexual abuse.[1638]

The are two main problems related to this approach. First, the provision only covers solicitation through ICTs. Other forms of solicitation are not covered by the provision. The drafters expressed the view that the focus on such technologies is justified since they are difficult to monitor.[1639] However, no scientifically reliable data were provided to demonstrate that the solicitation of children is a mere online problem. In addition, there are good reasons not only to avoid situations where something that is illegal when committed offline is legal when committed online, but also, conversely, to make sure not to criminalize conduct online when it is legal offline. The 2001 Joint Declaration on Challenges to Freedom of Expression in the New Century, for example, points out that states should not adopt separate rules limiting Internet content.[1640]

Another problem with the criminalization of this preparatory act is the fact that it might lead to conflicts in the criminal law system, insofar as the preparation of even more serious acts is not covered. It would challenge a country's value system if the preparation of sexual abuse of a child were to be criminalized, while the preparation of murder of a child was not. Therefore, any such approach should be formulated within an overall discussion of the advantages and risks of the criminalization of preparatory acts.

### 6.2.10 Hate speech, racism

The degree of criminalization of hate speech differs significantly.[1641] Especially in countries with strong constitutional protection of freedom of speech,[1642] hate speech is often not criminalized. Prohibitions can be found especially in Africa and Europe.[1643]

#### Council of Europe Convention on Cybercrime (Additional Protocol)

The Council of Europe is playing an active role in the fight against racism, and after the Vienna Summit in 1993 adopted a Declaration and Action Plan on Combating Racism, Xenophobia, Anti-Semitism and Intolerance.[1644] In 1995, the Council of Europe adopted recommendations on fighting racism.[1645] During the negotiation of the Council of Europe Convention on Cybercrime, the criminalization of online hate speech and racism was discussed. Since the parties negotiating the Convention on Cybercrime could not agree[1646] on a common position on the criminalization of hate speech and xenophobic material, provisions related to these offences were integrated into a separate First Protocol to the Convention.[1647] One of the main difficulties of provisions criminalizing xenophobic material is to keep a balance between ensuring freedom of speech[1648] on the one hand and preventing the violation of the rights of individuals or groups on the other hand. Without going into detail, the difficulties in the negotiation of the Council of Europe Convention on Cybercrime[1649] and the status of the signatures/ratifications of the Additional Protocol[1650] demonstrate that the different extent of the protection of freedom of speech is hindering a harmonization process.[1651] Especially with regard to the common principle of dual criminality,[1652] lack of harmonization leads to difficulties in enforcement in cases with an international dimension.[1653]

### The provision

***Article 3 – Dissemination of racist and xenophobic material through computer systems***

*1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.*

*2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.*

*3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.*

***Article 4 – Racist and xenophobic motivated threat***

*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.*

***Article 5 – Racist and xenophobic motivated insult***

*1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.*

*2. A Party may either:*

*a. require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or*

*b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.*

***Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity***

*1. Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right: distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.*

*2. A Party may either*

*a. require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise*

*b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.*

### The acts covered:

Article 3 criminalizes the intentional distribution and making available of xenophobic material to the public through a computer system.[1654] Consequently, traditional ways of distribution that do not involve computer systems (like books and magazines) are not covered. Based on the definition provided by Article 2, racist and xenophobic material is any written material, image or any other representation of ideas or theories which advocates, promotes or incites hatred, discrimination or violence, against any

individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors. "Distribution" means the active dissemination of material.[1655] "Making available" covers the act of placing material online.[1656] It requires that users can gain access to the material. The act can be committed by placing material on websites or connecting to file-sharing systems and enabling others to access such material in unblocked storage capacities or folders. The Explanatory Report points out that also the creation or compilation of hyperlinks should be covered. [1657] Since hyperlinks only facilitate the access to material, such an interpretation goes beyond the text of the provision. Distribution covers active acts of forwarding racist or xenophobic material to others. Criminalization requires in addition that the distribution and making available include an interaction with the public, and thereby excludes private communication.[1658]

Article 6 follows a similar approach to Article 3, criminalizing distributing or making available, through a computer system to the public,[1659] material which denies, grossly minimizes, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognized as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognized by that Party.

Article 4 criminalizes threatening persons, through a computer system, with the commission of a serious criminal offence, for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, or a group of persons which is distinguished by any of these characteristics. It refers to threats which create fear in the persons at whom they are directed that they will suffer the commission of an offence.[1660] The term "threatening", unlike Article 3, does not require any interaction with the public and therefore also covers sending out e-mails to the victim.

Article 5 adopts a similar approach to Article 4, criminalizing insulting persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or a group of persons which is distinguished by any of these characteristics. "Insulting" refers to any offensive or invective expression which prejudices the dignity of a person and is directly connected with the insulted person's belonging to the group. To avoid conflict with the principle of freedom of speech,[1661] it is necessary to define the act of insult narrowly. The main difference between Article 4 and Article 5 is the fact that the provision only requires publicly insulting, and therefore excludes private communication (such as e-mail).[1662]

#### Stanford Draft International Convention

The informal[1663] 1999 Stanford Draft International Convention (the "Stanford Draft") does not include a provision criminalizing hate speech. The drafters of the Stanford Draft pointed out that in general no type of speech, or publication, is to be treated as criminal under the Stanford Draft.[1664] Recognizing different national approaches, the drafters of the Stanford Draft left it to the states to decide about this aspect of criminalization.[1665]

### *6.2.11 Religious offences*

The intensity of the protection of religions and their symbols differs between countries.[1666] A number of concerns are expressed with regard to criminalization. It is pointed out in the 2006 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression that in "many countries, overbroad rules in this area are abused by the powerful to limit non-traditional, dissenting, critical, or minority voices, or discussion about challenging social issues".[1667] The 2008 Joint Declaration highlights that international organizations, including the United Nations General Assembly and Human Rights Council, should resist from the further adoption of statements supporting the idea of criminalizing defamation of religions.

### Council of Europe Convention on Cybercrime (Additional Protocol)

Negotiations on this topic among the parties of the Convention on Cybercrime encountered the same difficulties that were discovered with regard to xenophobic material.[1668] Nonetheless, the countries that negotiated the provisions for the First Additional Protocol to the Convention on Cybercrime agreed to add religion as a subject of protection in two provisions.

### The provisions

***Article 4 – Racist and xenophobic motivated threat***
*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.*

***Article 5 – Racist and xenophobic motivated insult***

1. *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.*
   *[…]*

Although these two provisions treat religion as a characteristic, they do not protect religion or religious symbols through criminalization. The provisions criminalize threats and insults to people for the reason that they belong to a group.

### Examples from national legislation

Some countries go beyond this approach and further criminalize acts related to religious issues. One example is section 295B to section 295C of the Pakistani Penal Code.

***295-B**. Defiling, etc., of Holy Qur'an: Whoever wilfully defiles, damages or desecrates a copy of the Holy Qur'an or of an extract therefrom or uses it in any derogatory manner or for any unlawful purpose shall be punishable with imprisonment for life.*
***295-C**. Use of derogatory remarks, etc., in respect of the Holy Prophet: Whoever by words, either spoken or written, or by visible representation or by any imputation, innuendo, or insinuation, directly or indirectly, defiles the sacred name of the Holy Prophet Muhammad (peace be upon him) shall be punished with death, or imprisonment for life, and shall also be liable to fine.*

With regard to uncertainties regarding the application of this provision, the draft of the Pakistan Electronic Crime Bill 2006 had contained two provisions that focused on Internet-related offences,[1669] but those provisions were deleted when the bill was reintroduced as the Prevention of Electronic Crimes Act in 2007,[1670] proclaimed in December 2007.[1671]

***20. Defiling etc, of copy of Holy Quran** – Whoever, using any electronic system or electronic device wilfully defiles, damages or desecrates a copy of the Holy Quran or of an extract there from or uses it in any derogatory manner or for any unlawful purpose shall be punished with imprisonment of life.*

***21. Use of derogatory remarks etc, in respect of the Holy Prophet*** *– Whoever, using any electronic system or electronic device by words, either spoken or written, or by visible representation, or by any imputation, innuendo, or insinuation, directly or indirectly, defiles the sacred name of the Holy Prophet Mohammed (peace be upon him) shall be punished with death, or imprisonment for life and shall be liable to fine.*

As with provisions criminalizing the distribution of xenophobic material via the Internet, one of the main challenges of global approaches criminalizing religious offences is the principle of freedom of speech.[1672] As pointed out previously, the different extent of protection of freedom of speech is a hindrance for the harmonization process.[1673] Especially with regard to the common principle of dual criminality,[1674] the lack of harmonization leads to difficulties in enforcement in cases with an international dimension.[1675]

### 6.2.12 Illegal gambling

The growing number of websites offering illegal gambling is a concern,[1676] as they can be used to circumvent the prohibition on gambling in force in some countries.[1677] If services are operated from places that do not prohibit online gambling, it is difficult for countries that criminalize the operation of Internet gambling to prevent their citizens from using these services.[1678]

#### Example from national legislation

The Council of Europe Convention on Cybercrime does not contain a prohibition of online gambling. One example of a national approach in this regard is section 284 German Penal Code:

#### Example

*Section 284 Unauthorized Organization of a Game of Chance*
*(1) Whoever, without the permission of a public authority, publicly organizes or runs a game of chance or makes the equipment therefore available, shall be punished with imprisonment for not more than two years or a fine.*
*(2) Games of chance in clubs or private parties in which games of chance are regularly organized shall qualify as publicly organized.*
*(3) Whoever, in cases under subsection (1), acts:*
*1. professionally; or*
*2. as a member of a gang which has combined for the continued commission of such acts, shall be punished with imprisonment from three months to five years.*
*(4) Whoever recruits for a public game of chance (subsections (1) and (2)), shall be punished with imprisonment for not more than one year or a fine.*

The provision intends to limit the risks of addiction[1679] to gambling by defining procedures for the organization of such games.[1680] It does not explicitly focus on Internet-related games of chance, but includes them as well.[1681] In this regard, it criminalizes the operation of illegal gambling, without the permission of the competent public authority. In addition, it criminalizes anyone who (intentionally) makes equipment available that is then used for illegal gambling.[1682] This criminalization goes beyond the consequences of aiding and abetting, as offenders can face higher sentences.[1683]

To avoid criminal investigations, the operator of illegal gambling websites can physically move their activities[1684] to countries that do not criminalize illegal gambling.[1685] Such move to locations is a challenge for law-enforcement agencies because the fact that a server is located outside the territory of a country[1686] does not in general affect the possibilities of users inside the country to access it.[1687] In order to improve the ability of law-enforcement agencies to fight against illegal gambling, the German Government has extended the criminalization to users.[1688] Based on section 285, law-enforcement agencies can prosecute users who participate in illegal gambling and can initiate investigations even where operators of games of chance cannot be prosecuted, if they are located outside Germany:

*Section 285 Participation in an Unauthorized Game of Chance*
*Whoever participates in a public game of chance (Section 284) shall be punished with imprisonment for not more than six months or a fine of not more than one hundred eighty daily rates.*

If offenders use gambling sites for money-laundering activities, the identification of offenders is often difficult.[1689] One example of an approach[1690] to prevent illegal gambling and money-laundering activities is the United States Unlawful Internet Gambling Enforcement Act of 2005.[1691]

***§ 5363. Prohibition on acceptance of any financial instrument for unlawful Internet gambling***
*No person engaged in the business of betting or wagering may knowingly accept, in connection with the participation of another person in unlawful Internet gambling*
*(1) credit, or the proceeds of credit, extended to or on behalf of such other person (including credit extended through the use of a credit card);*
*(2) an electronic fund transfer, or funds transmitted by or through a money transmitting business, or the proceeds of an electronic fund transfer or money transmitting service, from or on behalf of such other person;*
*(3) any check, draft, or similar instrument which is drawn by or on behalf of such other person and is drawn on or payable at or through any financial institution; or*
*(4) the proceeds of any other form of financial transaction, as the Secretary may prescribe by regulation, which involves a financial institution as a payor or financial intermediary on behalf of or for the benefit of such other person.*
***§ 5364. Policies and procedures to identify and prevent restricted transactions***
*(a) Before the end of the 270-day period beginning on the date of the enactment of this subchapter, the Secretary, in consultation with the Board of Governors of the Federal Reserve System and the Attorney General, shall prescribe regulations requiring each designated payment system, and all participants therein, to identify and prevent restricted transactions through the establishment of policies and procedures reasonably designed to identify and prevent restricted transactions in any of the following ways:*
*(1) The establishment of policies and procedures that*
*(A) allow the payment system and any person involved in the payment system to identify restricted transactions by means of codes in authorization messages or by other means; and*
*(B) block restricted transactions identified as a result of the policies and procedures developed pursuant to subparagraph (A).*
*(2) The establishment of policies and procedures that prevent the acceptance of the products or services of the payment system in connection with a restricted transaction.*
*(b) In prescribing regulations under subsection (a) the Secretary shall*
*(1) identify types of policies and procedures, including nonexclusive examples, which would be deemed, as applicable, to be reasonably designed to identify, block, or prevent the acceptance of the products or services with respect to each type of restricted transaction;*
*(2) to the extent practical, permit any participant in a payment system to choose among alternative means of identifying and blocking, or otherwise preventing the acceptance of the products or services of the payment system or participant in connection with, restricted transactions; and*
*(3) consider exempting restricted transactions from any requirement imposed under such regulations, if the Secretary finds that it is not reasonably practical to identify and block, or otherwise prevent, such transactions.*
*(c) A financial transaction provider shall be considered to be in compliance with the regulations prescribed under subsection (a), if*
*(1) such person relies on and complies with the policies and procedures of a designated payment system of which it is a member or participant to*
*(A) identify and block restricted transactions; or*
*(B) otherwise prevent the acceptance of the products or services of the payment system, member, or participant in connection with restricted transactions; and*

*(2) such policies and procedures of the designated payment system comply with the requirements of regulations prescribed under subsection (a).*

*(d) A person that is subject to a regulation prescribed or order issued under this subchapter and blocks, or otherwise refuses to honor a transaction*

*(1) that is a restricted transaction;*

*(2) that such person reasonably believes to be a restricted transaction; or*

*(3) as a member of a designated payment system in reliance on the policies and procedures of the payment system, in an effort to comply with regulations prescribed under subsection (a), shall not be liable to any party for such action.*

*(e) The requirements of this section shall be enforced exclusively by the Federal functional regulators and the Federal Trade Commission, in the manner provided in section 505(a) of the Gramm-Leach-Bliley Act.*

***5366. Criminal penalties***

*(a) Whoever violates section 5363 shall be fined under title 18, or imprisoned for not more than 5 years, or both.*

*(b) Upon conviction of a person under this section, the court may enter a permanent injunction enjoining such person from placing, receiving, or otherwise making bets or wagers or sending, receiving, or inviting information assisting in the placing of bets or wagers.*

The intention of the act is to address the challenges and threats of (cross-border) Internet gambling.[1692] The act contains two important regulations. First, it prohibits acceptance of any financial instrument for unlawful Internet gambling by any person engaged in the business of betting or wagering. This provision does not regulate action undertaken by the user of Internet gambling sites or financial institutions.[1693] A violation of this prohibition can lead to criminal sanctions.[1694] Second, it requires the Secretary of the Treasury and the Board of Governors of the Federal Reserve System to prescribe regulations that require financial transaction providers to identify and block restricted transactions in connection with unlawful Internet gambling through reasonable policies and procedures. This second regulation applies not only to persons engaged in the business of betting or wagering, but to all financial institutions in general. Unlike the acceptance of financial instruments for unlawful Internet gambling by persons engaged in the business of betting or wagering, financial institutions do not in general face criminal liability. With regard to the international impact of the regulation, potential conflicts with the General Agreement on Trade in Services (GATS)[1695] are currently being investigated.[1696]

### 6.2.13 Libel and defamation

Libel and the publication of false information are not acts that are exclusively committed on networks. But as pointed out previously, the possibility of anonymous communication[1697] and logistic challenges related to the huge amount of available information in the Internet[1698] are abstract parameters that support those acts.

The question whether this requires criminalization of defamation is controversial.[1699] Concerns regarding the criminalization of defamation are especially related to potential conflict with the principle of "freedom of speech". Thus, a number of organizations have called for a replacement of criminal defamation laws.[1700] The UN Special Rapporteur on Freedom of Opinion and Expression and the OSCE Representative on Freedom of the Media have stated: "Criminal defamation is not a justifiable restriction on freedom of expression; all criminal defamation laws should be abolished and replaced, where necessary, with appropriate civil defamation laws".

Despite these concerns, some countries[1701] have implemented criminal law provisions that criminalize libel, as well as the publication of false information. It is important to highlight that even in the countries that criminalize defamation the number of cases varies considerably. While in the United Kingdom nobody in 2004 and just one suspect in 2005 was charged with libel,[1702] the German crime statistics record 187 527 defamation offences for 2006.[1703] The Council of Europe Convention on Cybercrime, the Commonwealth Model Law and the Stanford Draft do not contain any provisions directly addressing these acts.

#### Example from national legislation

One example of a criminal law provision addressing libel is section 365 of the Criminal Code of Queensland (Australia). Queensland reintroduced criminal liability for defamation by the 2002 Criminal Defamation Amendment Bill 2002.[1704]

#### The provision

*365 Criminal defamation*[1705]
*(1) Any person who, without lawful excuse, publishes matter defamatory of another living person (the relevant person)—*

*(a) knowing the matter to be false or without having regard to whether the matter is true or false; and*

*(b) intending to cause serious harm to the relevant person or any other person or without having regard to whether serious harm to the relevant person or any other person is caused; commits a misdemeanour. Maximum penalty—3 years imprisonment.*

*(2) In a proceeding for an offence defined in this section, the accused person has a lawful excuse for the publication of defamatory matter about the relevant person if, and only if, subsection (3) applies. […]*

Another example of the criminalization of libel is section 185 of the German Penal Code:

#### The provision

*Section 185 Insult*
*Insult shall be punished with imprisonment for not more than one year or a fine and, if the insult is committed by means of violence, with imprisonment for not more than two years or a fine.*

Both provisions were not designed to cover Internet-related acts only. Their application is not limited to certain means of communication, so it can cover acts committed within the network, as well as acts committed outside the network.

### 6.2.14 Spam

Having regard to the fact that up to 75 per cent[1706] of all e-mails are reported to be spam[1707] e-mails, the need for criminal sanctions on spam e-mails has been discussed intensively.[1708] National legislative solutions addressing spam differ.[1709] One of the main reasons why spam is still a problem is that filter technology still cannot identify and block all spam e-mails.[1710] Protection measures offer only limited protection against unsolicited e-mails.

In 2005, OECD published a report that analysed the impact of spam for developing countries.[1711] The report points out that representatives from developing countries often express the view that Internet users in their countries are suffering much more from the impact of spam and net abuse. An analysis of the results of the report proves that the impression of the representatives is right. Due to the more limited and more expensive resources, spam turns out to be a much more serious issue in developing countries than in western countries.[1712]

However, it is not only the identification of spam e-mail that poses problems. Distinguishing between e-mails that are unwanted by recipients, but sent legally, and those that are sent unlawfully, is a challenge. The current trend towards computer-based transmission (including e-mail and VoIP) highlights the importance of protecting communications from attack. If spam exceeds a certain level, spam e-mails can seriously hinder the use of ICTs and reduce user productivity.

### Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime does not explicitly criminalize spam.[1713] The drafters suggested that the criminalization of such acts should be limited to serious and intentional hindering of communication.[1714] This approach does not focus on unsolicited e-mails, but on the effects on a computer system or network. According to the legal approach adopted in the Council of Europe Convention on Cybercrime, the fight against spam can only be based on unlawful interference with computer networks and systems:

> ***Article 5 – System interference***
> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.*

### Stanford Draft International Convention

The informal[1715] 1999 Stanford Draft Convention does not include a provision criminalizing spam. Like the Council of Europe Convention on Cybercrime, the Stanford Draft only criminalizes spam if the unsolicited e-mails lead to intended system interference.

### HIPCAR Cybercrime Legislative Text

One example of a specific approach is section 15 of the HIPCAR[1716] Cybercrime legislative text:[1717]

> ***SPAM***
> ***15. (1)*** *A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification:*
> *a. initiates the transmission of multiple electronic mail messages from or through such computer system; or*
> *b. uses a protected computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead users, or any electronic mail or Internet service provider, as to the origin of such messages, or*
> *c. materially falsifies header information in multiple electronic mail messages and intentionally initiates the transmission of such messages, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*
> *(2) A country may restrict the criminalization with regard to the transmission of multiple electronic messages within customer or business relationships. A country may decide not to criminalize the conduct in section 15 (1) (a) provided that other effective remedies are available.*

The provision contains three different acts. section 15 (1) (a) covers the process of initiating the transmission of multiple electronic mails. section 3(14) defines multiple electronic mail messages as a mail message, including e-mail and instant messaging, sent to more than a thousand recipients. In this context, the Explanatory Note points out that the limitation of criminalization to acts carried out without lawful excuse or justification plays an important role in distinguishing between legitimate mass mailings (like newsletters) and illegal spam.[1718] Section 15 (1) (b) criminalizes the circumvention of anti-spam technology by abusing protected computer systems to relay or transmit electronic messages. Section 15 (1) (c) covers the circumvention of anti-spam technology by falsifying header information. The Explanatory Note highlights that section 15 requires that the offender carries out the offences intentionally and without lawful excuse or justification.[1719]

### United States Code

This limits the criminalization of spam to those cases where the amount of spam e-mails has a serious impact on the processing power of computer systems. Spam e-mails which undermine the effectiveness

of commerce, but not necessarily the computer system, cannot be prosecuted. A number of countries therefore take a different approach. One example is the United States legislation – 18 USC § 1037.[1720]

> ***§ 1037. Fraud and related activity in connection with electronic mail***
> *(a) In General – Whoever, in or affecting interstate or foreign commerce, knowingly –*
> *(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,*
> *(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,*
> *(3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,*
> *(4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or*
> *(5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses,*
> *or conspires to do so, shall be punished as provided in subsection (b).*
> *(b) Penalties – The punishment for an offense under subsection (a) is–*
> *(1) a fine under this title, imprisonment for not more than 5 years, or both, if–*
> *(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or*
> *(B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;*

The provision was implemented by the CAN-SPAM Act of 2003.[1721] The intention of the act was to create a single national standard designed to control commercial e-mail.[1722] It applies to commercial electronic messages, but not to messages relating to transactions and existing business relationships. The regulatory approach requires that commercial electronic messages include an indication of solicitation, including opt-out instructions and the physical address of the sender.[1723] 18 USC. § 1037 criminalizes the senders of spam e-mails especially if they falsify the header information of e-mails to circumvent filter technology.[1724] In addition, the provision criminalizes unauthorized access to a protected computer and initiation of the transmission of multiple commercial electronic mail messages.

### 6.2.15 Misuse of devices

Another serious issue is the availability of software and hardware tools designed to commit crimes.[1725] Apart from the proliferation of "hacking devices", the exchange of passwords that enables unauthorized users to access computer systems is a serious challenge.[1726] The availability and potential threat of these devices makes it difficult to focus criminalization on the use of these tools to commit crimes only. Most national criminal law systems have some provision criminalizing the preparation and production of these tools, in addition to the "attempt of an offence". One approach to fight against the distribution of such devices is criminalization of the production of the tools. In general, this criminalization – which usually accompanies extensive forward displacement of criminal liability – is limited to the most serious crimes. Especially in EU legislation, there are tendencies to extend criminalization of preparatory acts to less grave offences. [1727]

#### Council of Europe Convention on Cybercrime

Taking into account other Council of Europe initiatives, the drafters of the Convention on Cybercrime established an independent criminal offence for specific illegal acts regarding certain devices or access to

data to be misused for the purposes of committing offences against the confidentiality, integrity and availability of computer systems or data:[1728]

### The provision

***Article 6 – Misuse of devices***

*(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:*

*(a) the production, sale, procurement for use, import, distribution or otherwise making available of:*

*(i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;*

*(ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and*

*(b) the possession of an item referred to in paragraphs a) i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.*

*(2) This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.*

*(3) Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.*

### The objects covered

Paragraph 1(a) identifies both the devices[1729] designed to commit and promote cybercrime and passwords that enable access to a computer system. The term "devices" covers hardware as well as software-based solutions to commit one of the mentioned offences. The Explanatory Report mentions for example software such as virus programs, or programs designed or adapted to gain access to computer systems.[1730] "Computer password, access code, or similar data", unlike devices, do not perform operations, but constitute access codes. One question discussed in this context is the question whether the publication of system vulnerabilities is covered by the provision.[1731] Unlike classic access codes, system vulnerabilities do not necessarily enable immediate access to a computer system, but enable the offender to make use of the vulnerabilities to successfully attack a computer system.

### The acts covered

The Convention on Cybercrime criminalizes a wide range of actions. In addition to production, it also sanctions the sale, procurement for use, import, distribution or other availability of devices and passwords. A similar approach (limited to devices designed to circumvent technical measures) can be found in EU legislation on the harmonization of copyrights,[1732] and a number of countries have implemented similar provisions in their criminal law.[1733] "Distribution" covers active acts of forwarding devices or passwords to others.[1734] In the context of Article 6, "sale" describes activities involved in selling the devices and passwords in return for money or other compensation. "Procurement for use" covers acts related to the active obtaining of passwords and devices.[1735] The fact that the act of procuring is linked to the use of such tools generally requires intent on the part of the offender to procure the tools for a use that goes beyond the "regular" intent, i.e. "that it be used for the purpose of committing any of the offences established in Articles 2 through 5". "Import" covers acts of obtaining devices and access codes from foreign countries.[1736] As a result, offenders that import such tools to sell them can be prosecuted even before they offer the tools. Having regard to the fact that the procurement of such tools is only criminalized if it can be linked to use, it is questionable whether the sole import without the intention to sell or use the tools is covered by Article 6 of the Council of Europe Convention on Cybercrime. "Making

available" refers to an act that enables other users to get access to items.[1737] The Explanatory Report suggests that the term "making available" is also intended to cover the creation or compilation of hyperlinks in order to facilitate access to such devices. [1738]

### Dual use tools

Unlike the European Union approach to the harmonization of copyrights,[1739] the provision does not only apply to devices that are exclusively designed to facilitate committing cybercrime; the Convention on Cybercrime also covers devices that are generally used for legal purposes, where the offenders' specific intent is to commit cybercrime. In the Explanatory Report, the drafters suggested that the limitation to devices designed solely to commit crimes was too narrow and could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision virtually inapplicable or only applicable in rare instances.[1740]

To ensure the proper protection of computer systems, experts use and possess various software tools that could make them a possible focus of law enforcement. The Convention on Cybercrime addresses these concerns in three ways[1741]: It enables the parties in Article 6, paragraph 1, sub-paragraph (b) to make reservations regarding the possession of a minimum number of such items before criminal liability is attributed. Apart from this, criminalization of the possession of these devices is limited by the requirement of intent to use the device to commit a crime as set out in Article 2 to 5 of the Convention on Cybercrime.[1742] The Explanatory Report points out that this special intent was included to "avoid the danger of over-criminalisation where devices are produced and put on the market for legitimate purposes, e.g. to counter attacks against computer systems".[1743] Finally, the drafters of the Convention on Cybercrime clearly state in paragraph 2 that tools created for authorized testing or for the protection of a computer system are not covered by the provision, as the provision covers unauthorized acts.

### Criminalization of possession

Paragraph 1, sub-paragraph (b) takes the regulation in paragraph 1, sub-paragraph (a) further, by criminalizing the possession of devices or passwords, if linked to the intent to commit cybercrime. Criminalization of the possession of tools is controversial.[1744] Article 6 is not limited to tools that are designed exclusively for committing crimes, and opponents of criminalization are concerned that criminalization of the possession of these devices could create unacceptable risks for system administrators and network-security experts.[1745] The Convention on Cybercrime enables the parties to require that a certain number of such items be possessed before criminal liability attaches.

### Mental element

Like all other offences defined by the Council of Europe Convention on Cybercrime, Article 6 requires that the offender is carrying out the offences intentionally.[1746] In addition to the regular intent with regard to the acts covered, Article 6 of the Convention on Cybercrime requires an additional specific intent that the device is used for the purpose of committing any of the offences established in Article 2-5 of the Convention.[1747]

### Without right

Similarly to the provisions discussed above, the acts must be committed "without right".[1748] With regard to the fears that the provision could be used to criminalize the legitimate operation of software tools under self-protection measures. the drafters of the Convention on Cybercrime pointed out that such acts are not considered as being carried out "without right".[1749]

### Restrictions and reservations

Due to the debate on the need for criminalization of the possession of devices, the Convention on Cybercrime offers the option of a complex reservation in Article 6, paragraph 3 (in addition to paragraph 1, sub-paragraph (b), sentence 2). If a Party uses this reservation, it can exclude criminalization of the

possession of tools and a number of illegal actions under paragraph 1, sub-paragraph (a), e.g. in the production of such devices.[1750]

### Commonwealth Computer and Computer-related Crimes Model Law

An approach similar to Art. 6 of the Council of Europe Convention on Cybercrime can be found in Sec. 9 of the 2002 Commonwealth Model Law.[1751]

> ***Illegal devices***
> ***9.***
> *(1) A person commits an offence if the person:*
> *(a) intentionally or recklessly, without lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available:*
> *(i) a device, including a computer program, that is designed or adapted for the purpose of committing an offence against section 5, 6, 7 or 8; or*
> *(ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed;*
> *with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8; or*
> *(b) has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8.*
> *(2) A person found guilty of an offence against this section is liable to a penalty of imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*

While the devices covered by the provision and the acts mentioned are the same, the main difference from the Council of Europe Convention on Cybercrime is the fact that the Commonwealth Model Law criminalizes reckless acts in addition to intentional acts, while the Convention on Cybercrime requires an intention in all cases. During negotiation of the Commonwealth Model Law, further amendments to the provision that criminalize the possession of such devices were discussed. The expert group suggested criminalization of offenders possessing more than one item.[1752] Canada proposed a similar approach without predefining the number of items that would lead to criminalization. [1753]

### Stanford Draft International Convention

The informal[1754] 1999 Stanford Draft International Convention ("Stanford Draft") includes a provision criminalizing acts related to certain illegal devices.

> ***Article 3*** *– Offenses*
> *1. Offenses under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognized authority, permission, or consent:*
> *[...]*
> *(e) manufactures, sells, uses, posts, or otherwise distributes any device or program intended for the purpose of committing any conduct prohibited by Articles 3 and 4 of this Convention;*

The drafters of the Stanford Draft pointed out that in general no type of speech, or publication, is to be treated as criminal under the Stanford Draft.[1755] The only exemption they make relates to illegal devices.[1756] In this context, the drafters highlighted that criminalization should be limited to the acts mentioned and, for example, not cover the discussion of system vulnerabilities.[1757]

### HIPCAR Cybercrime Legislative Text

An interesting approach can be found in the legislative text developed by the beneficiary states within the HIPCAR initiative.[1758]

***Illegal Devices***
***10***.
*[…]*
*(3) A country may decide not to criminalize the mere unauthorized access provided that other effective remedies are available. Furthermore, a country may decide to limit the criminalization to devices listed in a Schedule.*

In order to prevent over-criminalization, the drafter decided to include the possibility of limiting the criminalization by introducing a blacklist. In this case, only devices contained in the list are covered by the provision. Such an approach limits the risks of criminalizing acts that are desirable from the point of view of cybersecurity. However, maintaining such a list would very likely require significant resources.

### 6.2.16 Computer-related forgery

Criminal proceedings involving computer-related forgery have tended to be rare, because most legal documents have been tangible documents. With digitization, this situation is changing.[1759] The trend towards digital documents is supported by the creation of a legal background for their use, e.g. by the legal recognition of digital signatures. In addition, provisions against computer-related forgery play an important role in the fight against "phishing".[1760]

#### Council of Europe Convention on Cybercrime

Most criminal law systems criminalize the forgery of tangible documents.[1761] The drafters of the Convention on Cybercrime pointed out that the dogmatic structures of national legal approaches vary.[1762] While one concept is based on the authenticity of the author of the documents another is based on the authenticity of the statement. The drafters decided to implement minimum standards and protect the security and reliability of electronic data by creating a parallel offence to the traditional forgery of tangible documents to fill gaps in criminal law that might not apply to electronically stored data.[1763]

#### The provision

***Article 7 – Computer-related forgery***
*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.*

#### The object covered

The target of a computer-related forgery is data – irrespective of whether they are directly readable and/or intelligible. Computer data is defined by the Convention on Cybercrime[1764] as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function". The provision does not only refer to computer data as the object of one of the acts mentioned. In addition, it is necessary that the acts result in inauthentic data.

Article 7 requires – at least with regard to the mental element – that the data be the equivalent of a public or private document. This means that data must be legally relevant:[1765] the forgery of data that cannot be used for legal purposes is not covered by the provision.

#### The acts covered

The "input" of data[1766] must correspond to the production of a false tangible document.[1767] The term "alteration" refers to the modification of existing data.[1768] The Explanatory Report particularly specifies

variations and partial changes.[1769] The term "suppression" of computer data denotes an action that affects the availability of data.[1770] In the Explanatory Report, the drafters specifically refer to holding back or concealment of data.[1771] The act can for example be carried out by blocking certain information from a database during the automatic creation of an electronic document. The term "deletion" corresponds to the definition of the term in Article 4 covering acts where information is removed.[1772] The Explanatory Report only refers to the removal of data from a data medium.[1773] But the scope of the provision strongly supports a broader definition of the term "deletion". Based on such a broad definition, the act can either be carried out by removing an entire file or by partly erasing information in a file.[1774]

#### Mental element

Like all other offences defined by the Council of Europe Convention on Cybercrime, Article 3 requires that the offender is carrying out the offences intentionally.[1775] The Convention on Cybercrime does not contain a definition of the term "intentionally". In the Explanatory Report, the drafters pointed out that "intentionally" should be defined on a national level.[1776]

#### Without right

Acts of forgery can only be prosecuted under Article 7 of the Convention on Cybercrime if they occur "without right". [1777]

#### Restrictions and reservations

Article 7 also offers the possibility of making a reservation in order to limit criminalization, by requiring additional elements, such as the intent to defraud, before criminal liability arises.[1778]

#### Commonwealth Computer and Computer-related Crimes Model Law

The 2002 Commonwealth Model Law does not contain any provision criminalizing computer-related forgery.[1779]

#### Stanford Draft International Convention

The informal[1780] 1999 Stanford Draft International Convention includes a provision criminalizing acts related to falsified computer data.

> ***Article 3 – Offenses***
> *1. Offenses under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognized authority, permission, or consent:*
> *[...]*
> *(b) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data in a cyber system for the purpose and with the effect of providing false information in order to cause substantial damage to persons or property;*
> *[...]*

The main difference in relation to Article 7 of the Council of Europe Convention on Cybercrime is the fact that Article 3 1b) does not focus on the mere manipulation of data, but requires interference with a computer system. Article 7 of the Council of Europe Convention on Cybercrime does not require such an act; it is sufficient that the offender has acted with the intent that it be considered or acted upon for legal purposes as if it were authentic.

### *6.2.17 Identity theft*

Taking into consideration media coverage,[1781] the results of recent surveys[1782] and the numerous legal and technical publications[1783] in this field, it seems appropriate to refer to identity theft as a mass phenomenon.[1784] Despite the global aspects of the phenomenon, not all countries have yet implemented

provisions in their national criminal law system that criminalize all acts related to identity theft. The Commission of the European Union (the EC) recently stated that identity theft has not yet been criminalized in all EU Member States.[1785] The EC expressed its view that "EU law enforcement cooperation would be better served, were identity theft criminalised in all Member States" and announced that it will shortly commence consultations to assess whether such legislation is appropriate. [1786]

One of the problems with comparing the existing legal instruments in the fight against identity theft is the fact that they differ dramatically.[1787] The only consistent element of existing approaches is the fact that the condemned behaviour relates to one or more of the following phases:[1788]

- Phase 1: Act of obtaining identity-related information.
- Phase 2: Act of possessing or transferring the identity-related information.
- Phase 3: Act of using the identity-related information for criminal purposes.

Based on this observation, there are in general two systematic approaches to criminalize identity theft:

- The creation of a single provision that criminalizes the act of obtaining, possessing and using identity-related information (for criminal purposes).
- The individual criminalization of typical acts related to obtaining identity-related information (like illegal access, the production and dissemination of malicious software, computer-related forgery, data espionage and data interference) as well as acts related to the possession and use of such information (like computer-related fraud).

### Examples of single-provision approaches

The most well-known examples of single-provision approaches are 18 USC § 1028(a)(7) and 18 USC 1028A(a)(1). The provisions cover a wide range of offences related to identity theft. Within this approach, criminalization is not limited to any given phase but covers all of the three above-mentioned phases. Nevertheless, it is important to highlight that the provision does not cover all identity-theft related activities – especially not those where the victim and not the offender is acting.

***§ 1028. Fraud and related activity in connection with identification documents, authentication features, and information***

*(a) Whoever, in a circumstance described in subsection (c) of this section –*

*(1) knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document;*

*(2) knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority;*

*(3) knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other*
*than those issued lawfully for the use of the possessor), authentication features, or false identification documents;*

*(4) knowingly possesses an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States;*

*(5) knowingly produces, transfers, or possesses a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature which will be so used;*

*(6) knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States which is stolen or produced without lawful authority knowing that such document or feature was stolen or produced without such authority;*

*(7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or*

*(8) knowingly traffics in false or actual authentication features for use in false identification documents, document-making implements, or means of identification;*

*shall be punished as provided in subsection (b) of this section.*

*[…]*

***§ 1028A. Aggravated identity theft***

*(a) Offenses.–*

*(1) In general.– Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.*

*[…]*

### Phase 1

In order to commit crimes related to identity theft, the offender needs to obtain possession of identity-related data.[1789] By criminalizing the "transfer" of means of identification with the intent to commit an offence, the provisions criminalize the acts related to phase 1 in a very broad way.[1790] Due to the fact that the provisions focus on the transfer act, they do not cover acts undertaken by the offender prior to initiation of the transfer process.[1791] Acts like sending out phishing mails and designing malicious software that can be used to obtain computer identity related data from the victims are not covered by 18 USC § 1028(a)(7) and 18 USC 1028A(a)(1).

### Phase 2

By criminalizing possession with the intent to commit an offence, the provisions again take a broad approach with regard to the criminalization of acts related to the second phase. This includes, especially, the possession of identity-related information with the intention to use it later in one of the classic offences related to identity theft.[1792] The possession of identity-related data without the intent to use them is not covered.[1793]

### Phase 3

By criminalizing the "use" with the intent to commit an offence, the provisions cover the acts related to phase 3. 18 USC § 1028(a)(7) is, as mentioned above, not linked to a specific offence (like fraud).

Another example is section 14 of the Cybercrime legislative text that was developed by the beneficiary states within the HIPCAR initiative.[1794]

***Identity-related Crimes***

***14.***

*A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer system in any stage of the offence, intentionally transfers, possesses, or uses, without lawful excuse or justification, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*

The provision covers the major phases of typical identity-related crimes described above. Only the first phase, in which the offender obtains the identity-related information, is not covered. "Transfer" of means of identity covers data-transmission processes from one computer to another computer system. This act is especially relevant to cover the sale (and related transfer) of identity-related information.[1795] "Possession" is the control a person intentionally exercises over identity-related information. "Use" covers a wide range of practices, such as submitting such information for purchase online. With regard to the mental element, the provision requires that the offender acts intentionally with regard to all objective elements and in addition has specific intent to undertake the activity to commit, aid or abet any unlawful activity that goes beyond the transfer, possession or use of identity-related information.

#### Example of a multiple-provision approach

The main difference between the Council of Europe Convention on Cybercrime and single-provision approaches (like for example the United States approach) is the fact that the Convention on Cybercrime does not define a separate cyberoffence of the unlawful use of identity-related information.[1796] Similar to the situation with regard to the criminalization of obtaining identity-related information, the Convention on Cybercrime does not cover all possible acts related to the unlawful use of personal information.

#### Phase 1

The Council of Europe Convention on Cybercrime[1797] contains a number of provisions that criminalize Internet-related identity-theft acts in phase 1. These are especially:

- Illegal access (Article 2)[1798]
- Illegal interception (Article 3)[1799]
- Data interference (Article 4)[1800]

Taking into consideration the various ways in which an offender can access the data, it must be pointed out that not all possible acts in phase 1 are covered. One example of an offence that is often related to phase 1 of identity theft but is not covered by the Council of Europe Convention on Cybercrime is data espionage.

#### Phase 2

Acts that take place between obtaining information and using it for criminal purposes can hardly be covered by the Council of Europe Convention on Cybercrime. It is especially not possible to prevent a growing black market for identity-related information by criminalizing the sale of such information based on the provisions provided by the Convention on Cybercrime.

#### Phase 3

The Council of Europe Convention on Cybercrime defines a number of cybercrime-related offences. Some of these offences can be committed by the perpetrator using identity-related information. One example is computer-related fraud, which is often mentioned in the context of identity theft.[1801] Surveys on identity theft show that most of the data obtained are used for credit-card fraud.[1802] If the credit-card fraud is committed online, it is likely that the perpetrator can be prosecuted based on Article 8 of the Council of Europe Convention on Cybercrime. Other offences that can be carried out using identity-related information obtained previously that are not mentioned in the Convention on Cybercrime are not covered by the legal framework. It is especially not possible to prosecute the use of identity-related information with the intention to conceal identity.

### *6.2.18 Computer-related fraud*

Fraud is a popular crime in cyberspace.[1803] It is also a common problem beyond the Internet, so most national laws contain provisions criminalizing fraud offences.[1804] However, the application of existing provisions to Internet-related cases can be difficult, where traditional national criminal law provisions are based on the falsity of a person.[1805] In many cases of fraud committed over the Internet, it is in fact a

computer system that responds to an act of the offender. If traditional criminal provisions addressing fraud do not cover computer systems, an update of the national law is necessary.[1806]

### Council of Europe Convention on Cybercrime

The Convention on Cybercrime seeks to criminalize any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property, by providing an article on computer-related fraud:[1807]

### The provision

> ***Article 8 – Computer-related fraud***
> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:*
> *a. any input, alteration, deletion or suppression of computer data,*
> *b. any interference with the functioning of a computer system,*
> *with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.*

### The acts covered

Article 8 a) contains a list of the most relevant acts of computer-related fraud.[1808] "Input" of computer data covers all kind of input manipulation such as feeding incorrect data into the computer as well as computer software manipulations and other acts of interference in the course of data processing.[1809] "Alteration" refers to the modification of existing data.[1810] The term "suppression" of computer data denotes an action that affects the availability of data.[1811] "Deletion" corresponds to the definition of the term in Article 4 covering acts where information is removed.[1812]

In addition to the list of acts, Article 8, sub-paragraph b) contains the general clause that criminalizes fraud-related "interference with the functioning of a computer system". The general clause was added to the list of covered acts in order to leave the provision open to further developments.[1813]

The Explanatory Report points out that "interference with the functioning of a computer system" covers acts such as hardware manipulations, acts suppressing printouts and acts affecting recording or flow of data, or the sequence in which programs are run.[1814]

### Economic loss

Under most national criminal law, the criminal act must result in an economic loss. The Convention on Cybercrime follows a similar concept and limits criminalization to those acts where the manipulations produce direct economic or possessory loss of another person's property including money, tangibles and intangibles with an economic value.[1815]

### Mental element

As for the other offences listed, Article 8 of the Council of Europe Convention on Cybercrime requires that the offender has acted intentionally. This intent refers to the manipulation as well as the financial loss.

In addition, the Convention on Cybercrime requires that the offender has acted with a fraudulent or dishonest intent to gain economic or other benefit for self or other.[1816] As examples of acts excluded from criminal liability due to lack of specific intent, the Explanatory Report mentions commercial practices arising from market competition that may cause economic harm to one person and benefit to another, but that are not carried out with fraudulent or dishonest intent.[1817]

#### Without right

Computer-related fraud can only be prosecuted under Article 8 of the Convention on Cybercrime if it is carried out "without right". [1818] This includes the requirement that the economic benefit must be obtained without right. The drafters of the Convention on Cybercrime pointed out that acts carried out pursuant to a valid contract between the affected persons are not considered to be without right.[1819]

#### Commonwealth Computer and Computer-related Crimes Model Law

The 2002 Commonwealth Model Law does not contain a provision criminalizing computer-related fraud.[1820]

#### Stanford Draft International Convention

The informal[1821] 1999 Stanford Draft International Convention does not contain a provision criminalizing computer-related fraud.

### 6.2.19 Copyright crimes

The switch from analogue to digital distribution of copyright-protected content marks a turning point in copyright violation.[1822] The reproduction of music artwork and videos has historically been limited, since the reproduction of an analogue source was often accompanied by a loss of quality of the copy, which in turn limits the option to use the copy as a source for further reproductions. With the switch to digital sources, quality is preserved and consistent quality copies have become possible.[1823]

The entertainment industry has responded by implementing technical measures (digital rights management or DRM) to prevent reproduction[1824], but until now these measures have typically been circumvented shortly after their introduction.[1825] Various software tools are available over the Internet that enable users to copy music CDs and movie DVDs protected by DRM-systems. In addition, the Internet offers unlimited distribution opportunities. As a result, the infringement of intellectual property rights (especially of copyright) is a widely committed offence over the Internet.[1826]

#### Council of Europe Convention on Cybercrime

The Convention on Cybercrime includes a provision covering these copyright offences that seeks to harmonize the various regulations in national laws. This provision turned out to be one of the main obstacles to the use of the Convention on Cybercrime outside of Europe.

***Article 10 – Offences related to infringements of copyright and related rights***
*(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.*
*(2) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.*

*(3) A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.*

The infringement of copyrights is criminalized in some countries[1827] and addressed by a number of international treaties.[1828] The Convention on Cybercrime aims to provide fundamental principles regarding the criminalization of copyright violations in order to harmonize existing national legislation. Patent or trademark-related violations are not covered by the provision.[1829]

### Reference to international agreements

Unlike other legal frameworks, the Convention on Cybercrime does not explicitly name the acts to be criminalized, but refers to a number of international agreements.[1830] This is one of the aspects which has been criticized with regard to Article 10. Apart from the fact that it makes it more difficult to discover the extent of criminalization and that the agreements might subsequently be changed, the question was raised whether the Convention on Cybercrime obliges the signatory states to sign the international agreements mentioned in Article 10. The drafters of the Convention on Cybercrime pointed out that no such obligation shall be introduced by the Council of Europe Convention on Cybercrime.[1831] Those states that have not signed the mentioned international agreements are therefore neither obliged to sign the agreements nor forced to criminalize acts related to agreements they have not signed. Article 10 thus only places obligations on those parties that have signed one of the mentioned agreements.

### Mental element

Due to its general nature, the Convention on Cybercrime limits criminalization to acts committed by means of a computer system.[1832] In addition to acts committed over a computer system, criminal liability is limited to acts that are committed wilfully and on a commercial scale. The term "wilfully" corresponds to "intentionally" used in the other substantive law provisions of the Convention on Cybercrime and takes account of the terminology used in Article 61 of the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement[1833], which governs the obligation to criminalize copyright violations.[1834]

### Commercial scale

The limitation to acts that are committed on a commercial scale also takes account of the TRIPS Agreement, which requires criminal sanctions only for "piracy on a commercial scale". As most copyright violations in file-sharing systems are not committed on a commercial scale, they are not covered by Article 10. The Convention on Cybercrime seeks to set minimum standards for Internet-related offences. Thus, parties can go beyond the threshold of "commercial scale" in the criminalization of copyright violations.[1835]

### Without right

In general the substantive criminal law provisions defined by the Council of Europe Convention on Cybercrime require that the act is carried out "without right".[1836] The drafters of the Convention on Cybercrime pointed out that the term "infringement" already implies that the act was committed without authorization.[1837]

### Restrictions and reservations

Paragraph 3 enables signatories to make a reservation, as long as other effective remedies are available and the reservation does not derogate from the parties' international obligations.

### Stanford Draft International Convention

The informal[1838] 1999 Stanford Draft International Convention ("Stanford Draft") does not include a provision criminalizing copyright violations. The drafters of Stanford Draft pointed out that copyright

crimes were not included because this may have proven difficult.[1839] Instead, they referred directly to the existing international agreements.[1840]

### 6.2.20 Terrorist use of the Internet

As pointed out above, the term "terrorist use of the Internet" is used to describe a set of activities that range from spreading of propaganda to targeted attacks. With regard to the legal response, it is possible to distinguish between three different systematic approaches.

#### Systematic approaches

#### Use of existing cybercrime legislation

The first approach is the use of existing cybercrime legislation (developed to cover non-terrorist related acts) to criminalize terrorist use of the Internet. In this context, three aspects need to be taken into consideration. First, substantive criminal law provisions that were implemented to cover non-terrorist related acts such as system interference[1841] might be applicable in terrorist-related cases, but very often the range for sentencing will differ from specific terrorism legislation. This could influence the ability to use sophisticated investigation instruments that are restricted to terrorist or organized crime investigation. Secondly, the application of cybercrime-specific investigation instruments in cases of terrorist use of the Internet faces fewer challenges, insofar as most countries do not limit the application of sophisticated investigation instruments to traditional cybercrime offences, but include any offence involving computer data. Finally, regional legal instruments developed to address the challenge of cybercrime but not specifically terrorist use of the Internet often contain exemptions for international cooperation with regard to political offences. One example is Article 27, paragraph 4.a. of the Council of Europe Convention on Cybercrime.[1842]

> ***Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements***
> *[…]*
> *4. The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:*
> *a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or*
> *b it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.*
> *[…]*

The provision authorizes parties to the Convention to refuse mutual assistance requests if they concern an offence which the requested Party considers a political offence or an offence connected with a political offence. This can seriously hinder investigations. As a consequence, terrorism-specific legal frameworks such as the Council of Europe Convention on the Prevention of Terrorism from 2005[1843] contain an exclusion of the political exception clause.

> ***Article 20 – Exclusion of the political exception clause***
> *1 None of the offences referred to in Articles 5 to 7 and 9 of this Convention, shall be regarded, for the purposes of extradition or mutual legal assistance, as a political offence, an offence connected with a political offence, or as an offence inspired by political motives. Accordingly, a request for extradition or for mutual legal assistance based on such an offence may not be refused on the sole ground that it concerns a political offence or an offence connected with a political offence or an offence inspired by political motives.*
> *[…]*

### Use of existing anti-terrorism legislation

The second approach is the use of existing terrorism legislation to criminalize and prosecute terrorist use of the Internet. Such a traditional instrument is, for example, the 2005 Council of Europe Convention on the Prevention of Terrorism.[1844]

> ***Article 5 – Public provocation to commit a terrorist offence***
> *1. For the purposes of this Convention, public provocation to commit a terrorist offence means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed.*
> *2. Each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist offence, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.*

> ***Article 6 – Recruitment for terrorism***
> *1. For the purposes of this Convention, recruitment for terrorism means to solicit another person to commit or participate in the commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group.*
> *2. Each Party shall adopt such measures as may be necessary to establish recruitment for terrorism, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.*

The Convention on the Prevention of Terrorism contains several offences such as public provocation to commit a terrorist offence and recruitment for terrorism but does not, for example, contain provisions criminalizing terrorism-related attacks against computer systems. Furthermore, the Convention does not contain procedural instruments. Especially with regard to the investigation of Internet-related offences specific procedural instruments are often required. Identifying an offender who has incited terrorism using websites requires sophisticated instruments such as the expedited preservation of traffic data.

### Specific legislation

The third approach is the development of specific legislation addressing terrorist use of the Internet.

### Examples of specific legislation

As pointed out above, the term “terrorist use of the Internet” is used to describe a set of activities that range from spreading of propaganda to targeted attacks. In terms of the legal response, there are two main areas of regulation: computer-related attacks and illegal content.

### Computer-related attacks

One approach for a provision that specifically addresses terrorism-related computer attacks is Section 66F of the Indian Information Technology Act 2000, amended in 2008:

> *66F Punishment for cyber terrorism – Information Technology Act, 2000. [As Amended by Information technology (Amendment) Act 2008]*
> *(1) Whoever,-*
> *(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –*
> *(i) denying or cause the denial of access to any person authorized to access computer resource; or*
> *(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or*
> *(iii) introducing or causing to introduce any Computer Contaminant.*

*and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or*

*(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.*

*(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.*

Section 66F of the Indian Information Technology Act does not only require that the offender is acting with terrorism-related intent ("intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people") but also that the offence leads to severe damage such as death, injury or the disruption of services affecting critical information infrastructure.

### Illegal content

Illegal content such as terrorist propaganda is one area where states are particularly sticking to technology-neutral approaches. One example of such a technology-neutral approach is Article 10 of the Russian Federal Law 149-FZ of 27.07.2006 on Information, Information Technologies and Protection of Information.

***Article 10**. Spreading of Information or Providing of Information*

*[…]*

*6. It is forbidden to spread information aimed at war propaganda, national, racial or religious discrimination and hostility, as well other information whose spreading is liable to criminal or administrative responsibility.*

This provision does not specifically address the distribution of illegal content through computer networks or making content available on such networks, but was drafted so as to be technology neutral.

Another example of a technology-neutral approach is Article 3 of the 2008 amendment of the EU Council Framework Decision[1845] on Combating Terrorism.[1846]

***Article 3 – Offences linked to terrorist activities***

*1. For the purposes of this Framework Decision:*

*(a) "public provocation to commit a terrorist offence" shall mean the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of one of the offences listed in*

*Article 1(1)(a) to (h), where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed;*

*(b) "recruitment for terrorism" shall mean soliciting another person to commit one of the offences listed in Article 1(1)(a) to (h), or in Article 2(2);*

*(c) "training for terrorism" shall mean providing instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing one of the offences listed in Article 1(1)(a) to (h), knowing that the skills provided are intended to be used for this purpose.*

*2. Each Member State shall take the necessary measures to ensure that offences linked to terrorist activities include the following intentional acts:*

*(a) public provocation to commit a terrorist offence;*

*(b) recruitment for terrorism;*

*(c) training for terrorism;*

*(d) aggravated theft with a view to committing one of the offences listed in Article 1(1);*

*(e) extortion with a view to the perpetration of one of the offences listed in Article 1(1);*

*(f) drawing up false administrative documents with a view to committing one of the offences listed in Article 1(1)(a) to (h) and Article 2(2)(b).*

*3. For an act as set out in paragraph 2 to be punishable, it shall not be necessary that a terrorist offence be actually committed.'*

The drafters emphasize in the introduction that the existing legal framework criminalizes aiding, abetting and inciting terrorism but does not criminalize the dissemination of terrorist expertise through the Internet. In this context, the drafters pointed out that "the Internet is used to inspire and mobilise local terrorist networks and individuals in Europe and also serves as a source of information on terrorist means and methods, thus functioning as a 'virtual training camp'."[1847] Despite the fact that terrorist use of the Internet was explicitly mentioned in the introduction, the provision provided is drafted in a technology-neutral manner and consequently covers both online and offline acts of training for terrorism.[1848] One challenge related to the application of the provision in Internet-related cases is the difficulty of proving that the offender acted knowing that the skills provided were intended to be used for this purpose. It is quite likely that the need for such evidence will limit the provision's applicability to online guides to weaponry. As most weapons and explosives can be used to commit regular crimes as well as terrorist-related offences, the mere publication of this type of information does not prove that the publisher knew how it would be used. Therefore, the context of the publication (e.g. the fact that it appears on a website operated by a terrorist organization) will need to be considered. This can present challenges if the information published is outside the context of other terrorism-related content, e.g. disseminated through file-sharing systems or file-hosting services.

One example of an Internet-specific approach is Article 5 of the Chinese Computer Information Network and Internet Security, Protection and Management Regulations.

*"**Article 5**: No unit or individual may use the Internet to create, replicate, retrieve, or transmit the following kinds of information:*

*(1) Inciting to resist or breaking the Constitution or laws or the implementation of administrative regulations;*

*(2) Inciting to overthrow the government of the socialist system;*

*(3) Inciting division of the country, harming national unification;*

*(4) Inciting hatred or discrimination among nationalities or harming the unity of the nationalities;*

*(5) Making falsehoods or distorting the truth, spreading rumors, destroying the order of society;*

*(6) Promoting feudal superstitious, sexually suggestive material, gambling, violence, murder;*

*(7) Terrorism, or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people;*

*(8) Injuring the reputation of state organs;*

*(9) Other activities against the Constitution, law or administrative regulations."*

## Cyberwarfare

Although threats related to cyberwarfare have been discussed for several decades, the debate on legal response has only just started. Even more than cybercrime, cyberwarfare is governed by international law. The Hague Conventions, the Geneva Conventions and the UN Charter are important instruments of international law which contain regulations governing the laws of war. While there is significant practice of applying those instruments to regular armed conflicts, their application to computer and network-based attacks runs into difficulties. This can be demonstrated by analysing the applicability of Article 2(4) of the UN Charter, banning the use of force.

> ***Art. 2*** *UN Charter*
> *The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles.*
> *[...]*
> *(4) All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.*
> *[...]*

The prohibition of the use of force intends to enforce a comprehensive ban on all types of force, except those which are in line with the UN Charter.[1849] In recent decades, the prohibition of the use of force in Article 2 (4) has been challenged several times. One of the main challenges has been the shift from full-scale wars that constituted the focus when the UN Charter was drafted after World War II to small-scale warfare which is much more frequent nowadays.[1850] Covering computer-related attacks adds another dimension to the challenge, insofar as not only the scale but also the methods and tools used within the conflict differ.[1851] Consequently, the main difficulty related to the application of Article 2 is interpretation of the term "use of force". Neither the UN Charter nor any related international instrument clearly defines the term "use of force". It is widely accepted that not all types of hostile acts are prohibited by the UN Charter. Attacks with conventional weapons are covered, for example, but not the threat of force and economic coercion.[1852]

The two constituent elements of the use of force are the use of weapons and the involvement of state actors. Even though the importance of the latter, in particular, was questioned by Security Council resolutions after the 9/11 attacks, both elements remain essential with regard to the ban on the use of force.

### Use of weapons/destruction of life and property

The first constituting element is the use of weapons. Computer technology used to carry out Internet-related attacks can hardly be called a traditional weapon, insofar as such weapons in general involve a kinetic impact.[1853] Nevertheless, the need to include chemical and biological weapons has already required a shift from an action-oriented definition to an impact-oriented approach. Under such a broader approach, weapons could be defined as a tool to destroy life or property.[1854]

Even based upon a broad interpretation of this type, however, it is challenging to cover computer and network-based attacks as use of force and computer technology as weapons, since the impact of the attacks is different.[1855] Not only the methods used but also the effects differ in relation to traditional armed conflicts.[1856] Traditional military strategies involving the use of weapons focus on the physical termination of an enemy's military capabilities. Computer and network-based attacks can be carried out with minimal physical damage and loss of life.[1857] Unlike a missile attack, a denial-of-service attack that temporarily shuts down a government website does not cause any actual physical harm. However, it would be misleading to contend that computer attacks cannot lead to serious harm. A DoS attack against the computer system of a hospital or blood bank can pose a serious threat to health and endanger the lives of a large number of people. The discovery of the possible physical impact of Stuxnet is another example showing that computer attacks do not necessarily have non-physical consequences. If computer

and network-based attacks have such a physical impact, they can be considered to be similar to traditional weapons.[1858]

### Conflict among states

As pointed out above, the second requirement for the application of Article 2 of the UN Charter is that the use of force is undertaken by a state against another state. Despite recent trends to broaden the application of the UN Charter acts committed by non-state actors are not covered by Article 2 of the UN Charter. This is of great relevance for the coverage of cyberwarfare, insofar as here – unlike in traditional wars – non-state actors play a more important role. There are serious concerns with regard to proliferation, as non-state actors can acquire powerful resources that might even go beyond those controlled by states.[1859] The largest botnets contain several million computer systems. This number is potentially larger than the number of state-controlled computer systems available for military interventions in most states. The capabilities of non-state actors is highly relevant, since they primarily act outside the international legal framework which binds states. This raises concerns with regard to attribution. The application of Article 2 of the UN Charter so far requires that a computer attack be traced back to a state. Experiences with incidents in Estonia in 2007 and Georgia in 2008 underscore that, in most cases, identification or verification of the source of an attack may be an insuperable challenge.

## 6.3 Digital evidence

**Bibliography (selected):** *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Casey*, Digital Evidence and Computer Crime, 2004; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Cohen*, Digital Still Camera Forensics, Small Scale Digital Device Forensics Journal, 2007, Vol. 1, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V1_1_Cohen.pdf; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf; *Gercke*, Impact of Cloud Computing on the work of law enforcement agencies, published in *Taeger/Wiebe*, Inside the Cloud, 2009, page 499 *et seq.*; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2; *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002; *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-mail: A Trusted E-mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4; *Harrington*, A Methodology for Digital Forensics, T.M. Cooley J. Prac. & Clinical L., 2004, Vol. 7; *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No.3; *Heaton-Armstrong/Shepherd/Wolchover*, Analysing Witness Testimony: Psychological, Investigative and Evidential Perspective, 2002; *Hayes*, Forensic Handwriting Examination, 2006; *Hilton*, Identification of the Work from an IBM Selectric Typewriter, Journal of Forensic Sciences, 1962; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1; *Houck/Siegel*, Fundamentals of Forensic Science, 2010; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008; *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006; *Koppenhaver*, Forensic Document Examination: Principles and Practice, 2007; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2; *Liberatore/Erdely/Kerle/Levine/Shields*, Forensic investigation of peer-to-peer file sharing networks, Digital Investigations, 2010; *Luque*, Logical Level Analysis of Unix Systems in: Handbook of Computer Crime Investigations: Forensic Tools and Technology, 2001; *Marcella/Marcella/Menendez*, Cyber

Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007; *Makulilo*, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Meghanathan/Allam/Moore*, Tools and Techniques for Network Forensics, International Journal of Network Security and its Applications, 2009, Vol. 1, No.1; *Menezes*, Handbook of Applied Cryptography, 1996; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004; *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12; *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970; *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005; *Vaciago*, Digital Evidence, 2012; *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Wang*, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No.5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1; *Witkowski*, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law & Policy; *Zdziarski*, iPhone Forensics, 2008, available at: www.esearchbook.com/files/4/eSearchBook.1224255173.iPhone%20Forensics.pdf.

Especially due to increasing hard-drive capacities[1860] and the falling cost[1861] of the storage of digital documents compared to the storage of physical documents, the number of digital documents is growing.[1862] Today, a significant amount of data is stored in digital form only.[1863] In addition, computer and network technologies have become part of everyday life in developed countries and increasingly in developing countries. As a consequence, electronic documents such as text documents, digital videos and digital pictures[1864] are playing a role in cybercrime investigations and related court proceedings.[1865]

Yet the impact of digitization and the importance of digital evidence is stretching beyond cybercrime investigation: even when committing traditional crimes, offenders may leave digital traces, such as information on the location of their cellphone[1866] or suspicious search-engine requests.[1867] The ability to exploit specific data-related investigation tools and present digital evidence in court is therefore considered essential for both cybercrime-related and traditional crime investigation.[1868]

Dealing with "digital evidence" presents a number of challenges,[1869] but also opens up new possibilities for investigation and for the work of forensic experts and courts. Already at the first stage – the collection of evidence – the need to be able to handle digital evidence has changed the work of investigators. They need specific investigation tools to carry out investigations. The availability of such instruments is especially relevant if traditional evidence like fingerprints or witnesses is not available. In these cases, the ability to successfully identify and prosecute an offender may be based on the correct collection and evaluation of digital evidence.[1870] Beyond the collection of evidence, however, digitization also influences the way law-enforcement agencies and courts deal with evidence.[1871] While traditional documents are introduced by handing out the original document in court, digital evidence in some cases requires specific procedures that do not allow conversion into traditional evidence, e.g. by presenting a printout of files and other discovered data.[1872]

The following chapter provides an overview of practical and legal aspects of digital evidence and cybercrime investigations.

### 6.3.1 Definition of digital evidence

The digitization and emerging use of ICT has a huge impact on procedures for the collection of evidence and its use in court.[1873] As a consequence of the development, digital evidence has been introduced as a new source of evidence.[1874] There is no single definition of electronic or digital evidence.[1875] The United Kingdom (UK) Police and Criminal Evidence Code defines digital evidence as "all information contained in a computer".[1876] A broader approach defines digital evidence as any data stored or transmitted using computer technology that supports the theory of how an offence occurred.[1877]

### 6.3.2 Importance of digital evidence in cybercrime investigations

Digital evidence plays an important role in various phases of cybercrime investigations. It is in general possible to divide between two major phases[1878]: the investigation phase (identification of relevant evidence[1879], collection and preservation of evidence[1880], analysis of computer technology and digital evidence) and the presentation and use of evidence in court proceedings.

The first phase is linked to computer forensics, which will be discussed more in detail below. The term "computer forensics" describes the systematic analysis of IT equipment with the purpose of searching for digital evidence.[1881] The constant growth in the amount of data stored in digital format highlights the logistic challenges of investigations.[1882] Approaches to automated forensic procedures by, for example, using hash-value based searches for known child-pornography images[1883] or keyword searches[1884] therefore play an important role in addition to manual investigations.[1885] Computer forensics include investigations such as analysing the hardware and software used by a suspect,[1886] recovering deleted files,[1887] decrypting files[1888] or identifying Internet users by analysing traffic data.[1889]

The second phase relates to the presentation of digital evidence in court. It is closely linked to specific procedures that are required because digital information can only be made visible when printed out or displayed with the use of computer technology.

### 6.3.3 Growing importance of digital evidence in traditional crime investigations

The ability of investigators to search for data or seize evidence as well as the ability of courts to deal with digital evidence is not limited to cybercrime investigations. Due to the increasing integration of computer technology in people's everyday life, digital evidence is becoming an important source of evidence even in traditional investigation. One example is a murder trial in the US, in which records of search-engine requests stored on the suspect's computer were used to prove that, prior to the murder, the suspect was intensively using search engines to find information on undetectable poisons.

### 6.3.4 New opportunities for investigation

Depending on the ICT and Internet services used by a suspect, a wide variety of digital traces are left.[1890] If, for example, a suspect uses search engines to find online child pornography his search request, then IP-addresses and in some case even additional identity-related information (such as Google ID) are recorded.[1891] Digital cameras used to produce child-pornography images in some cases include geo-information in the file that enables investigators to identify the location where the picture was taken if such images are seized on a server.[1892] Suspects who download illegal content from file-sharing networks can in some cases be traced by the unique ID that is generated in the installation of the file-sharing software.[1893] And the falsification of an electronic document might generate metadata that enable the original author of the document to prove the manipulation.[1894]

Another aspect that is frequently quoted as an advantage is the neutrality and reliability of digital evidence.[1895] In comparison with some other categories of evidence such as witness statements, digital evidence is certainly less vulnerable to influence that can affect the preservation of evidence.[1896]

### 6.3.5 Challenges

In the early days of computer technology, the ability of law enforcement to carry out investigations involving digital data was limited by a lack of computer forensic equipment and expertise.[1897] The growing

importance of digital evidence has spawned an increasing number of computer forensic laboratories. Yet, while the logistical aspects of the issue can be solved fairly easily, a number of challenges remain.

The underlying reason for these challenges is the fact that, despite a number of similarities between digital evidence and other categories of evidence, there are major differences. Some of the general principles[1898], such as the requirement that the evidence be authentic, complete, reliable[1899] and accurate and that the process of obtaining the evidence take place in line with the legal requirements, still hold good.[1900] Alongside the similarities, however, there are a number of aspects that make digital evidence unique and therefore require special attention when dealing with digital evidence in criminal investigations.

### Need for scientific research and training

Digital evidence is a relatively new category of evidence and the field is developing fast. And despite the very limited time-frame available for basic scientific research, the procedures for searching, seizing and analysing digital evidence now already need to be based on scientifically reliable principles and procedures.[1901] Despite intensive research already undertaken there are various areas that require the attention of scientists. It is therefore important that scientific research in controversial areas such the reliability of evidence in general[1902] or the quantification of potential rates of error[1903] should continue. The impact of the constant evolution is not restricted to the need for ongoing scientific research. Given that developments might raise new challenges for forensic examination,[1904] it is necessary to be constantly training experts.

### Need for binding legal standards

Although computer and network technologies are used globally and the challenges related to the admissibility of digital evidence in court are – despite the different legal systems – similar, binding legal standards dealing with digital evidence have not been widely implemented.[1905] Only some countries have so far started to update their relevant legislation to enable courts to deal directly with digital evidence.[1906] As with regard to substantive criminal law and procedural instruments in the fight against cybercrime, here too there is a lack of global harmonization of legal standards, in the area of digital evidence.

### Quantitative aspects

As pointed out above, the low costs[1907] compared to the storage of physical documents are giving rise to an increasing number of digital documents.[1908] Despite the availability of tools to automate search processes[1909], identifying the relevant digital evidence on a storage device that can carry millions of documents is a logistical challenge for investigators.[1910]

### Reliance on expert statements

Analysing and evaluating digital evidence requires special skills and technical understanding which is not necessarily covered in the education received by judges, prosecutors and lawyers. They therefore rely increasingly on the support of experts in the recovery of digital evidence.[1911] While this situation is not significantly different from other sophisticated investigation techniques, such as DNA sequencing, it prompts the need for necessary debate on the consequences for such dependence. To avoid a negative influence, courts are encouraged to question the reliability of evidence and require qualification of the associated uncertainty.[1912]

### Fragile nature of digital evidence

Digital data are highly fragile and can so easily be deleted[1913] or modified[1914] that experts consider it alarming.[1915] Like other categories of evidence, digital data present some degree of uncertainty.[1916] To avoid a negative impact on reliability, the collection of digital evidence is often subject to certain technical requirements. The shutdown of a computer system will, for example, result in a loss of all memory stored in the RAM system memory[1917] unless special technical measures to prevent this process are applied.[1918] In cases where data are stored in a temporary memory, the technique of collecting the evidence can be

different from the process of collecting traditional digital evidence.[1919] Such a sophisticated approach can be necessary, for example, if the suspect is using encryption technology and the investigators want to examine whether information stored in the RAM memory can help them to access encrypted information.[1920]

Modifications can be made both intentionally by the offender or accidentally by the investigators. A loss or modification of data can in the worst scenario lead to wrongful conviction.[1921]

As a consequence of its fragility, one of the most fundamental principles of computer forensics is the need to maintain the integrity of digital evidence.[1922] Integrity can in this context be defined as the property whereby digital data have not been altered in an unauthorized manner since the time they were created, transmitted or stored by an authorized source.[1923] Protecting integrity is necessary to ensure reliability and accuracy.[1924] Handling evidence of this kind requires standards and procedures in order to maintain an effective quality system. This includes general aspects such as case records, the use of widely accepted technology and procedures, and operation by qualified experts only[1925], as well as the application of specific methods such as checksum, hash algorithm and digital signatures.[1926] The required methods are costly and cannot completely exclude the risks of alteration.[1927]

### Limited amount of data recorded

For many Internet users, it is surprising how much information about their activities is stored. The average user might not be aware that when accessing the Internet or carrying out specific actions like using a search engine[1928] he/she is leaving traces. These can be a valuable source of digital evidence in cybercrime investigation. Nonetheless, not all digital information generated during the use of computer technology is stored. Many actions and much information such as clicks and keystrokes are not retained unless special surveillance software is installed.[1929]

### Layer of abstraction

Even if a suspect's activities create digital evidence, this evidence is separated in time from the events it records and is therefore more of a historic record than a live observation.[1930] In addition, the evidence is not necessarily personalized. If, for example, a suspect is using a public Internet café to access child pornography, the traces do not necessarily contain identity-related information that allows identification. Unless the suspect at the same time downloads his e-mails or uses services that require a registration, in which case a link is created. But as this is not necessarily the case, experts point out that this leads to a layer of abstraction that can introduce errors.[1931]

### Requirements related to infrastructure

The design of courtrooms has followed similar principles for decades and in some countries even centuries. Leaving aside aspects of security (e.g. installed metal detectors and x-ray machines) and comfort (e.g. air conditioning), it is possible to use a courtroom designed and equipped a hundred years ago for criminal proceedings.[1932] The need to deal with digital evidence raises challenges, in terms of the layer of abstraction and the fact that digital evidence cannot be presented without tools like printers or screens, has implications for the design of courtrooms.[1933] Screens need to be installed to ensure that the judges, prosecutor, defence lawyers, the accused and of course the jury are able to follow the presentation of evidence. Installing and maintaining such equipment generates significant cost for judicial systems.

### Changing technical environment

As pointed out above, technology is constantly changing. This calls for constant review of procedures and equipment as well as related training in order to ensure the suitability and effectiveness of investigations.[1934] With ever new versions of operating systems or software products, the way data relevant for investigations is stored can change. Similar developments take place with regard to the hardware.[1935] In the past, data were stored on floppy disks. Today, investigators will find that relevant information might be stored on MP3-players or in watches that include a USB-storage device. The

challenges are not limited to keeping up with the latest trends in computer technology.[1936] Forensic experts also need to maintain equipment to deal with discontinued technology, such as 5.25 inch floppy disks. In addition to changes in hardware, discontinued software needs to be accessible: files from discontinued software tools can often not be opened without using the original software.

It is also necessary to carefully study fundamental changes in user behaviour. The availability of broadband access and remote storage servers has, for example, influenced the way information is stored. While in the past investigators were able to focus on the suspect's premises when searching for digital evidence, today they need to take into consideration that files might physically be stored abroad and accessed remotely by the suspect when necessary.[1937] The increasing use of cloud storage presents new challenges for investigators.[1938]

### 6.3.6 Equivalences of digital evidence and traditional evidence

Research undertaken in Europe in 2005/2006 highlighted various areas of equivalence of digital and traditional evidence in the 16 countries analysed.[1939] The most common equivalence is between electronic documents and documents in paper form. Additional equivalences frequently found are electronic mail and traditional mail, electronic signature and traditional handwritten signatures, and electronic notarial deeds and traditional notarial deeds.[1940]

### 6.3.7 Relation between digital evidence and traditional evidence

With regard to the relationship between digital evidence and traditional evidence, it is possible to distinguish between two processes: the replacement of traditional evidence by digital evidence, and the introduction of digital evidence as an additional source complementing traditional forms of evidence such as documents and witnesses.

One example of digital evidence replacing traditional evidence is the increasing use of e-mail instead of letters.[1941] In cases where no physical letters are sent, investigations need to focus on digital evidence. This has implications in respect of the methods available for analysing and presenting the evidence. In the past, when handwritten letters were the dominant means of non-verbal communication, forensic analysis concentrated on forensic handwriting investigation.[1942] Already back when typewriters became popular, the methods employed by forensic experts changed from handwriting forensics to typewriter analysis.[1943] With the ongoing shift from letters to e-mails, investigators need to deal with e-mail forensics[1944] instead.[1945] While, on the one hand, the resulting inability to use physical documents limits the possibility of related investigations, on the upside investigators can now use tools to automate e-mail investigations.[1946]

Although in the majority of cases involving electronic communication the focus will likely be on digital evidence[1947], other categories of evidence can still play in important role in the identification of the offender. This is especially relevant because not all computer operations leave digital traces and not all traces that are left can be linked to the suspect.[1948] If public Internet terminals are used to download child pornography, it might not be possible to link the download process to an identifiable person if that person did not register[1949] or leave any personal information; but the recording on a videosurveillance camera or fingerprints on the keyboard could be useful, if available. Conversely, in traditional crimes where fingerprints, DNA traces and witnesses play a dominant role, digital evidence can be a valuable additional source of evidence. Information about the location of the suspect's phone might allow law-enforcement agencies to identify his location[1950] and suspicious search-engine requests might lead to the location of a missing victim.[1951] With regard to crimes that include financial transactions (such as commercial exchange of child pornography[1952]), investigations can also include records kept by financial organizations in order to identify the offender. In 2007, a global child-pornography investigation relied on the identification of suspects based on records of financial transactions related to the purchase of child pornography.[1953]

### 6.3.8 Admissibility of digital evidence

There are two major areas of discussion with regard to digital evidence: the process of collection of digital evidence, and the admissibility of digital evidence in court. Specific requirements relating to the collection

of digital evidence will be discussed further in the chapter below dealing with procedural law. With regard to the admissibility of digital evidence, despite the differences compared to traditional evidence the fundamental principles are the same. Summarizing those principles is a challenge, though, since not only is there a lack of binding international agreements, but there are also substantial differences in the dogmatic approach to dealing with digital evidence. While some countries give judges wide discretion in admitting or rejecting digital evidence, others have started to develop a legal framework to address the admissibility of evidence in court.[1954]

### Legitimacy

One of the most fundamental requirements for the admissibility of both traditional categories of evidence[1955] and digital evidence alike is the legitimacy of evidence.[1956] This principle requires that digital evidence has been collected, analysed, preserved and finally presented in court in accordance with the appropriate procedures and without violating the fundamental rights of the suspect.[1957] Both the requirements relating to the collection, analysis, preservation and finally presentation of the evidence in court and the consequences of a violation of the suspect's rights differ from country to country. Principles and rules that can possibly be violated range from fundamental rights of a suspect such as privacy[1958] to failure to respect procedural requirements. Due to the often inadequate legislation, general principles of evidence are frequently applied to digital evidence.[1959]

The requirements for the collection of digital evidence are mainly set by criminal procedural law. In most countries, the interception of content data for example requires a court order and an extension of a search to remote storage devices requires that they be located in the same country. If interception takes place without a court order, the appropriate procedures are violated, and the investigation might therefore interfere with the rights of the suspect. The requirements for preservation of evidence are less often defined by law.[1960] However, the fundamental principle of the necessity to protect the integrity of digital evidence is certainly a guideline.[1961] Investigators need to make sure that evidence is not altered in any unauthorized manner from the time it was created, transmitted or stored by an authorized source.[1962] Protecting integrity is necessary in order to ensure reliability and accuracy and to comply with the principle of legitimacy.[1963] The procedures for the presentation of evidence in court are rarely defined by law.

As stated above, not only the requirements but also the consequences of a violation of procedures and the rights of the suspect vary significantly.[1964] While some countries consider evidence to be inadmissible only if collected in a manner which seriously violates the suspect's rights (and not, for example, if only formal requirements were violated) and do not exclude such evidence, other countries – especially those applying the fruit of the poisonous tree doctrine – apply other standards for admissibility.[1965]

### Best evidence rule

For common-law jurisdictions, the best evidence rule is of great importance.[1966] There are some references, mostly in old cases, to a "best evidence rule", which under common law provides that only the best available evidence of a fact at issue is said to be admissible. Whatever status this rule may once have enjoyed, however, there is now very little modern authority for its continued survival and some express assertions of its demise.[1967]

The general rule now appears to be that whether a given item of evidence is the best available evidence or not only affects its weight, not its admissibility.[1968] Closely related to the best evidence rule, the "primary evidence rule" formerly provided that in the case of documentary evidence, only the original document or an "enrolled" copy of that document was admissible to prove its contents and authenticity. However, the old rule has effectively been discarded by the courts, and any surviving remnants of this rule are further limited in criminal proceedings by legislation (which now generally permits the use of authenticated copies).[1969]

The logic of requiring the production of an original document where it is available rather than relying on possibly unsatisfactory copies, or the recollections of witnesses, is clear[1970], although modern techniques make objections to the first alternative weak. In the unavoidable absence of the best or primary evidence

of documents, the court will accept secondary evidence. This is evidence which suggests, on the face of it, that other and better evidence exists. Public and judicial documents are usually proven by copies, without accounting for the absence of the originals; and a statement contained in any document may now be proven by the production of an authenticated copy of the document.[1971] The underlying principle is that risks of mistranscriptions, testimonial misstatements of what the document contains and undetected tampering is reduced.[1972] The rule in strict interpretation permits secondary evidence (in the form of a copy) where the original has been lost.

In regard to digital evidence, this raises a number of questions, insofar as it is necessary to determine what the original is.[1973] As digital data can in general be copied without loss of quality and a presentation of the original data in court is not in all cases possible, the best evidence rule seems to be incompatible with digital evidence. But courts have started to open the rule to new developments by accepting an electronic copy as well as the original document.[1974] The best evidence rule in this broader interpretation does not require a written or witness testimony in every instance, but that the best obtainable evidence of its contents be used.[1975] Moreover, the best evidence rule has been enshrined in most of the statutory regimes established in the common law region.[1976]

### Rule against hearsay

The rule against hearsay is another principle that is particularly relevant for common law countries.[1977] Hearsay evidence is evidence given by a witness in court of a statement made by some other person out of court, when such evidence is tendered to prove the truth of the statement.[1978] Under common law, hearsay evidence was generally inadmissible; but in civil proceedings this rule was abolished in the UK by the Civil Evidence Act 1995, which provides for the admissibility of hearsay evidence subject to statutory safeguards, and preserves a number of common law exceptions to the rule against hearsay.[1979]

According to the common law rule against hearsay, an assertion other than one made by a person while giving oral evidence in the proceedings and tendered as evidence of the facts asserted is inadmissible[1980]. An out-of-court statement, for the purposes of the rule, means any statement other than one made by a witness in the course of giving his evidence, and could include, for example, a statement made in previous legal proceedings. Thus, the statement may have been made unsworn or on oath, orally, in writing or even by way of signs or gestures, by any person, whether or not called as a witness in the proceedings in question. [1981] In addition, the rule intends to enable cross-examination of the real witness and expose weaknesses in a statement.[1982] Instead, it is necessary that a witness with personal knowledge directly proves this. Not only can a witness testimony contain inadmissible hearsay but also exhibits may contain inadmissible hearsay.[1983] A number of reasons have been advanced to justify the common law rule against hearsay, such as the danger of manufactured evidence, relating to the potential unreliability of hearsay evidence. The rules governing the admissibility of hearsay evidence now apply if (and only if) the purpose, or one of the purposes, of the person making the statement appears to the court to have been to cause another person to believe the matter, or to cause another person to act or a machine to operate on the basis that the matter is as stated.[1984]

Having regard to the fact that data collected during an investigation (such as log-files) intend to prove the truth of the matter asserted in the digital evidence itself, strict application of the rule is problematical in an age where very often digital evidence is the most relevant category of evidence in court proceedings, and some common law countries have started to implement statutory exceptions to the hearsay rule.[1985] Evidence produced by computers, cameras or other machines without incorporating any human statement cannot be hearsay.[1986] Under common law, it used to be held that visual images, even when produced by human hands, were not “statements” of any facts they purported to represent and therefore could not be hearsay. But there is now express provision to the contrary.[1987]

Where no statutory exceptions exist, the application of the rule to digital evidence is questioned by pointing out that it only applies to statements that contain within them assertions made by human persons. Information generated mechanically without human intervention would on this basis not be considered as potentially hearsay evidence[1988] unless the process of creating the software is used as an argument to apply the rule even in those cases.[1989]

#### Relevance/effectiveness

Relevance and effectiveness are other common requirements for the admissibility of digital evidence.[1990] Taking into account the amount of data that is stored even on a private computer, only a tiny proportion of which might be relevant for the case, one can see the practical importance of this criterion in cybercrime investigation. Its application is important both to restrict the collection of evidence and for the presentation in court. Unlike with traditional evidence, where during the collection process irrelevant pieces of evidence can simply be ignored, the selection process is more challenging when it comes to digital evidence[1991], since at the time when the computer hardware is seized it is almost impossible to determine whether the storage devices concerned contain relevant information or not.

#### Transparency

Unlike traditional search and seizure operations, which are carried out openly and therefore guarantee that the suspect is aware that an investigation is being carried out, sophisticated investigation tools such as the real-time interception of communications do not require such disclosure. Despite the technical ability, not all countries allow law-enforcement agencies to carry out covert operations, or at least require that the suspect be informed afterwards. Transparency during the whole process of collecting, processing and using evidence in court affords a suspect the possibility to question the legitimacy and relevance of collected evidence.

### *6.3.9 Legal Framework*

While substantive criminal law provisions covering the most common forms of computer crimes can today be found in a large number of countries, the situation with regard to digital evidence is different. Only a few countries have so far addressed specific aspects of digital evidence and, in addition, international binding standards are lacking.[1992]

#### Commonwealth Electronic Evidence Model Law (2002)

In 2000, the Law Ministers of Small Commonwealth Jurisdictions decided to establish a working group to develop model legislation on electronic evidence. The main comparative law analysis finding of the study group was that, with regard to the admissibility of digital evidence, the reliability of the system by which the digital evidence was created is more important than the document itself. The model law from 2002[1993], which was based on legislation from Singapore[1994] and Canada[1995], reflects these findings and covers the most relevant aspects of digital evidence with regard to common law countries, such as application of the best evidence rule[1996] and the integrity of digital evidence.

***General Admissibility***

*3. Nothing in the rules of evidence shall apply to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record.*

Section 3 contains a common element of legal frameworks seeking to regulate aspects of digital evidence which can be found in similar form, for example, in Article 5 of the 1999 EU Directive on digital signatures.[1997] The provision intends to ensure that digital evidence is not inadmissible *per se*. In this respect, section 3 provides the foundation for the use of digital evidence in court proceedings. However, the admissibility of evidence is not guaranteed merely because the evidence is digital. It is necessary for the digital evidence to satisfy the ordinary rules of evidence. If the evidence is hearsay material, it does not become admissible because of section 3.

***Scope of the Act***

*4. (1) This Act does not modify any common law or statutory rule relating to the admissibility or records, except the rules relating to authentication and best evidence.*
*2) A court may have regard to evidence adduced under this Act in applying any common law or statutory rule relating to the admissibility of records.*

***Application of the Best Evidence Rule***

*6. (1) In any legal proceeding, subject to subsection (b), where the best evidence rule is applicable in respect of electronic record, the rule is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored.*
*(2) In any legal proceeding, where an electronic record in the form of printout has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, the printout is the record for the purposes of the best evidence rule.*

As described above, some of the criteria for digital evidence are in potential conflict with traditional principles related to the admissibility of evidence. This is especially relevant in regard to the best evidence rule, which is of great importance for common law countries.[1998] The aim of the best evidence rule is to minimize the risks of mistranscriptions, testimonial misstatements of what the document contains and undetected tampering.[1999] Admissibility of evidence requires that documentary evidence be the best evidence available to the party. Whether this excludes digital evidence *per se* is a matter of controversy.[2000] Sections 4 and 6 of the Commonwealth Electronic Evidence Model Law are examples of a statutory exemption. In this context, section 4 first of all clarifies that the model law modifies solely the principles of authentication and best evidence. Following this general clarification, section 6 modifies the best evidence rule to ensure that digital evidence is not inadmissible *per se*. Based on section 6, digital evidence is not inadmissible due to the best evidence rule provided that the integrity of the system that created the data can be proven.

#### Commonwealth Model Law on Computer and Computer-related Crime (2002)

In 2002, the Draft Commonwealth Model Law on Computer and Computer-related Crime was presented.[2001] In addition to substantive criminal law provisions and procedural instruments, it contains a specific provision dealing with digital evidence.

***Evidence***

*20 In proceedings for an offence against a law of [enacting country], the fact that:*
*(a) it is alleged that an offence of interfering with a computer system has been committed; and*
*(b) evidence has been generated from that computer system;*
*does not of itself prevent that evidence from being admitted.*

The approach is similar to Article 3 of the more specific Commonwealth Electronic Evidence Model Law from 2002.

## 6.4 Justisdiction

**Bibliography (selected):** *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004. *Hirst,* Jurisdiction and the Ambit of the Criminal Law, 2003; *Inazumi,* Universal Jurisdiction in Modern International Law, 2005; *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 5, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf; *Kohl*, Jurisdiction and the Internet: Regulatory Competence over Online Activity, 2007; *Krizek*, Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice, Boston University International Law Journal, 1988, page 337 et seq; *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 69 et seq; *Sachdeva*, International Jurisdiction in Cyberspace: A Comparative Perspective, Computer and Telecommunications Law Review, 2007,, page 245 et seq; *Scassa/Currie*, New First Principles? Assessing the Internet's Challenges to Jurisdiction,

Georgetown Journal of International Law, Vol. 42, 2001, page 117 et seq, available at: http://gjil.org/wp-content/uploads/archives/42.4/zsx00411001017.PDF; United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm; *Valesco*, Jurisdictional Aspects of Cloud Computing, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf; *Van Dervort*, International Law and Organizations: An Introduction, 1998; *Zittrain*, Jurisdiction, Internet Law Series, 2005;

### 6.4.1 Introduction

Cybercrime is a typical transnational crime that involves different jurisdictions. It is not unusual that several countries are affected. The offender might have acted from country A, used an Internet service in country B and the victim is based in country C. This is a challenge with regard to the application of criminal law[2002] and leads to questions about which of the countries has jurisdiction, which country should take forward the investigation and how to resolve disputes. While this case looks already challenging it is necessary to take into consideration that if the offence, for example, involves cloud computing services even more jurisdictions may be triggered.[2003]

The term "jurisdiction" is used to describe various different legal issues.[2004] Based upon principles of public international law "jurisdiction" describes the authority of a sovereign state to regulate certain conduct.[2005] It is therefore one aspect of national sovereignty.[2006] However, in the context of cybercrime investigation "jurisdiction" refers to the authority of a state to enforce its domestic law.[2007] In general, law enforcement will only be able to carry out an investigation if the country has jurisdiction.

### 6.4.2 Different principles of jurisdiction

It is possible to differentiate between different principles of jurisdiction.

### 6.4.3 Principle of territoriality / principle of objective territoriality

The most fundamental principle and most common basis of jurisdiction is the principle of territoriality.[2008] It is applicable if an offence – regardless of the nationality of the offender or victim – is committed within the territory of a sovereign state.[2009] The fact that jurisdiction in general only makes sense if it can be enforced and enforcement of law requires control (that is in general limited to the territory) explains the relevance of the principle. One approach of a computer-specific codification of the principles of territoriality is Article 22 paragraph 1.a Council of Europe Convention on Cybercrime.

***Article 22 – Jurisdiction***
*1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:*
*a. in its territory; or*
*b. on board a ship flying the flag of that Party; or*
*c. on board an aircraft registered under the laws of that Party; or*
*d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.*
*[…]*

The provision is computer specific as it only refers to offences listed in Article 2 to 11 Convention on Cybercrime.

However, the application with regard to cybercrime cases is going along with challenges. A crime was certainly committed if the offender and the victim were physically present in the country while the offender illegally accessed the victim's computer system. But was the offence committed within the

territory of a state if the offender acted from abroad when accessing the computer system of the victim in the country?

Those cases have an extraterritorial element. However, the International Court of Justices expressed in the "Lotus" case that even in cases where countries apply jurisdiction only on the basis of territoriality, extraterritorial conduct may nevertheless be regarded as committed in the territory if one of the constituent elements of the offence (especially its effect) have taken place in the country.[2010] This doctrine, that is also referred to as "principle of objective territoriality"[2011] is highly relevant in cybercrime cases.[2012] But taking into account that a malicious software that was sent out by an offender might affect computer systems in various countries underlines that such extensive definition of territoriality easily leads to possible conflicts of jurisdiction.[2013] The risk of potential conflicts increases even more if the principle of territoriality is applied to cases where neither the offender nor victim are located within the country but only the infrastructure within a country was used within the commission of a crime – for example if an e-mail with illegal content was sent out by using an e-mail provider in one country or a website with illegal content is stored on the server of a hosting provider in the country.

One codification of such broad approach is section 11(3)(b) Singapore Computer Misuse Act 2007.

***Territorial scope of offences under this Act***
*[…]*
*11. —(1) Subject to subsection (2), the provisions of this Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore.*
*(2) Where an offence under this Act is committed by any person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore.*
*(3) For the purposes of this section, this Act shall apply if, for the offence in question —*
*(a) the accused was in Singapore at the material time; or*
*(b) the computer, program or data was in Singapore at the material time.*

This broad approach very likely even leads to an applicability of Singapore legislation with regard to data only transiting through computer systems in Singapore.[2014]

### 6.4.4 Flag principle

The flag principle is closely related to the principle of territoriality but extends the application of domestic laws to aircrafts and ships. Taking into account the availability of Internet access solutions for maritime and air transportation,[2015] raises questions related to the application of criminal law in cases where either the offender, victim or affected computer systems is not located in the territory but outside the territorial borders of country on board of a ship or aircraft.

One example for an approach to regulate such cases is Article 22 paragraph 1.b and 1c Council of Europe Convention on Cybercrime.

***Article 22 – Jurisdiction***
*1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:*
*a. in its territory; or*
*b. on board a ship flying the flag of that Party; or*
*c. on board an aircraft registered under the laws of that Party; or*
*d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.*
*[…]*

### 6.4.5 Effects doctrine / Protective principle

The effects doctrine deals with the establishment of jurisdiction for a crime committed by a foreign national, occurring outside the territory with no element of the conduct taking place in the territory but still having a substantial effect within the territory.[2016] Closely related is the protective principle that establishes jurisdiction in similar cases where a fundamental national interest is triggered. Due to the fact of the absence of the offender, victim and used infrastructure, there are only weak links to a country and the application of the principle is controversially discussed.[2017]

### 6.4.6 Principle of active nationality

The principle of nationality refers to jurisdiction exercised with regard to activities of nationals abroad.[2018] It is related to the power of the state to regulate the behaviour of its nationals not only within its territory but also abroad. This principle is more common in civil law countries than common law countries.[2019] As a consequence common law countries tend to compensate the lack of jurisdiction based on the principle of nationality by a more extensive interpretation of the principle of territoriality.

With regard to the fact that Internet-related crimes can be committed without leaving the country the principle is of less relevance when it comes to cybercrime cases. However, it can be highly relevant in the context of production of child pornography for the purpose of distributing it though computer networks.[2020]

One example for an approach to regulate the principle of nationality is Article 22 paragraph 1.d Council of Europe Convention on Cybercrime.

***Article 22 – Jurisdiction***
*1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:*
*a. in its territory; or*
*b. on board a ship flying the flag of that Party; or*
*c. on board an aircraft registered under the laws of that Party; or*
*d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.*
*[…]*

### 6.4.6 Principle of passive nationality

The principle of passive nationality refers to jurisdiction based on the nationality of the victim. Taking into account the overlapping with the principle of territory, it is only relevant if a national became victim of a crime while being outside the country. The application of the principle is controversially discussed[2021] – especially because it indicates that foreign law is insufficient to protect foreigners – but it has gained more acceptance in the last decades.[2022]

One – non Internet-specific – codification of the principle of passive nationality is section 7 of the German Penal Code.

***Section 7***
*Offences committed abroad—other cases*
*(1) German criminal law shall apply to offences committed abroad against a German, if the act is a criminal offence at the locality of its commission or if that locality is not subject to any criminal jurisdiction.*

### 6.4.7 Principle of universality

The universality principle established jurisdiction in relation to specific crimes that are in the interest of the international community.[2023] This principle is especially relevant with regard to serious crimes such as

crimes against humanity and war crimes.[2024] However, various countries that recognise the principle have developed it further.[2025] As a consequence the principle is under certain circumstances even applicable with regard to cybercrime.

One example for a provision that can be applicable in cybercrime cases is section 6(6) of the German Penal Code.

***Section 6***
*Offences committed abroad against internationally protected legal interests*
*German criminal law shall further apply, regardless of the law of the locality where they are committed, to the following offences committed abroad:*

*1. (repealed) ;*
*2. offences involving nuclear energy, explosives and radiation under section 307 and section 308(1) to (4), section 309(2) and section 310;*
*3. attacks on air and maritime traffic (section 316c);*
*4. human trafficking for the purpose of sexual exploitation, for the purpose of work exploitation and assisting human trafficking (Sections 232 to 233a);*
*5. unlawful drug dealing;*
*6. distribution of pornography under sections 184a, 184b (1) to (3) and section 184c (1) to (3), also in conjunction with section 184d, 1st sentence;*

*[...]*

Based upon section 6 (6) Germany may exercise jurisdiction with regard to Internet websites that offer child pornography for download even if the operator of the website is not located in Germany, the servers are not based in Germany and no German Internet user accessed the website.

## 6.5 Procedural law

**Bibliography (selected):** ABA International Guide to Combating Cybercrime, 2002; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 91; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law, 2007, Vol. 8, No.1; *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Gercke*, Impact of Cloud Computing on the work of law-enforcement agencies, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2; *Gercke*, Convention on Cybercrime, Multimedia und Recht. 2004, page 801; *Gercke*, Preservation of User Data, DUD 2002, page 577 *et seq.*; *Gercke/Tropina*, From Telecommunication Standardization to Cybercrime Harmonization, Computer Law Review International, 2009, Issue 5; *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002; *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No. 3; *Houck/Siegel*, Fundamentals of Forensic Science, 2010; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008; *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004; *Menezes*, Handbook of Applied Cryptography, 1996; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital

Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004; *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12; *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970; *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf; *Slobogin*, Technologically-assisted physical surveillance: The American Bar Association's Tentative Draft Standards, Harvard Journal of Law & Technology, Vol. 10, Nr. 3, 1997; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005; *Vaciago*, Digital Evidence, 2012; *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1.

### 6.5.1 Introduction

As explained in the sections above, the fight against cybercrime requires adequate substantive criminal law provisions.[2026] At least in civil law countries, law-enforcement agencies will not be able to investigate crimes without those laws in place. But the requirement of law-enforcement agencies in the fight against cybercrime is not limited to substantive criminal law provisions.[2027] In order to carry out the investigations they need to undertake – in addition to training and equipment – procedural instruments that enable them to take the measures that are necessary to identify the offender and collect the evidence required for the criminal proceedings.[2028] These measures can be the same ones that are undertaken in other investigations not related to cybercrime – but having regard to the fact that the offender does not necessarily need to be present at or even close to the crime scene, it is very likely that cybercrime investigations need to be carried out in a different way compared to traditional investigations.[2029]

The reason why different investigation techniques are necessary is not only due to the independence of place of action and the crime scene. It is in most cases a combination of a number of the above-mentioned challenges for law-enforcement agencies that make cybercrime investigations unique.[2030] If the offender is based in a different country[2031], uses services that enable anonymous communication and, in addition, commits the crimes by using different public Internet terminals, the crime can hardly be investigated based on traditional instruments like search and seizure alone. To avoid misunderstanding, it is important to point out that cybercrime investigations require classic detective work as well as the application of traditional investigation instruments – but cybercrime investigations face challenges that cannot be solved solely using traditional investigation instruments.[2032]

Some countries have already developed new instruments to enable law-enforcement agencies to investigate cybercrime, as well as traditional crimes that require the analysis of computer data.[2033] As is the case with regard to the substantive criminal law, the Council of Europe Convention on Cybercrime contains a set of provisions that reflect wide accepted minimum standards regarding procedural instruments required for cybercrime investigations.[2034] The following overview will therefore refer to the instruments offered by this international convention and in addition highlight national approaches that go beyond the regulations of the Convention on Cybercrime.

### 6.5.2 Computer and Internet investigations (Computer Forensics)

The term computer forensics is used to describe the systematic collection of data and analysis of computer technology with the purpose of searching for digital evidence.[2035] Such analysis generally takes

place after the crime was committed.[2036] It is thus a major part of computer crime and cybercrime investigation. Investigators carrying out such investigations are confronted with several challenges that are described in more detail in Chapter 3.

The extent of the possible involvement of experts in computer forensics demonstrates its importance in the investigation process. In addition, the dependence of the success of Internet investigations on the availability of forensic resources highlights the need for training in this area. Only if the investigators are either trained in computer forensics or have access to experts in the area can efficient investigation and prosecution of cybercrime be conducted.

### Definition

There are various definitions of "computer forensics".[2037] It can be defined as "the examination of IT equipment and systems in order to obtain information for criminal or civil investigation".[2038] When committing crimes, offenders leave traces.[2039] This statement is valid in traditional investigations as well as computer investigations. The main difference between a traditional investigation and a cybercrime investigation is that a cybercrime investigation generally requires specific data-related investigation techniques and can be facilitated by specialized software tools.[2040] In addition to adequate procedural instruments, carrying out such analysis requires that the authorities possess the ability to manage and analyse the relevant data. Depending on the offences and the computer technology involved, the requirements in terms of procedural investigation tools and forensic analysis techniques differ[2041] and present unique challenges.[2042]

### Phases of forensic investigations

It is in general possible to distinguish between two major phases:[2043] the investigation phase (identification of relevant evidence,[2044] collection and preservation of evidence,[2045] analysis of computer technology and digital evidence) and the presentation and use of evidence in court proceedings. In order to explain the different activities, the following chapter expands the model to four phases.

### Evidence identification procedures

Increasing hard drive capacities[2046] and the falling cost[2047] of the storage of digital documents compared to the storage of physical documents is generating constant growth in the number of digital documents.[2048] Given the need to focus investigations on relevant evidence in order to prevent inadmissibility, special attention must be paid to the identification of evidence.[2049] Consequently, forensic experts play an important role in the design of investigation strategies and the selection of relevant evidence. They can, for example, determine the location of relevant evidence on large storage systems. This enables investigators to limit the scope of the investigation to those parts of the computer infrastructure that are relevant for the investigation and avoid inappropriate and large-scale seizure of computer hardware.[2050] This selection process is relevant as various types of storage device are available that can make identification of the storage location of relevant evidence challenging.[2051] This is especially valid if the suspect is not storing information locally but uses means of remote storage. The availability of broadband access and remote storage servers has influenced the way information is stored. If the suspect is storing information on a server that is located in another country, this simple act can make it more difficult to seize evidence. Forensic analysis can in this case be used to determine whether remote-storage services were used.[2052] Identification of relevant digital information is not confined to files themselves. Databases of software tools that are made available by operating systems to quickly identify files might contain relevant information, too.[2053] Even system-generated temporary files might contain evidence for criminal proceedings.[2054]

Another example of evidence identification is the involvement of forensic experts in determining the right procedural instruments. A number of countries enable law-enforcement agencies to carry out two types of real-time observation – the collection of traffic data in real time, and the interception of content data in real time. In general, the interception of content data is more intrusive than the collection of traffic data. Forensic experts can determine whether the collection of traffic data is sufficient to prove the committing of a crime, and thereby help investigators to strike the right balance between the need to

collect effective evidence and the obligation to protect the rights of the suspect by choosing the least intensive instrument out of the group of equally effect options. Both examples show that the role of forensic investigators is not restricted to the technical aspects of an investigation, but includes a responsibility for protecting the suspect's fundamental rights and thereby avoiding inadmissibility of the evidence collected.[2055]

### Collection and preservation of the evidence

Involvement in the collection of digital evidence requires complex skills, since the techniques used to collect evidence that is stored on the hard drive of a home computer and those employed to intercept a data- transmission process are significantly different. Especially when it comes to high level-offenders, investigators are often confronted with situations that call for quick decisions. One example is whether a running computer system should be turned off or not, and how this procedure should be carried out. To avoid interfering with the integrity of relevant digital evidence, a common instruction is to pull the plug, as this stops any alteration of files.[2056] However, such a disruption of energy can activate encryption[2057] and thereby hinder access to stored data.[2058] First responders, who undertake the first steps to collect digital evidence, bear a significant responsibility for the entire investigation process, as any wrong decision can have a major impact on the ability to preserve relevant evidence.[2059] If they make wrong decisions on preservation, important traces can be lost.

Forensic experts need to ensure that all relevant evidence is identified.[2060] This can be difficult if offenders hide files in a storage device in order to prevent law-enforcement agencies from analysing the content of the file. Forensic investigations can identify hidden files and make them accessible.[2061] Similar recovery processes are necessary if digital information has been deleted.[2062] Files that are deleted by simply placing them in a virtual trash bin does not necessarily render them unavailable to law-enforcement agencies, as they may be recovered using special forensic software tools.[2063] However, if offenders are using tools to ensure that files are securely deleted by overwriting the information, recovery is in general not possible.[2064] The collection of evidence can also face challenges if criminals are trying to prevent access to relevant information by using encryption technology. Such technology is more and more frequently used.[2065] Given that this prevents law-enforcement agencies from accessing and examining the encrypted information, the use of encryption technology entails significant challenges for law-enforcement agencies.[2066] Forensic experts can try to decrypt encrypted files.[2067] If this is not possible, they can support law-enforcement agencies in developing strategies to gain access to encrypted files, for example by using a keylogger.[2068]

Involvement in the collection of evidence includes the evaluation and implementation of new instruments. One example of a new approach is the debate on remote forensic tools.[2069] Remote forensic tools enable investigators to collect evidence remotely in real time[2070] or remotely monitor a suspect's activity[2071] without the suspect being aware of investigations on his system. Where such a tool is available, it can play a role in the development of a strategy to collect digital evidence.

### Communication with service providers

Internet service providers (ISPs) play an important role in many cybercrime investigations, since most users are utilizing their services to access the Internet or store websites. The fact that in some cases the ISPs have the technical capability to detect and prevent crimes and to support law-enforcement agencies in their investigations has prompted an intensive debate on the role of ISPs in cybercrime investigations. Obligations discussed range from the mandatory implementation of prevention technology to voluntary support of investigations.[2072] Forensic experts can also support an investigation by preparing requests that are submitted to service providers[2073] and assisting the investigators in producing adequate case histories[2074] which are necessary to prove the reliability of the collected evidence. Cooperation between law-enforcement agencies and ISPs in such investigations requires the application of certain procedures.[2075] The Council of Europe Guidelines for the Cooperation of Law Enforcement and ISPs[2076] contain a set of fundamental procedures, including issues such as providing explanations and assistance regarding investigation techniques[2077] and prioritization,[2078] and the assistance of forensic experts can be useful in this respect to improve the efficiency of procedures.

Close cooperation with ISPs is especially relevant in connection with the identification of a suspect. Suspects who commit cybercrime do leave traces.[2079] Traffic data analysis, like the examination of log-files kept by ISPs, can lead the investigators to the connection used by the offender to log on to the Internet.[2080] Offenders can try to hinder investigations by making use of anonymous communication technology.[2081] But even in this case, investigations are not impossible if investigators and ISPs cooperate closely.[2082] One example is the forensic tool CIPAV (Computer and Internet Protocol Address Verifier) that was used in the US to identify a suspect who had been using anonymous communication services.[2083] Another example of cooperation between ISPs and investigators is e-mail investigation. E-mails have become a very popular means of communication.[2084] To avoid identification, offenders sometimes use free e-mail addresses which they were able to register using fake personal information. However, even in this case, examination of header information[2085] and log-files of the e-mail provider will in some instances enable identification of the suspect.

The need to cooperate and communicate with providers is not limited to ISPs. Since some crimes such as phishing[2086] and the commercial distribution of child pornography include financial transactions, one strategy to identify the offender is to obtain data from financial institutions involved in the transactions.[2087] One example is an investigation in Germany where offenders who downloaded child pornography from a commercial website were identified on the basis of credit-card records. Based on a request from the investigators, the credit-card companies analysed their customer records to identify customers who used their credit card to purchase child pornography on the specific website.[2088] Such investigations are more challenging when anonymous payment methods are used.[2089]

### Examination of ICT

The first step in most investigations is to prove that the offender had the ability to commit the crime. One of the main tasks of forensic experts is the examination of seized hardware and software.[2090] Checks can either be performed on the spot during the search of the suspect's premises[2091] or after seizure. To enable such investigation, first responders usually seize all relevant storage devices – each of them potentially carrying millions of files that quite often pose a logistical challenge.[2092] As pointed out above, the principles of relevance and effectiveness are of great importance for the admissibility of digital evidence.[2093] Identifying and selecting the relevant hardware is therefore one of the major tasks within an investigation.[2094]

An analysis of available hardware components can, for example, prove that the suspect's computer was capable of carrying out a denial-of-service attack[2095] or is equipped with a chip that prevents manipulations of the operating system. Hardware analysis can also be necessary in the process of identifying a suspect. Some operating systems analyse the hardware configuration of a computer system during an installation process and submit it to the software producer. If the suspect's hardware profile can be detected based on information from the software company, hardware analysis can be helpful to verify that the seized computer system matches. Hardware analysis does not necessarily mean focusing on physical components attached to a computer system. Most operating systems keep logs of hardware that was attached to a computer system during an operation.[2096] Based on the entries in log files such as the Windows Registry, forensic examiners can even identify hardware that was used in the past but was not present during the search and seizure procedure.

In addition to hardware analysis, software analysis is a regular task in cybercrime investigations. Computer software is necessary to operate a computer system. In addition to the operating systems, additional software tools can be installed to gear the functioning of computer systems to the demand of the user. Forensic experts can analyse the functioning of software tools in order to prove that a suspect was capable of committing a specific crime. They can, for example, investigate whether the suspect's computer system contains a software that enables the encryption of data in pictures (steganography[2097]). An inventory of software tools installed on the suspect's computer can also help to design further investigation strategies. If, for example, the investigators find encryption software or tools used to delete files securely, they can specifically search for encrypted or deleted evidence.[2098] Investigators can also determine the functions of computer viruses or other forms of malicious software and reconstruct software-operation processes.[2099] In some cases, where illegal content has been found on suspects'

computers, the suspects have claimed that they did not download the files but that it must have been done by computer virus. In such cases, forensic investigations can try to identify malicious software installed on the computer system and determine its functions. Similar investigations can be carried out if a computer system could have been infected and turned into part of a botnet.[2100] Furthermore, software analysis can be important to determine if a software is produced solely for committing crimes or can be used for legitimate as well as illegal purposes (dual use). This differentiation can be relevant, insofar as some countries limit criminalization of the production of illegal devices to those that are either solely or primarily designed to commit crimes.[2101]

Data-related investigations are not confined to the software function, but also include analysis of non-executable files such as pdf-documents or video files. These investigations range from content analysis of specific files to automatic keyword search[2102] for text files and image search for known images on the suspect's computer.[2103] File analysis also includes the examination of digital documents that might have been forged[2104] as well as metadata investigation.[2105] Such analysis can determine the time[2106] the document was last opened or modified.[2107] Furthermore, metadata analysis can be used to identify the author of a file containing a threatening message, or the serial number of the camera that was used to produce a child-pornography image. Authors can also be identified based on linguistic analysis, which can assist in determining if the suspect has written articles before and left information that can help identification in this context.[2108]

#### Tracking and reporting

One of the greatest challenges related to digital evidence is the fact that it is highly fragile and can rather easily be deleted[2109] or modified.[2110] As pointed out above, one consequence of the fragility of digital evidence is the need to maintain its integrity.[2111] Case records are therefore required. The involvement of qualified experts [2112] in the production of case records is one approach to maintaining the integrity of evidence where forensic experts can be involved.[2113] But forensic experts also play a role when the seizure of hardware is either impossible or inadequate. In those cases, some countries enable investigators to copy files. Special attention then needs to be paid to protecting the integrity of copied files against any kind of alteration during the copy process.[2114]

#### Presentation of the evidence in court

The final phase of investigations is in general the presentation of evidence in court. While the presentation of evidence in court is customarily undertaken by the prosecution and defence lawyers, forensic experts can play an important role in criminal proceedings as expert witnesses who can help the people involved in the court proceedings to understand the processes by which the evidence was created, the procedures used to collect the evidence and evaluation of the evidence.[2115] Given the complexity of digital evidence, the need to involve forensic experts increases, which leads *de facto* to a reliance of judges, juries, prosecutors and lawyers on expert statements.[2116]

#### Forensic examination operations

Although computer forensics deals to a large degree with computer hardware and computer data, it is not necessarily always automated, and computer forensics remains to a large extent manual work.[2117] This is especially true with regard to the development of strategies and the search for possible evidence within search and seizure procedures. The amount of time necessary for such manual operations and the ability of offenders to automate their attacks underline the challenges that law-enforcement agencies face, especially in investigations involving a large number of suspects and large data volumes.[2118] However, some processes like the search for suspicious keywords or the recovery of deleted files can be automated using special forensic analysis tools.[2119]

### *6.5.3 Safeguards*

Over the last few years, law-enforcement agencies around the world have highlighted the urgent need for adequate investigation instruments.[2120] Taking this into consideration, it is perhaps surprising that the Council of Europe Convention on Cybercrime has been criticized with regard to procedural

instruments.[2121] The criticism focuses mainly on the aspect that the Convention on Cybercrime contains a number of provisions that establish investigation instruments (Articles 16-21) but only one provision (Article 15) that deals with safeguards.[2122] In addition, it can be noted that unlike for the substantive criminal law provisions in the Convention on Cybercrime, there are only very few possibilities for national adjustments in respect of the implementation of the Convention on Cybercrime.[2123] The criticism as such focuses mainly on the quantitative aspects. It is correct that the Convention on Cybercrime follows the concept of centralized regulation of safeguards instead of attaching them individually to each instrument. But this does not necessarily mean a weaker protection of suspects' rights.

The Council of Europe Convention on Cybercrime was designed from the outset as an international framework and instrument for the fight against cybercrime that is not limited solely to the Council of Europe member countries.[2124] While negotiating the necessary procedural instruments, the drafters of the Convention on Cybercrime, which included representatives from non-European countries like the United States and Japan, realized that the existing national approaches related to safeguards and especially the way these protected the suspect in the various criminal law systems were so different that it would not be possible to provide one detailed solution for all Member States.[2125] The drafters of the Convention on Cybercrime therefore decided not to include specific regulations in the text of the Convention, but instead to request Member States to ensure that fundamental national and international standards of safeguards are applied.[2126]

***Article 15 – Conditions and safeguards***

*1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.*

*2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.*

*3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.*

Article 15 is based on the principle that the signatory states shall apply the conditions and safeguards that already exist under domestic law. If the law provides central standards that apply to all investigation instruments, these principles shall apply to Internet-related instruments as well.[2127] In case the domestic law is not based on a centralized regulation of safeguards and conditions, it is necessary to analyse the safeguards and conditions implemented with regard to traditional instruments that are comparable to Internet-related instruments.

But the Convention on Cybercrime does not refer solely to existing safeguards in national legislation. This would have the drawback that the requirements for application would differ in such a way that the positive aspects of harmonization would no longer apply. To ensure that signatory states which might have differing legal traditions and safeguards in place implement certain standards[2128], the Council of Europe Convention on Cybercrime defines the minimum standards by referring to fundamental frameworks, such as the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights instruments.

As the Convention on Cybercrime can be signed and ratified also by countries that are not members of the Council of Europe[2129], it is important to highlight that not only the United Nations International Covenant on Civil and Political Rights but also the Council of Europe Convention for the Protection of Human Rights

and Fundamental Freedoms will be taken into consideration when evaluating the systems of safeguards in signatory states that are not members of the Council of Europe Convention on Cybercrime.

With regard to cybercrime investigation, one of the most relevant provisions in Article 15 of the Council of Europe Convention on Cybercrime is the reference to Article 8, paragraph 2 of the European Convention on Human Rights.

> ***Art. 8***
> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The European Court of Human Rights has undertaken efforts to define more precisely standards that govern electronic investigations and especially surveillance. Today, case law has become one of the most important sources for international standards in respect of investigations related to communication.[2130] The case law takes particularly into consideration the gravity of the interference of the investigation[2131], its purpose[2132] and its proportionality.[2133] Fundamental principles that can be extracted from case law are: the need for a sufficient legal basis for investigation instruments[2134], the requirement that the legal basis must be clear with regard to the subject[2135], competences of the law-enforcement agencies need to be foreseeable[2136] and surveillance of communication can only be justified in context of serious crimes.[2137]

In addition to this, Article 15 of the Council of Europe Convention on Cybercrime takes into account the principle of proportionality.[2138] This provision is especially relevant for signatory states that are not members of the Council of Europe. In cases where the existing national system of safeguards does not adequately protect suspects, it is mandatory for Member States to develop the necessary safeguards within the ratification and implementation process.

Finally, Article 15 paragraph 2 of the Council of Europe Convention on Cybercrime, explicitly refers to some of the most relevant safeguards,[2139] including supervision, grounds justifying application, and limitation of procedure with regard to scope and duration.

Unlike the fundamental principles described above, the safeguards mentioned here do not necessarily need to be implemented with regard to any instrument but only if appropriate in view of the nature of the procedure concerned. The decision as to when this is the case is left to the national legislatures.[2140]

An important aspect related to the system of safeguards provided by the Council of Europe Convention on Cybercrime is the fact that the ability of law-enforcement agencies to use the instruments in a flexible way on the one hand and the guarantee of effective safeguards on the other depends on the implementation of a graded system of safeguards. The Convention on Cybercrime does not explicitly hinder the parties from implementing the same safeguards (e.g. the requirement of a court order) for all instruments, but such an approach would influence the flexibility of the law-enforcement agencies. The ability to ensure an adequate protection of the suspect's rights within a graded system of safeguards depends largely on balancing the potential impact of an investigation instrument with the related safeguards. To achieve this it is necessary to differentiate between less and more intensive instruments. There are a number of examples of such differentiation in the Council of Europe Convention on Cybercrime that enable the parties to further develop a system of graded safeguards. These include the following: Differentiation between the interception of content data (Article 21)[2141] and the collection of traffic data (Article 20)[2142]. Unlike the collection of traffic data, the interception of content data is limited to serious crimes.[2143] Differentiation between the order for an expedited preservation of stored computer data (Article 16)[2144] and the submission of the preserved computer data based on the production order (Article 18).[2145] Article 16 only enables law enforcement agencies to order the preservation of data but not their disclosure.[2146] And finally, differentiation between the obligation to submit "subscriber information"[2147] and "computer data"[2148] in Article 18.[2149]

If the intensity of an investigation instrument and the potential impact on a suspect are correctly evaluated and the safeguards are designed in line with the results of the analysis, the system of graded safeguards does not lead to an unbalanced system of procedural instruments.

### 6.5.4 Expedited preservation and disclosure of stored computer data (Quick freeze procedure)

The identification of an offender who has committed a cybercrime often requires the analysis of traffic data.[2150] The IP address, in particular, can help law-enforcement agencies to trace the offender. As long as the law-enforcement agencies have access to the relevant traffic data, it is in some cases even possible to identify an offender who is using public Internet terminals that do not require identification.[2151]

One of the main difficulties that investigators face is that traffic data highly relevant for the information in question are often automatically deleted after a rather short period of time. The reason for this automatic deletion is the fact that, after the end of a process (e.g. the sending out of an e-mail, accessing the Internet or downloading a movie), the traffic data that were generated during the process and enabled the process to be carried out are no longer needed. From an economic point of view, most Internet providers are interested in deleting the information as soon as possible, since storing the data for longer periods would require even larger (expensive) storage capacity.[2152]

However, the economic aspects do not constitute the only reason why law-enforcement agencies need to carry out their investigations quickly. Some countries have strict laws that prohibit the storage of certain traffic data after the end of a process. One example of such restriction is Article 6 of the European Union's Directive on Privacy and Electronic Communication.[2153]

***Article 6 – Traffic data***
*1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).*
*2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.*

Time is therefore a critical aspect of Internet investigations. In general, since it is likely that some time will elapse between the perpetration of a crime, its discovery, and notification of the law-enforcement agencies, it is important to implement mechanisms that prevent relevant data from being deleted during the sometimes lengthy investigation process. In this regard, two different approaches are currently being discussed,[2154] namely data retention and data preservation ("quick freeze procedure").

A data-retention obligation forces the provider of Internet services to save traffic data for a certain period of time.[2155] In the latest legislative approaches, the records need to be saved for up to 24 months.[2156] This would enable law-enforcement agencies to obtain access to data that are necessary to identify an offender even months after perpetration of the crime.[2157] A data-retention obligation was recently adopted by the European Parliament[2158] and is currently also under discussion in the United States.[2159] With regard to the principles of data retention, more information can be found below.

#### Convention on Cybercrime

Data preservation is a different approach to ensuring that a cybercrime investigation does not fail just because traffic data were deleted during lengthy investigation proceedings.[2160] Based on data-preservation legislation, law-enforcement agencies can order a service provider to prevent the deletion of certain data. The expedited preservation of computer data is a tool that should enable law-enforcement agencies to react immediately and avoid the risk of deletion as a result of lengthy procedures.[2161] The drafters of the Council of Europe Convention on Cybercrime decided to focus on "data preservation" rather than "data retention".[2162] A regulation can be found in Article 16 of the Convention.

***Article 16 – Expedited preservation of stored computer data***
*1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.*
*2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.*
*3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.*
*4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.*

Seen from an Internet service provider's perspective, data preservation is a less constraining instrument compared to data retention.[2163] ISPs do not need to store all data for all users, but instead have to ensure that specific data are not deleted as soon as they receive an order from a competent authority. Data preservation offers advantages insofar as it covers data preservation not only from a provider's point of view but also from the data-protection perspective. It is not necessary to preserve the data from millions of Internet users but only data that are related to possible suspects in criminal investigations. Nevertheless, it is important to point out that data retention offers advantages in cases where data are deleted immediately after a crime is perpetrated. In such cases, the data-preservation order would, unlike a data-retention obligation, not be able to prevent the deletion of the relevant data.

The order pursuant to Article 16 only obliges the provider to save data that were processed by the provider and not deleted at the time the provider receives the order.[2164] It is not limited to traffic data, as traffic data is just mentioned as one example. Article 16 does not force the provider to start collecting information it would not normally store.[2165] In addition, Article 16 does not oblige the provider to transfer the relevant data to the authorities. The provision only authorizes law-enforcement agencies to prevent the deletion of the relevant data but not to pledge the providers to transfer the data. The transfer obligation is regulated in Articles 17 and 18 of the Council of Europe Convention on Cybercrime. The advantage of a separation of the obligation to preserve the data and the obligation to disclose them is the fact that it is possible to require different conditions for application of the two obligations.[2166] In view of the importance of immediate reaction, it would for example be supportive to waive the requirement for an order by a judge and enable the prosecution or police to order the preservation.[2167] This would enable the competent authorities to react faster. Protection of the suspect's rights can then be achieved by requiring a judge's order for the disclosure of the data.[2168]

The disclosure of the preserved data is among other aspects regulated in Article 18 of the Council of Europe Convention on Cybercrime:

***Article 18 – Production order***
*1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:*
*a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and*
*b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.*
*2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.*

*3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:*

*a. the type of communication service used, the technical provisions taken thereto and the period of service;*

*b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;*

*c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.*

Based on Article 18 paragraph 1.a of the Council of Europe Convention on Cybercrime, the providers that have preserved the data can be obliged to disclose the data.

Article 18 of the Convention on Cybercrime is not only applicable after a preservation order pursuant to Article 16 of the Convention has been issued.[2169] The provision is a general instrument that law-enforcement agencies can make use of. If the receiver of the production order voluntarily transfers the requested data, law-enforcement agencies are not restricted to seizing the hardware, but can apply the less constraining production order. Compared to the actual seizure of hardware, the order to submit the relevant information is in general less constraining. Its application is therefore especially relevant in cases where forensic investigations do not require access to the hardware.

In addition to the obligation to submit computer data, Article 18 of the Council of Europe Convention on Cybercrime enables law-enforcement agencies to order the submission of subscriber information. This investigation instrument is of great importance in IP-based investigations. If the law-enforcement agencies are able to identify an IP-address that was used by the offender while carrying out the offence, they will need to identify the person[2170] who used the IP-address at the time of the offence. Based on Article 18, paragraph 1.b of the Convention on Cybercrime, a provider is obliged to submit the subscriber information listed in Article 18, paragraph 3.[2171]

In cases where the law-enforcement agencies trace back the route to an offender and need immediate access to identify the path through which the communication was transmitted, Article 17 enables them to order the expedited partial disclosure of traffic data.

***Article 17 – Expedited preservation and partial disclosure of traffic data***

*1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:*

*a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and*

*b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.*

*2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.*

As mentioned above, the Convention on Cybercrime strictly separates the obligation to preserve data on request and the obligation to disclose them to the competent authorities.[2172] Article 17 provides a clear classification, as it combines the obligation to ensure the preservation of traffic data in cases where a number of service providers were involved with the obligation to disclose the necessary information to identify the transmission path. Without such partial disclosure, law-enforcement agencies would in some cases not be able to trace back the offender if more than one provider was involved.[2173] Due to the combination of the two obligations, which affect the rights of suspects in different ways, it is necessary to discuss the focus of the safeguards related to this instrument.

### Commonwealth Computer and Computer-related Crimes Model Law

Similar approaches can be found in the 2002 Commonwealth Model Law.[2174]

**The provision**

***Production of data***

***15*** *If a magistrate is satisfied on the basis of an application by a police officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that:*

*(a) a person in the territory of [enacting country] in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; and*

*(b) an Internet service provider in [enacting country] produce information about persons who subscribe to or otherwise use the service; and*

*(c)*[2175] *a person in the territory of [enacting country] who has access to a specified computer system process and compile specified computer data from the system and give it to a specified person.*

***Disclosure of stored traffic data***

***16.***[2176] *If a police officer is satisfied that data stored in a computer system is reasonably required for the purposes of a criminal investigation, the police officer may, by written notice given to a person in control of the computer system, require the person to disclose sufficient traffic data about a specified communication to identify:*

*(a) the service providers; and*

*(b) the path through which the communication was transmitted.*

***Preservation of data***

*17. (1) If a police officer is satisfied that:*

*(a) data stored in a computer system is reasonably required for the purposes of a criminal investigation; and*

*(b) there is a risk that the data may be destroyed or rendered inaccessible;*

*the police officer may, by written notice given to a person in control of the computer system, require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days as specified in the notice.*

*(2) The period may be extended beyond 7 days if, on an ex parte application, a [judge] [magistrate] authorizes an extension for a further specified period of time.*

### 6.5.5 Data retention

A data-retention obligation forces the provider of Internet services to save traffic data for a certain period of time.[2177] The implementation of a data retention obligation is an approach to avoid the above-mentioned difficulties of gaining access to traffic data before they are deleted. An example for such an approach is the European Union Directive on Data Retention.[2178]

***Article 3 – Obligation to retain data***

*1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.*

*2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.*

***Article 4 – Access to data***

*Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.*

***Article 5 – Categories of data to be retained***

*1. Member States shall ensure that the following categories of data are retained under this Directive:*

*(a) data necessary to trace and identify the source of a communication:*

*(1) concerning fixed network telephony and mobile telephony:*

*(i) the calling telephone number;*

*(ii) the name and address of the subscriber or registered user;*

*(2) concerning Internet access, Internet e-mail and Internet telephony:*

*(i) the user ID(s) allocated;*

*(ii) the user ID and telephone number allocated to any communication entering the public telephone network;*

*(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;*

*(b) data necessary to identify the destination of a communication:*

*(1) concerning fixed network telephony and mobile telephony:*

*(i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;*

*(ii) the name(s) and address(es) of the subscriber(s) or registered user(s);*

*(2) concerning Internet e-mail and Internet telephony:*

*(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;*

*(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;*

*(c) data necessary to identify the date, time and duration of a communication:*

*(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;*

*(2) concerning Internet access, Internet e-mail and Internet telephony:*

*(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;*

*(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;*

*(d) data necessary to identify the type of communication:*

*(1) concerning fixed network telephony and mobile telephony: the telephone service used;*

*(2) concerning Internet e-mail and Internet telephony: the Internet service used;*

*(e) data necessary to identify users' communication equipment or what purports to be their equipment:*

*(1) concerning fixed network telephony, the calling and called telephone numbers;*

*(2) concerning mobile telephony:*

*(i) the calling and called telephone numbers;*

*(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;*

*(iii) the International Mobile Equipment Identity (IMEI) of the calling party;*

*(iv) the IMSI of the called party;*

*(v) the IMEI of the called party;*

*(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;*

*(3) concerning Internet access, Internet e-mail and Internet telephony:*
*(i) the calling telephone number for dial-up access;*
*(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;*
*(f) data necessary to identify the location of mobile communication equipment:*
*(1) the location label (Cell ID) at the start of the communication;*
*(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.*
*2. No data revealing the content of the communication may be retained pursuant to this Directive.*
***Article 6 – Periods of retention***
*Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.*
***Article 7 – Data protection and data security***
*Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:*
*(a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network;*
*(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;*
*(c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only; and*
*(d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.*
***Article 8 – Storage requirements for retained data***
*Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.*

The fact that key information about any communication on the Internet will be covered by the Directive has prompted intense criticism from human rights organizations.[2179] This could in turn lead to a review of the Directive and its implementation by constitutional courts.[2180] In addition, in her conclusion in the case Productores de Música de España (Promusicae) v. Telefónica de España,[2181] the adviser to the European Court of Justice, Advocate General Juliane Kokott, pointed out that it is questionable whether the data-retention obligation can be implemented without a violation of fundamental rights.[2182] Difficulties with regard to the implementation of such regulations were already pointed out by the G8 in 2001.[2183]

But the criticism is not limited to this aspect. Another reason why data retention has turned out to be less effective in the fight against cybercrime is the fact that the obligations can be circumvented. The easiest ways to circumvent the data retention obligation include the use of different public Internet terminals or prepaid mobile phone data services that do not require registration[2184] and the use of anonymous communication services that are (at least partially) operated in countries where the data-retention obligation is not applied.[2185]

If offenders use different public terminals or prepaid mobile phone data services where they do not need to register the data stored by the providers, the data-retention obligation will only lead the law-enforcement agencies to the service provider but not to the actual offender.[2186]

Offenders can in addition circumvent the data-retention obligation by using anonymous communication servers.[2187] In this case, law-enforcement agencies might be able to prove the fact that the offender used an anonymous communication server, but, having no access to traffic data in the country where the anonymous communication server is located, they will not be able to prove the participation of the offender in the perpetration of a criminal offence.[2188]

Given that it is very easy to circumvent the provision, the implementation of the data-retention legislation in the European Union is coupled with the fear that the process will require side-measures necessary to ensure the effectiveness of the instrument. Possible side-measures could include the obligation to register prior to the use of online services[2189] or a ban on the use of anonymous communication technology.[2190]

### 6.5.6 Search and seizure

Although new investigation instruments like real-time collection of content data and the use of remote forensic software to identify an offender are under discussion and already implemented by some countries, search and seizure remains one of the most important investigation instruments.[2191] As soon as the offender is identified and law enforcement seizes his IT equipment, the computer forensic experts can analyse the equipment to collect the evidence necessary for the prosecution.[2192]

The possibility of replacing or amending the search and seizure procedure is currently being discussed in some European countries and in the United States.[2193] One way to avoid the need to enter the suspect's house to search and seize computer equipment would be to perform an online search. This instrument, which will be described more in detail in sections below, describes a procedure where law-enforcement agencies access the suspect's computer via the Internet to perform secret search procedures.[2194] Although law-enforcement agencies could clearly benefit from the fact that the suspect does not realize that the investigation is being carried out, physical access to the hardware enables more efficient investigation techniques.[2195] This underlines the important role of search and seizure procedures within Internet investigation.

#### Council of Europe Convention on Cybercrime

Most national criminal procedural laws contain provisions that enable law-enforcement agencies to search and seize objects.[2196] The reason why the drafters of the Council of Europe Convention on Cybercrime nevertheless included a provision dealing with search and seizure is that national laws often do not cover data-related search and seizure procedures.[2197] Some countries, for example, limit the application of seizure procedures to seizing physical objects.[2198] Based on such provisions, investigators are able to seize an entire server but not seize only the relevant data by copying them from the server. This can cause difficulties in cases where the relevant information is stored on a server together with the data of hundreds of other users, which would no longer be available after the law-enforcement agencies have seized that server. Another example where traditional search and seizure of tangible items is not sufficient is the case where the law-enforcement agencies do not know the physical location of the server but are able to access it via the Internet.[2199] Article 19, like other procedural instruments provided by the Convention on Cybercrime, does not specify the conditions and requirements that must be fulfilled for investigators to carry out such investigations. The provision itself neither states that a court order is necessary nor defines under what circumstances an exception to the requirement of a court order can be made. Taking into account the intrusion into the suspect's civil liberties and rights that search and seizure procedures[2200] entail, most countries limit the applicability of the instrument.[2201]

Article 19 paragraph 1 of the Council of Europe Convention on Cybercrime aims to establish an instrument that enables the search of computer systems which is as efficient as traditional search procedures.[2202]

> ***Article 19 – Search and seizure of stored computer data***
> *1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:*
> *a. a computer system or part of it and computer data stored therein; and*
> *b. a computer-data storage medium in which computer data may be stored in its territory.*
> *[…]*

Although the search and seizure procedure is an instrument that is frequently used by investigators, there are a number of challenges that accompany its application in cybercrime investigations.[2203] One of the main difficulties is that search orders are often limited to certain places (e.g. the home of the suspect).[2204]

With regard to the search for computer data it can turn out during the investigation that the suspect did not store them on local hard drives but on an external server that was accessed via the Internet.[2205] Using Internet servers to store data and process data is becoming increasingly popular amongst Internet users ("cloud computing"). One of the advantages of storing information on an Internet server is that the information can be accessed from any place with an Internet connection. To ensure that investigations can be carried out efficiently, it is important to maintain a certain flexibility in investigations. If the investigators discover that relevant information is stored on another computer system, they should be able to extend the search to that system.[2206] The Council of Europe Convention on Cybercrime addresses this issue in Article 19 paragraph 2.

***Article 19 – Search and seizure of stored computer data***
*[…]*
*2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.*
*[…]*

Another challenge is related to the seizure of computer data. If the investigators come to the conclusion that the seizure of the hardware that is used to store the information is not necessary or would not be adequate, they may still need other instruments that enable them to continue the search and seizure procedure with regard to the stored computer data.[2207] The necessary instruments are not limited to the act of copying the relevant data.[2208] In addition, there are a number of side-measures that are necessary to maintain required efficiency, such as the seizure of the computer system itself. The most important aspect is maintaining the integrity of the copied data.[2209] If the investigators do not have permission to take the necessary measures to ensure the integrity of the copied data, the copied data may not be accepted as evidence in criminal proceedings.[2210] After the investigators have copied the data and taken measures to maintain its integrity, they will need to decide how to treat the original data. Since investigators will not remove the hardware during the seizure process, the information would in general remain there. Especially in investigations related to illegal content[2211] (e.g. child pornography), the investigators will not be able to leave the data on the server. Therefore, they need an instrument that allows them to remove the data or at least ensure that the data can no longer be accessed.[2212] The Council of Europe Convention on Cybercrime addresses the above mentioned issues in Article 19 paragraph 3.

***Article 19 – Search and seizure of stored computer data***
*[…]*
*3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:*
*a. seize or similarly secure a computer system or part of it or a computer-data storage medium;*
*b. make and retain a copy of those computer data;*
*c. maintain the integrity of the relevant stored computer data;*
*d. render inaccessible or remove those computer data in the accessed computer system.*
*[…]*

One more challenge regarding search orders pertaining to computer data is the fact that it is sometimes difficult for law-enforcement agencies to find the location of the data. Often they are stored in computer systems outside the specific national territory. Even when the exact location is known, the amount of stored data often hinders expedited investigations.[2213] In these cases, the investigations present unique difficulties, insofar as they have an international dimension that requires international cooperation within the investigations.[2214] Even when the investigations are related to computer systems located within the

national borders, and the investigators have identified the hosting provider that operates the servers where the offender has stored the relevant data, the investigators might face difficulties in identifying the exact location of the data. It is very likely that even small and medium-sized hosting providers have hundreds of servers and thousands of hard disks. Very often the investigators will not be able to identify the exact location with the help of the system administrator responsible for the server infrastructure.[2215] But even when they are able to identify the specific hard drive, protection measures might stop them from searching for the relevant data. The drafters of the Convention on Cybercrime decided to address this issue by implementing a coercive measure to facilitate the search and seizure of computer data. Article 19 paragraph 4 enables the investigators to compel a system administrator to assist law-enforcement agencies. Although the obligation to follow the orders of the investigator is limited to necessary information and support for the case, this instrument changes the nature of search and seizure procedures. In many countries, search and seizure orders only force the people affected by the investigation to tolerate the proceedings – they do not need to actively support the investigation. With regard to a person who has special knowledge that is needed by the investigators, implementation of the Council of Europe Convention on Cybercrime will change the situation in two ways. First of all they will need to provide the necessary information to the investigators. The second change is related to this obligation. The obligation to provide – reasonable – support to the investigators will relieve the person with special knowledge from contractual obligations or orders given by supervisors.[2216] The Convention on Cybercrime does not define the term "reasonable", but the Explanatory Report points out that reasonable *"may include disclosing a password or other security measure to the investigating authorities"* but does in general not cover *"the disclosure of the password or other security measure"* where this would go along with *"unreasonably threaten the privacy of other users or other data that is not authorised to be searched".*[2217]

***Article 19 – Search and seizure of stored computer data***
*[…]*
*4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.*
*[…]*

### Commonwealth Computer and Computer-related Crimes Model Law

A similar approach can be found in the 2002 Commonwealth Model Law.[2218]

***Definitions for this Part***
***11.*** *In this Part:*
*[...]*
*"seize" includes:*
*(a) make and retain a copy of computer data, including by using onsite equipment; and*
*(b) render inaccessible, or remove, computer data in the accessed computer system; and*
*(c) take a printout of output of computer data.*
*[…]*

***Search and seizure warrants***
***12***[2219]***.*** *(1) If a magistrate is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds [to suspect] [to believe] that there may be in a place a thing or computer data:*
*(a) that may be material as evidence in proving an offence; or*
*(b) that has been acquired by a person as a result of an offence;*
*the magistrate [may] [shall] issue a warrant authorising a [law enforcement] [police] officer, with such assistance as may be necessary, to enter the place to search and seize the thing or computer data.*
*[…]*

***Assisting Police***

***13***[2220]*.(1) A person who is in possession or control of a computer data storage medium or computer system that is the subject of a search under section 12 must permit, and assist if required, the person making the search to:*

*(a) access and use a computer system or computer data storage medium to search any computer data available to or in the system; and*

*(b) obtain and copy that computer data; and*

*(c) use equipment to make copies; and*

*(d) obtain an intelligible output from a computer system in a plain text format that can be read by a person.*

*(2) A person who fails without lawful excuse or justification to permit or assist a person commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*

### 6.5.7 Production order

Even if an obligation like the one in Article 19 paragraph 4 of the Council of Europe Convention on Cybercrime is not implemented in national law, providers will often cooperate with law-enforcement agencies to avoid a negative impact on their business. If – due to a lack of cooperation of the provider – investigators are unable to find the data or the storage devices they need to search and seize, it is likely that the investigators will need to seize more hardware than actually necessary. Therefore, providers will in general support investigations and provide the relevant data on request of the law-enforcement agencies. The Council of Europe Convention on Cybercrime contains instruments that allow investigators to do without search orders if the person who is in possession of relevant data submits them to the investigators.[2221]

Although the joint efforts of law-enforcement agencies and service providers even in cases where there is no legal basis seem to be a positive example of public-private partnership, there are a number of difficulties with unregulated cooperation. In addition to data-protection issues, the main concern is that service providers could violate their contractual obligations with their customers if they follow a request to submit certain data that is not founded on a sufficient legal basis.[2222]

***Article 18 – Production order***

*1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:*

*a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and*

*b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.*

Article 18 contains two obligations. Based on Article 18 paragraph 1.a, any person (including service provider) is obliged to submit specified computer data that are in the person's possession or control. Unlike Subparagraph 1b), the application of the provision is not limited to specific data. The term "possession" requires that the person have physical access to the data storage devices where the specified information is stored.[2223] The application of the provision is extended by the term "control". Data are under control of a person if he/she has no physical access but is managing the information. This is, for example, the case if the suspect has stored relevant data on a remote online storage system. In the Explanatory Report, the drafters of the Convention on Cybercrime nevertheless point out that the mere technical ability to remotely access stored data does not necessary constitute control.[2224] The application of Article 18 of the Council of Europe Convention on Cybercrime is therefore limited to cases where the degree of control of the suspect goes beyond the potential possibility to access the data.

Subparagraph 1b) contains a production order that is limited to certain data. Based on Article 18 Subparagraph 1b), investigators can order a service provider to submit subscriber information. Subscriber

information can be necessary to identify an offender. If the investigators are able to discover the IP address that was used by the offender, they need to link this number to a person.[2225] In most cases, the IP address only leads to the Internet provider that provided the IP address to the user. Before enabling the use of a service, Internet providers generally require a user to register with his subscriber information.[2226] Article 18 paragraph 1.b permits investigators to order the provider to submit this subscriber information. In this context, it is important to highlight that Article 18 of the Council of Europe Convention on Cybercrime does not, however, impose either a data-retention obligation[2227] or an obligation for service providers to register subscriber information.[2228]

The differentiation between "computer data" in Subparagraph 1a) and "subscriber information" in Subparagraph 1b) seems at first sight not to be necessary, insofar as subscriber information that is stored in digital form is also covered by Subparagraph 1a). The first reason for the differentiation stems from the different definitions of "computer data" and "subscriber information". Unlike "computer data", the term "subscriber information" does not require that the information be stored as computer data. Article 18 Subparagraph 1b) of the Council of Europe Convention on Cybercrime enables the competent law authorities to submit information that is kept in non-digital form.[2229]

***Article 1 – Definitions***
*For the purposes of this Convention:*

*[…]*
*b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;*

***Article 18 – Production order***

*[…]*
*3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:*
*a. the type of communication service used, the technical provisions taken thereto and the period of service;*
*b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;*
*c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.*

The second reason for the distinction between "computer data" and "subscriber information" is that it enables law-makers to implement different requirements with regard to the application of the instruments.[2230] It is for example possible to impose stricter requirements[2231] for a production order under Subparagraph 1b), as this instrument allows law-enforcement agencies to get access to any kind of computer data, including content data.[2232] The differentiation between the real-time collection of traffic data (Article 20)[2233] and the real-time collection of content data (Article 21)[2234] shows that the drafters of the Convention on Cybercrime realized that, depending on the kind of data law-enforcement agencies get access to, different safeguards need to be implemented.[2235] With the differentiation between "computer data" and "subscriber information", Article 18 of the Council of Europe Convention on Cybercrime enables the signatory states to develop a similar system of graded safeguards with regard to the production order.[2236]

### Commonwealth Computer and Computer-related Crimes Model Law

A similar approach can be found in the 2002 Commonwealth Model Law.[2237]

***Production of data***

***15.*** *If a magistrate is satisfied on the basis of an application by a police officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that:*

*(a) a person in the territory of [enacting country] in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; and*

*(b) an Internet service provider in [enacting country] produce information about persons who subscribe to or otherwise use the service; and*

*(c)*[2238] *a person in the territory of [enacting country] who has access to a specified computer system process and compile specified computer data from the system and give it to a specified person.*

### 6.5.8 Real-time collection of data

Telephone surveillance is an instrument that is used in capital crime investigations in many countries.[2239] Many offences involve the use of a phone – especially mobile phones – either in the preparation or the execution of the offence. Especially in cases involving drug trafficking, surveillance of conversations between perpetrators can be essential for the success of the investigation. The instrument allows investigators to collect valuable information, although it is limited to information exchanged over the observed lines/phones. If the offender uses other means of exchange (e.g. letters) or lines that are not included in the observation, the investigators will not be able to record the conversation. In general, the situation is the same when it comes to direct conversation without the use of phones.[2240]

Today, the exchange of data has replaced conventional phone conversations. The exchange of data is not limited to e-mails and file-transfers. An increasing amount of voice communication is performed using technology based on Internet protocols (voice-over-IP).[2241] Seen from a technical point of view, a voice-over-IP phone call is much more comparable to the exchange of e-mails than to a conventional phone call using the telephone wire, and the interception of this type of call presents unique difficulties. [2242]

Since many computer crimes involve the exchange of data, the ability to also intercept these processes or otherwise use data related to the exchange process can become an essential requirement for successful investigations. The application of existing telephone surveillance provisions and provisions related to the use of telecommunication traffic data in cybercrime investigations has turned out to be difficult in some countries. The difficulties encountered are related to technical issues[2243] as well as legal issues. From a legal point of view, authorization to record a telephone conversation does not necessarily include authorization to intercept data-transfer processes.

The Council of Europe Convention on Cybercrime aims to close existing gaps in the ability of law-enforcement agencies to monitor data-transfer processes.[2244] Within this approach, the Convention on Cybercrime distinguishes between two subsets of data-transfer observation. Article 20 authorizes investigators to collect traffic data. The term “traffic data” is defined in Article 1.d of the Convention.

***Article 1 – Definitions***

*[…]*

*d. “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.*

The distinction between “content data” and “traffic data” is the same as the differentiation used in most related national laws.[2245]

### 6.5.9 Collection of traffic data

#### Council of Europe Convention on Cybercrime

Bearing in mind that the definition of traffic data varies from country to country,[2246] the drafters of the Council of Europe Convention on Cybercrime decided to define this term in order to improve the application of the related provision in international investigations. The term "traffic data" is used to describe data that are generated by computers during the communication process in order to route a communication from its origin to its destination. Whenever a user connects to the Internet, downloads e-mails or opens a website, traffic data is generated. For cybercrime investigations, the most relevant origin and destination traffic data are IP addresses that identify the communication partners in Internet-related communication.[2247]

Unlike "content data", the term "traffic data" covers only data produced within data-transfer processes, but not the transferred data themselves. Although access to the content data might be necessary in some cases as it enables law-enforcement agencies to analyse the communication much more effectively, traffic data plays an important role in cybercrime investigation.[2248] While access to content data enables law-enforcement agencies to analyse the nature of the messages or files exchanged, traffic data can be necessary to identify an offender. In child-pornography cases, traffic data can for example enable the investigators to identify a webpage where the offender is uploading child-pornography images. By monitoring the traffic data generated during the use of Internet services, law-enforcement agencies are able to identify the IP address of the server and can then try to determine its physical location.

***Article 20 – Real-time collection of traffic data***

*1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:*

*a. collect or record through the application of technical means on the territory of that Party, and*

*b. compel a service provider, within its existing technical capability:*

*i. to collect or record through the application of technical means on the territory of that Party; or*

*ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.*

*2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.*

*3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.*

*4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.*

Article 20 contains two different approaches for the collection of traffic data, both of which are supposed to be implemented.[2249]

The first approach is to impose an obligation on Internet service providers to enable law-enforcement agencies to collect the relevant data directly. This generally requires the installation of an interface which law-enforcement agencies can use to access the Internet service provider's infrastructure.[2250]

The second approach is to enable law-enforcement agencies to compel an Internet service provider to collect data at their request. This approach enables investigators to make use of existing technical capacities and the knowledge the providers in general have at hand. One of the intentions behind combining the two approaches is to ensure that if providers do not have the technology in place to record the data, law-enforcement agencies should be able to carry out the investigation (based on Article 20 paragraph 1.b) without the assistance of the provider.[2251]

The Council of Europe Convention on Cybercrime is neither drafted with preference to a specific technology nor intended to set standards that result in the need for high financial investments for the industry involved.[2252] From that perspective, Article 20 paragraph 1.a of the Convention on Cybercrime seems to be the better solution. However, the regulation in Article 20 paragraph 2 shows that the drafters of the Convention on Cybercrime were aware that some countries might have difficulties in implementing legislation that enables law-enforcement agencies to carry out the investigations directly.

One of the major difficulties in investigations based on Article 20 is the use of means of anonymous communication. As explained above,[2253] offenders can use services in the Internet that enable anonymous communication. If the offender is using an anonymous communication service like the software Tor,[2254] investigators are in most cases unable to analyse the traffic data and identify the communication partners successfully. Offenders can achieve a similar result by using public Internet terminals.[2255]

Compared to traditional search and seizure procedures, one of the advantages of the collection of traffic data is that the suspect of a crime does not necessary realize that an investigation is taking place.[2256] This limits his/her possibilities to manipulate or delete evidence. To ensure that offenders are not informed by the service provider about the ongoing investigation, Article 20 paragraph 3 addresses this issue and obliges the signatory states to implement legislation that ensures that service providers keep knowledge of the ongoing investigation confidential. For the service provider, this is coupled with the advantage that the provider is relieved from the obligation[2257] to inform the users.[2258]

The Council of Europe Convention on Cybercrime was designed to improve and harmonize legislation with regard to cybercrime-related issues.[2259] In this context, it is important to highlight that based on the text in Article 21 thereof, the provision does not only apply to cybercrime-related offences, but to any offence. Given that the use of electronic communication can be relevant not only in cybercrime cases, the application of this provision outside of cybercrime offences can be useful within investigations. This would, for example, enable law-enforcement agencies to use traffic data that are generated during the exchange of e-mails between offenders for the preparation of a traditional crime. Article 14 paragraph 3 gives the parties the right to make reservations and limit the application of the provision to certain offences.[2260]

#### Commonwealth Computer and Computer-related Crimes Model Law

A similar approach can be found in the 2002 Commonwealth Model Law.[2261]

***Interception of traffic data***
*19. (1) If a police officer is satisfied that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the police officer may, by written notice given to a person in control of such data, request that person to:*

*(a) collect or record traffic data associated with a specified communication during a specified period; and*

*(b) permit and assist a specified police officer to collect or record that data.*

*(2) If a magistrate is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds [to suspect] that traffic data is reasonably required for the purposes of a criminal investigation, the magistrate [may] [shall] authorize a police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.*

### 6.5.10 Interception of content data

#### Council of Europe Convention on Cybercrime

Apart from the fact that Article 21 deals with content data, the structure is similar to Article 20. The possibility to intercept data-exchange processes can be important in cases where law-enforcement agencies already know who the communication partners are but have no information about the type of information exchanged. Article 21 gives them the possibility to record data communication and analyse

the content.[2262] This includes files downloaded from websites or file-sharing systems, e-mails sent or received by the offender and chat conversations.

***Article 21 – Interception of content data***

*1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:*

*a. collect or record through the application of technical means on the territory of that Party, and*

*b. compel a service provider, within its existing technical capability:*

*i. to collect or record through the application of technical means on the territory of that Party, or*

*ii. to co-operate and assist the competent authorities in the collection or recording of,*

*content data, in real-time, of specified communications in its territory transmitted by means of a computer system.*

*2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.*

*3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.*

*4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.*

Unlike in the case of traffic data, the Council of Europe Convention on Cybercrime does not provide a definition of content data. As is implicit in the term itself, "content data" refers to the content of the communication.

Examples of content data in cybercrime investigations include:

- the subject of an e-mail;
- content on a website opened by the suspect;
- the content of a VoIP conversation.

One of the most important difficulties for investigations based on Article 21 is the use of encryption technology.[2263] As explained in detail previously, the use of encryption technology can enable offenders to protect the content exchanged in a way that makes it impossible for law-enforcement agencies to gain access to it. If the offender encrypts the content he/she transfers, law-enforcement agencies are only able to intercept the encrypted communication but not analyse the content. Without access to the key that was used to encrypt the files, any possible decryption could take a very long time.[2264]

### Commonwealth Computer and Computer-related Crimes Model Law

A similar approach can be found in the 2002 Commonwealth Model Law.[2265]

***Interception of electronic communications***

*18. (1) If a [magistrate] [judge] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds [to suspect][to believe] that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the magistrate [may] [shall]:*

*(a) order an Internet service provider whose service is available in [enacting country] through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or*

*(b) authorize a police officer to collect or record that data through application of technical means.*

### 6.5.11 Regulation regarding encryption technology

As described above, offenders can also hinder content-data analysis by using encryption technology. Various software products are available that enable users to effectively protect files as well as data-transfer processes against unauthorized access.[2266] If suspects have used such a product and the investigation authorities do not have access to the key that was used to encrypt the files, the required decryption could take a long time.[2267]

The use of encryption technology by offenders is a challenge for law-enforcement agencies.[2268] There are various national and international approaches[2269] to address the problem.[2270] Owing to differing estimates of the threat of encryption technology, there is as yet no widely accepted international approach to address the topic.

One approach is to authorize law-enforcement agencies to break encryption if necessary.[2271] Without such authorization, or the possibility of issuing a production order, investigation authorities could be unable to collect the necessary evidence. In addition, or as an option, investigators can be authorized to use keylogger software to intercept a passphrase to an encrypted file in order to break an encryption.[2272]

Another approach is to limit the performance of encryption software by restricting key length.[2273] Depending on the degree of the limitation, this would enable investigators to break keys within a reasonable period of time. Opponents of such a solution fear that the limitations would not only enable investigators to break encryption, but also economic spies trying to obtain access to encrypted business information.[2274] In addition, the restriction would only stop offenders using a stronger encryption if such software tools are available. This would first of all require international standards to prevent producers of strong encryption products from offering their software in countries without proper restrictions on key length. In any event, offenders could relatively easily develop their own encryption software with no limit on key length.

The obligation to establish a key escrow system or key recovery procedure for strong encryption products is another approach.[2275] Implementing such regulations would enable users to continue to use strong encryption technology but enable investigators to gain access to the relevant data by forcing the user to submit the key to a special authority which holds the key and provides it to investigators if necessary.[2276] Opponents of such a solution fear that people could obtain access to the submitted keys and with them decrypt secret information. In addition, offenders could relatively easily circumvent the regulation by developing their own encryption software that does not require the submission of the key to the authority.

Lastly, countries try to address the challenge by implementing a production order.[2277] This term describes the obligation to disclose a key used to encrypt data. The implementation of such an instrument was discussed within the 1997 G8 Meeting in Denver.[2278] A number of countries have implemented such obligations.[2279] An example of national implementation is section 69 of India's Information Technology Act 2000.[2280] Another example of such an obligation is section 49 of the United Kingdom Regulation of Investigatory Powers Act 2000:[2281]

***Notices requiring disclosure***

***49****.(1) This section applies where any protected information -*

*(a) has come into the possession of any person by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so;*

*(b) has come into the possession of any person by means of the exercise of any statutory power to intercept communications, or is likely to do so;*

*(c) has come into the possession of any person by means of the exercise of any power conferred by an authorisation under section 22(3) or under Part II, or as a result of the giving of a notice under section 22(4), or is likely to do so;*

*(d) has come into the possession of any person as a result of having been provided or disclosed in pursuance of any statutory duty (whether or not one arising as a result of a request for information), or is likely to do so; or*

*(e) has, by any other lawful means not involving the exercise of statutory powers, come into the possession of any of the intelligence services, the police or the customs and excise, or is likely so to come into the possession of any of those services, the police or the customs and excise.*

*(2) If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds-*

*(a) that a key to the protected information is in the possession of any person,*

*(b) that the imposition of a disclosure requirement in respect of the protected information is –*

*(i) necessary on grounds falling within subsection (3), or*

*(ii) necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty,*

*(c) that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and*

*(d) that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section,*

*the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information.*

*(3) A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary-*

*(a) in the interests of national security;*

*(b) for the purpose of preventing or detecting crime; or*

*(c) in the interests of the economic well-being of the United Kingdom.*

*(4) A notice under this section imposing a disclosure requirement in respect of any protected information-*

*(a) must be given in writing or (if not in writing) must be given in a manner that produces a record of its having been given;*

*(b) must describe the protected information to which the notice relates;*

*(c) must specify the matters falling within subsection (2)(b)(i) or (ii) by reference to which the notice is given;*

*(d) must specify the office, rank or position held by the person giving it;*

*(e) must specify the office, rank or position of the person who for the purposes of Schedule 2 granted permission for the giving of the notice or (if the person giving the notice was entitled to give it without another person's permission) must set out the circumstances in which that entitlement arose;*

*(f) must specify the time by which the notice is to be complied with; and*

*(g) must set out the disclosure that is required by the notice and the form and manner in which it is to be made;*

*and the time specified for the purposes of paragraph (f) must allow a period for compliance which is reasonable in all the circumstances.*

To ensure that the person obliged to disclose the key follows the order and actually submits the key, the United Kingdom Investigatory Powers Act 2000 contains a provision that criminalized failure to comply with the order.

***Failure to comply with a notice.***

***53****(1) A person to whom a section 49 notice has been given is guilty of an offence if he knowingly fails, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice.*

*(2) In proceedings against any person for an offence under this section, if it is shown that that person was in possession of a key to any protected information at any time before the time of the giving of the section 49 notice, that person shall be taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent times, unless it is shown that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it.*

*(3) For the purposes of this section a person shall be taken to have shown that he was not in possession of a key to protected information at a particular time if-*

*(a) sufficient evidence of that fact is adduced to raise an issue with respect to it; and*

*(b) the contrary is not proved beyond a reasonable doubt.*

*(4) In proceedings against any person for an offence under this section it shall be a defence for that person to show*

*(a) that it was not reasonably practicable for him to make the disclosure required by virtue of the giving of the section 49 notice before the time by which he was required, in accordance with that notice, to make it; but*

*(b) that he did make that disclosure as soon after that time as it was reasonably practicable for him to do so.*

*(5) A person guilty of an offence under this section shall be liable-*

*(a) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both;*

*(b) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.*

*[…]*

The Regulation of Investigatory Powers Act 2000 obliges the suspect of a crime to support the work of law-enforcement agencies.[2282]

A general concern to this regulation is that the obligation leads to potential conflict with the fundamental rights of a suspect against self-incrimination.[2283] Instead of leaving the investigation to the competent authorities, the suspect has to actively support the investigation. The strong protection against self-incrimination in many countries thus raises the question of how far such regulation has the potential to become a model solution to address the challenge posed by encryption technology.[2284]

Another concern is that losing the key could lead to a criminal investigation. Although the criminalization requires that the offender knowingly refuses to disclose the key, losing the key could involve people using encryption keys in unwanted criminal proceedings. In particular, however, section 53(2) potentially interferes with the burden of proof.[2285]

Finally, there are technical solutions that enable offenders to circumvent the obligation to disclose the key used to encrypt data. One example of how the offender can circumvent the obligation is the use of encryption software based on the "plausible deniability[2286]" principle.[2287]

### 6.5.12 Remote forensic software

As explained above, the search for evidence on the suspect's computer requires physical access to the relevant hardware (computer system and external storage media). This procedure in general implies the need to access the apartment, house or office of the suspect. In this case, the suspect will be aware of an ongoing investigation as soon as the investigators start carrying out the search.[2288] This information could lead to a change in behaviour.[2289] If the offender, for example, attacked some computer systems to test his capabilities in order to participate in the preparation of a much larger series of attacks together with other offenders at a future date, the search procedure could hinder the investigators from identifying the other suspects as it is very likely the offender will stop communicating with them.

To avoid the detection of ongoing investigations, law-enforcement agencies demand an instrument that allows them to access computer data stored on the suspect's computers, and that can be secretly used like telephone surveillance for monitoring telephone calls.[2290] Such an instrument would enable law-enforcement agencies to remotely access the suspect's computer and search for information. Currently, the question whether or not such instruments are necessary is being intensively discussed.[2291] Already in 2001, reports pointed out that the United States FBI was developing a keylogger tool for Internet-related investigations called the "magic lantern".[2292] In 2007, reports were published that law-enforcement agencies in the United States were using software to trace back suspects that use means of anonymous

communication.[2293] The reports were referring to a search warrant where the use of a tool called CIPAV[2294] was requested.[2295] After the Federal Court in Germany decided that the existing Criminal Procedural Law provisions do not allow investigators to use remote forensic software to secretly search the suspect's computer, a debate about the need to amend the existing laws in this area started.[2296]Within the debate, information was published that investigation authorities had unlawfully used remote forensic software in a couple of investigations.[2297]

Various concepts of "remote forensic software" and especially its possible functions have been discussed.[2298] Seen from a theoretical perspective the software could have the following functions: one function could be a search function. This function would enable law-enforcement agencies to search for illegal content and collect information about the files stored on the computer.[2299] Another possibility is recording. Investigators could record data that are processed on the computer system of the suspect without being permanently stored. If, for example, the suspect uses voice-over-IP services to communicate with other suspects, the content of the conversation would in general not be stored.[2300] The remote forensic software could record the processed data to preserve them for the investigators. If the remote forensic software contains a module to record key strokes, this module could be used to record passwords that the suspect uses to encrypt files.[2301] Furthermore, such a tool could include identification functions that enable the investigators to prove the suspect's participation in a criminal offence, even if he/she used anonymous communication services that make it difficult for investigators to identify the offender by tracing back the IP-address used.[2302] Finally, remote software could be used to activate a webcam or the microphone for room-observation purposes.[2303]

Although the possible functions of the software seem to be very useful for investigators, it is important to point out that there are a number of legal as well as technical difficulties related to the use of such software. Seen from a technical point of view, the following aspects need to be taken into consideration.

### Difficulties with regard to the installation process

The software needs to be installed on the suspect's computer system. The spread of malicious software proves that the installation of software on the computer of an Internet user without his permission is possible. But the main difference between a virus and a remote forensic software is the fact that the remote forensic software needs to be installed on a specific computer system (the suspect's computer) while a computer virus aims to infect as many computers as possible without needing to focus on a specific computer system. There are a number of techniques by which the software can be transmitted to the suspect's computer. For example: installation with physical access to the computer system; placing the software on a website for download; online access to the computer system by circumventing security measures; and hiding the software in the data stream that is generated during Internet activities, to mention just a few.[2304] Due to protection measures such as virus scanners and firewalls that most computers are equipped with, all remote installation methods present difficulties for investigators.[2305]

### Advantage of physical access

A number of the analyses conducted (e.g. physical inspection of data processing media) require access to the hardware. In addition, remote forensic software would only enable investigators to analyse computer systems that are connected to the Internet.[2306] Furthermore, working remotely, it is difficult to maintain the integrity of the suspect's computer system.[2307] With regard to these aspects, remote forensic software will in general not be able to replace physical examination of the suspect's computer system.

In addition, a number of legal aspects need to be taken into consideration before implementing a provision that enables investigators to install remote forensic software. The safeguards established in the criminal procedural codes as well as the constitutions of many countries limit the potential functions of such software. In addition to the national aspects, the installation of remote forensic software could violate the principle of national sovereignty.[2308] If the software is installed on a notebook that is taken out of the country after the installation process, the software might enable the investigators to perform criminal investigations in a foreign territory without the necessary permission of the responsible authorities.

**Example**

One approach can be found in the legislative text developed by the beneficiary states within the HIPCAR initiative.[2309]

***Forensic Software***
***27.****(1) If a [judge] [magistrate] is satisfied on the basis of [information on oath/affidavit] that in an investigation concerning an offence listed in paragraph 7 herein below there are reasonable grounds to believe that essential evidence can not be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] on application authorize a police officer to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information:*

*(a) suspect of the offence, if possible with name and address, and*

*(b) description of the targeted computer system, and*

*(c) description of the intended measure, extent and duration of the utilization, and*

*(d) reasons for the necessity of the utilization.*

*(2) Within such investigation it is necessary to ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation it is necessary to log*

*(a) the technical mean used and time and date of the application; and*

*(b) the identification of the computer system and details of the modifications undertaken within the investigation;.*

*(c) any information obtained.*

*Information obtained by the use of such software need to be protected again any modification, unauthorized deletion and unauthorized access.*

*(3) The duration of authorization in section 27 (1) is limited to [3 month]. If the conditions of the authorization is no longer met, the action taken are to stop immediately.*

*(4) The authorization to install the software includes remotely accessing the suspects computer system.*

*(5) If the installation process requires physical access to a place the requirements of section 20 need to be fulfilled.*

*(6) If necessary a [law enforcement] [police] officer may pursuant to the order of court granted in (1) above request that the court order an internet service provider to support the installation process.*

*(7) [List of offences]*

*(8) A country may decide not to implement section 27.*

The drafters of the legislative text pointed out that they are aware that application of the instrument could be very intrusive and potentially interfere with fundamental rights of the suspect.[2310] Several safeguards have therefore been implemented. Firstly, the use of such software requires that evidence cannot be collected by means of other processes. Secondly, an order by a judge or magistrate is required. Thirdly, the application needs to contain four key elements. In addition, the authorized acts are limited by both paragraphs 1 and 2.

### 6.5.13 Authorization requirement

Offenders can take certain measures to complicate investigations. In addition to using software that enables anonymous communication,[2311] identification can be complicated if the suspect is using public Internet terminals or open wireless networks. Restrictions on the production of software enabling the user to hide his/her identity and on making public Internet access terminals available that do not require identification could help law-enforcement agencies to conduct investigations more efficiently. An example of an approach to restrict the use of public terminals to commit criminal offences is Article 7[2312] of Italian Decree 144,[2313] which was converted into a law in 2005 (Legge No. 155/2005).[2314] This provision forces anybody who intends to offer public Internet access (e.g. Internet cafes or universities[2315]) to apply for authorization. In addition, the person in question is obliged to request identification from his/her

customers prior to giving them access to use the service. Since a private person who sets up a wireless access point is in general not covered by this obligation, monitoring can quite easily be circumvented if offenders make use of unprotected private networks to hide their identity.[2316]

It is questionable whether the extent of improvement in investigations justifies the restriction of access to the Internet and to anonymous communication services. Free access to the Internet is today recognized as an important aspect of the right of free access to information that is protected by the constitution in a number of countries. Registration obligation can interfere with the right to operate Internet services without authorization, as emphasized by the 2005 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression.[2317] It is likely that the requirement for identification will affect the use of the Internet, insofar as users will then always have to fear that their Internet usage is monitored. Even when users know that their activities are legal, it can still influence their interaction and usage.[2318] At the same time, offenders who want to prevent identification can easily circumvent the identification procedure. They can, for example, use prepaid phonecards bought abroad which do not require identification to access the Internet.

Similar concerns arise with regard to legislation targeting anonymous communication services. There is an ongoing debate on whether similar instruments discussed with regard to encryption technology should be applied to anonymous communication technology and services.[2319] Apart from the conflict between protecting privacy and ensuring the ability to investigate offences, the arguments against the practicability of the various legal approaches to address the challenge of encryption (especially lack of enforceability) apply equally to anonymous communication.

## 6.6 International cooperation

**Bibliography (selected):** *Brenner*, Organized Cybercrime, North Carolina Journal of Law & Technology, 2002, Issue 4; *Choo,* Trends in Organized Crime, 2008, page 273 *et seq.*; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005; *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992; *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2; *Krone*, International Police Operations Against Online Child Pornography, Trends and Issues in Crime and Criminal Justice, No. 296; *Pop*, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science, 2008, page 160 *et seq.*; *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf; Recueil Des Cours, Collected Courses, Hague Academy of International Law, 1976; *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf; *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001; *Stowell*, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931; *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9; *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003.

### 6.6.1 Introduction

An increasing number of cybercrimes have an international dimension.[2320] As pointed out above, one reason behind this phenomenon is the fact that there is very little need for physical presence of the offender at the place where a service is offered.[2321] Offenders do not therefore generally need to be present at the place where the victim is located. As there is no comprehensive international legal framework and no supranational body able to investigate such offences, transnational crimes require cooperation of authorities in the countries involved.[2322] The mobility of offenders, the independence from presence of the offender and the impact of the offence make it necessary for law-enforcement and judicial authorities to collaborate and assist the state that has assumed jurisdiction.[2323] Due to differences in national law and limited instruments, international cooperation is considered to be one of the major challenges of a globalization of crime.[2324] This is relevant for traditional forms of transnational crimes as well as cybercrime. One of the key demands of investigators in transnational investigations is immediate reaction of their counterparts in the country where the offender is located.[2325] Especially when it comes to this issue, traditional instruments of international judicial cooperation in criminal law matters very often do not meet requirements in terms of the speed of investigations in the Internet.[2326]

### 6.6.2 Mechanisms for international cooperation

For cybercrime investigations, the most relevant formal mechanisms supporting international cooperation are mutual legal assistance and extradition. Other mechanisms such as transfer of prisoners, transfer of proceedings in criminal matters, confiscation of criminal proceeds and asset recovery are less important in practice. In addition to the formal mechanisms, there are informal ways of cooperation such as exchange of intelligence among law-enforcement agencies in different countries.

### 6.6.3 Overview of applicable instruments

There are three main scenarios when it comes to identifying the applicable instrument for international cooperation. First, relevant procedures can be part of international agreements, such as the United Nations Convention against Transnational Organized Crime (UNTOC)[2327] and its three protocols,[2328] or regional conventions, such as the Inter-American Convention on Mutual Assistance in Criminal Matters,[2329] the European Convention on Mutual Assistance in Criminal Matters[2330] and the Council of Europe Convention on Cybercrime.[2331] The second possibility is for procedures to be regulated by bilateral agreements. Such agreements in general refer to specific requests that can be submitted and define the relevant procedures and forms of contact as well as the rights and obligations of the requesting and requested states.[2332] Australia, for example, has signed more than 30 bilateral agreements with other countries regulating aspects of extradition.[2333] Some negotiations of such agreements have also addressed cybercrime as a topic, but it is uncertain to what extent the existing agreements adequately govern cybercrime.[2334] If neither a multilateral nor a bilateral agreement is applicable, international cooperation generally needs to be founded on international courtesy, based on reciprocity.[2335] As cooperation based on bilateral agreements and courtesy very much depends on the circumstances of the actual case and the countries involved, the following overview focuses on international and regional conventions.

### 6.6.4 United Nations Convention against Transnational Organized Crime

The main international instrument for judicial cooperation in criminal matters is the United Nations Convention against Transnational Organized Crime (UNTOC).[2336] This convention contains important instruments for international cooperation, but was not specifically designed to address cybercrime-related issues. Nor does it provide specific provisions dealing with urgent requests to preserve data.

#### Application of the United Nations Convention against Transnational Organized Crime

Based on Article 3, paragraph 1, the convention is only applicable in cybercrime cases if the offence involves an organized crime group. Article 2 of UNTOC defines an organized crime group as a structured group of three or more people.

***Article 2**. Use of terms*
*For the purposes of this Convention:*

*(a) "Organized criminal group" shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit;*

*[...]*

***Article 3**. Scope of application*
*1. This Convention shall apply, except as otherwise stated herein, to the prevention, investigation and prosecution of:*

*(a) The offences established in accordance with articles 5, 6, 8 and 23 of this Convention; and*

*(b) Serious crime as defined in article 2 of this Convention; where the offence is transnational in nature and involves an organized criminal group.*

The convention is therefore particularly relevant for cases involving forms of organized crime. Without doubt, organized crime is involved in cybercrime. However, the extent of the involvement and therefore the relevance of UNTOC in transnational cybercrime investigations is uncertain. As a matter of fact, the determination of involvement of organized crime is highly relevant. However, analysing the link between identity-related crime and organized crime presents difficulties. The first main obstacle is the absence of scientifically reliable research in this area. Unlike the technical aspects of offences, the organized crime component of offences is less intensively analysed. There have been successful investigations identifying several crime gangs involved in cybercrime. However, the structure of those groups is not necessarily comparable to that of traditional organized crime groups. Cybercrime groups tend to have a looser and more flexible structure.[2337] In addition, groups are often much smaller compared to traditional organized crime groups.[2338] The Internet enables close cooperation with others and coordination of activities without ever having met face-to-face.[2339] This makes it feasible for offenders to work together in fluid ad hoc groups.[2340].

### Requests for mutual legal assistance

The procedures for mutual legal assistance are defined in Art. 18. This provision contains a whole set of procedures.

***Article 18**. Mutual legal assistance*
*1. States Parties shall afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to the offences covered by this Convention as provided for in article 3 and shall reciprocally extend to one another similar assistance where the requesting State Party has reasonable grounds to suspect that the offence referred to in article 3, paragraph 1 (a) or (b), is transnational in nature, including that vic-tims, witnesses, proceeds, instrumentalities or evidence of such offences are located in the requested State Party and that the offence involves an organized criminal group.*
*2. Mutual legal assistance shall be afforded to the fullest extent possible under relevant laws, treaties, agreements and arrangements of the requested State Party with respect to investigations, prosecutions and judicial proceedings in relation to the offences for which a legal person may be held liable in accordance with article 10 of this Convention in the requesting State Party.*
*[...]*

Article 18 (1)-(2) contains general principles for international cooperation.[2341] They are relevant for cybercrime investigation as well as traditional investigation. The Council of Europe Convention on Cybercrime contains similar regulation.

***Article 18**. Mutual legal assistance*

*[…]*
*3. Mutual legal assistance to be afforded in accordance with this article may be requested for any of the following purposes:*
*(a) Taking evidence or statements from persons;*
*(b) Effecting service of judicial documents;*
*(c)Executing searches and seizures, and freezing;*
*(d) Examining objects and sites;*
*(e) Providing information, evidentiary items and expert evaluations;*
*(f) Providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records;*
*(g) Identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes;*
*(h) Facilitating the voluntary appearance of persons in the requesting State Party;*
*(i) Any other type of assistance that is not contrary to the domestic law of the requested State Party.*
*[…]*

Article 18(3) contains specific mutual legal assistance requests. The list is complex and ranges from taking evidence to tracing proceeds of crime. As mentioned above, UNTOC does not contain specific wording for data-related requests, such as requests to intercept communication or preserve data. However, Article 18(3)(i) opens the provision to other requests, so UNTOC can also be used for data-related requests. While it is in general worth discussing the advantages of specific regulation of requests, comparable regional instruments containing specific requests, like the Council of Europe Convention on Cybercrime, usually only refer to procedural instruments in national law, without defining specific procedures for mutual legal requests.

***Article 18**. Mutual legal assistance*
*[…]*
*4. Without prejudice to domestic law, the competent authorities of a State Party may, without prior request, transmit information relating to criminal matters to a competent authority in another State Party where they believe that such information could assist the authority in undertaking or successfully concluding inquiries and criminal proceedings or could result in a request formulated by the latter State Party pursuant to this Convention.*
*5. The transmission of information pursuant to paragraph 4 of this article shall be without prejudice to inquiries and criminal proceedings in the State of the competent authorities providing the information. The competent authorities receiving the information shall comply with a request that said information remain confidential, even temporarily, or with restrictions on its use. However, this shall not prevent the receiving State Party from disclosing in its proceedings information that is exculpatory to an accused person. In such a case, the receiving State Party shall notify the transmitting State Party prior to the disclosure and, if so requested, consult with the transmitting State Party. If, in an exceptional case, advance notice is not possible, the receiving State Party shall inform the transmitting State Party of the disclosure without delay.*
*[…]*

Article 18 (4)-(5) deals with intelligence sharing. It stipulates a form of cooperation[2342] which takes place on a voluntary basis, without the need for the receiving party to submit a mutual legal assistance request.[2343] It covers information relating to criminal matters, such as information about potential consumers of child pornography located in another country that has been discovered during an investigation. Especially in complex investigations, where recourse to formal mutual instruments is time-consuming and hence can hinder investigations, law-enforcement agencies tend to shift to non-formal means of cooperation. However, information-sharing will only be able to work as a substitute if the state receiving the information is able to collect all relevant evidence on its own. In all other cases, formal cooperation is usually required in any event in order to ensure the chain of custody. In the debate on

shifting international cooperation from formal requests to spontaneous information sharing, it is necessary to keep in mind that the formal process was developed to protect the integrity of a state as well the rights of the accused. Sharing of information should therefore not circumvent the dogmatic structure of mutual legal assistance.

***Article 18**. Mutual legal assistance*
*[…]*
*6. The provisions of this article shall not affect the obligations under any other treaty, bilateral or multilateral, that governs or will govern, in whole or in part, mutual legal assistance.*
*7. Paragraphs 9 to 29 of this article shall apply to requests made pursuant to this article if the States Parties in question are not bound by a treaty of mutual legal assistance. If those States Parties are bound by such a treaty, the corresponding provisions of that treaty shall apply unless the States Parties agree to apply paragraphs 9 to 29 of this article in lieu thereof. States Parties are strongly encouraged to apply these paragraphs if they facilitate cooperation.*
*8.States Parties shall not decline to render mutual legal assistance pursuant to this article on the ground of bank secrecy.*
*9. States Parties may decline to render mutual legal assistance pursuant to this article on the ground of absence of dual criminality. However, the requested State Party may, when it deems appropriate, provide assistance, to the extent it decides at its discretion, irrespective of whether the conduct would constitute an offence under the domestic law of the requested State Party.*
*10. A person who is being detained or is serving a sentence in the territory of one State Party whose presence in another State Party is requested for purposes of identification, testimony or otherwise providing assistance in ob-taining evidence for investigations, prosecutions or judicial proceedings in relation to offences covered by this Convention may be transferred if the following conditions are met:*
*(a) The person freely gives his or her informed consent;*
*(b) The competent authorities of both States Parties agree, subject to such conditions as those States Parties may deem appropriate.*
*11.For the purposes of paragraph 10 of this article:*
*(a) The State Party to which the person is transferred shall have the authority and obligation to keep the person transferred in custody, unless other- wise requested or authorized by the State Party from which the person was transferred;*
*(b) The State Party to which the person is transferred shall without delay implement its obligation to return the person to the custody of the State Party from which the person was transferred as agreed beforehand, or as otherwise agreed, by the competent authorities of both States Parties;*
*(c) The State Party to which the person is transferred shall not require the State Party from which the person was transferred to initiate extradition pro-ceedings for the return of the person;*
*(d) The person transferred shall receive credit for service of the sentence being served in the State from which he or she was transferred for time spent in the custody of the State Party to which he or she was transferred.*
*12. Unless the State Party from which a person is to be transferred in accordance with paragraphs 10 and 11 of this article so agrees, that person, whatever his or her nationality, shall not be prosecuted, detained, punished or subjected to any other restriction of his or her personal liberty in the territory of the State to which that person is transferred in respect of acts, omissions or convictions prior to his or her departure from the territory of the State from which he or she was transferred.*
*[…]*

Article 18 (6)-(12) deals with procedural aspects of mutual legal assistance. Of particular interest for cybercrime cases are paragraphs 8 and 9. Paragraph 9 enables states to decline mutual assistance requests on the grounds of absence of dual criminality. This is particularly important insofar as the scope of approaches to harmonize substantive criminal provisions with regard to cybercrime – such as the Council of Europe Convention on Cybercrime – is currently limited. By mid-2010, only 30 countries had ratified this instrument and set corresponding minimum standards with regard to cybercrime offences. This can hinder cooperation based on UNTOC.

***Article 18**. Mutual legal assistance*
*[…]*
*13. Each State Party shall designate a central authority that shall have the responsibility and power to receive requests for mutual legal assistance and either to execute them or to transmit them to the competent authorities for execution. Where a State Party has a special region or territory with a separate system of mutual legal assistance, it may designate a distinct central authority that shall have the same function for that region or territory. Central authorities shall ensure the speedy and proper execution or transmission of the requests received. Where the central authority transmits the request to a competent authority for execution, it shall encourage the speedy and proper execution of the request by the competent authority. The Secretary-General of the United Nations shall be notified of the central authority designated for this purpose at the time each State Party deposits its instrument of ratification, acceptance or approval of or accession to this Convention. Requests for mutual legal assistance and any communication related thereto shall be transmitted to the central authorities designated by the States Parties. This requirement shall be without prejudice to the right of a State Party to require that such requests and communications be addressed to it through diplomatic channels and, in urgent circumstances, where the States Parties agree, through the International Criminal Police Organization, if possible.*
*14. Requests shall be made in writing or, where possible, by any means capable of producing a written record, in a language acceptable to the requested State Party, under conditions allowing that State Party to establish authenticity. The Secretary-General of the United Nations shall be notified of the language or languages acceptable to each State Party at the time it deposits its instrument of ratification, acceptance or approval of or accession to this Convention. In urgent circumstances and where agreed by the States Parties, requests may be made orally, but shall be confirmed in writing forthwith.*
*15. A request for mutual legal assistance shall contain:*
*(a) The identity of the authority making the request;*
*(b) The subject matter and nature of the investigation, prosecution or judicial proceeding to which the request relates and the name and functions of the authority conducting the investigation, prosecution or judicial proceeding;*
*(c) A summary of the relevant facts, except in relation to requests for the purpose of service of judicial documents;*
*(d) A description of the assistance sought and details of any particular procedure that the requesting State Party wishes to be followed;*
*(e)Where possible, the identity, location and nationality of any person concerned; and*
*(f) The purpose for which the evidence, information or action is sought.*
*16. The requested State Party may request additional information when it appears necessary for the execution of the request in accordance with its domestic law or when it can facilitate such execution.*
*[…]*

Article 18 (13)-(16) defines the form and content of requests, as well as the channels of communication. With regard to channels of communication, the Convention follows the idea that requests are transmitted from central authority to central authority.[2344] The Convention underscores the importance of this procedure to ensure speedy and proper execution of the request. The roles of central authorities may differ, and range from direct involvement in handling and executing requests to forwarding them to the competent authorities. The Convention leaves it up to states whether to require the transmittal through diplomatic channels. This latter option being a lengthy process, such a procedure would dramatically slow down transmission and especially hinder expedited measures such as the preservation of traffic data. Unlike the Council of Europe Convention on Cybercrime,[2345] UNTOC does not define means of expedited cooperation, but provides a general procedure for cases of urgency. If states agree, the International Criminal Police Organization (Interpol) can be used as a channel for communication. In order to facilitate identification of the relevant authority in another country, the United Nations Office on Drugs and Crimes (UNODC) maintains an online directory.[2346] It provides the issuing authority with details of the central authority of the requested state, the channels of communication and other relevant information.[2347]

When submitting the request, it is necessary to meet the formal requirements as defined by paragraphs 14 and 15. Oral requests are only permitted in urgent cases and need to be followed by a written request. The reports of the State Parties concerning application of the Convention show that while many states have legislation requiring MLA requests to be made in writing, only a handful of countries have admitted temporary advance requests forwarded by e-mail.[2348] In this respect, UNTOC differs from the Council of Europe Convention on Cybercrime, which encourages states to use means of electronic communication in urgent cases.[2349] UNODC provides a software for drafting such requests with the aim of ensuring that requests are complete (Mutual Legal Assistance Request Writer Tool).[2350]

***Article 18. Mutual legal assistance***

*[…]*

*17. A request shall be executed in accordance with the domestic law of the requested State Party and, to the extent not contrary to the domestic law of the requested State Party and where possible, in accordance with the procedures specified in the request.*

*18. Wherever possible and consistent with fundamental principles of domestic law, when an individual is in the territory of a State Party and has to be heard as a witness or expert by the judicial authorities of another State Party, the first State Party may, at the request of the other, permit the hearing to take place by video conference if it is not possible or desirable for the individual in question to appear in person in the territory of the requesting State Party. States Parties may agree that the hearing shall be conducted by a judicial authority of the requesting State Party and attended by a judicial authority of the requested State Party.*

*19. The requesting State Party shall not transmit or use information or evidence furnished by the requested State Party for investigations, prosecutions or judicial proceedings other than those stated in the request without the prior consent of the requested State Party. Nothing in this paragraph shall prevent the requesting State Party from disclosing in its proceedings information or evi-dence that is exculpatory to an accused person. In the latter case, the requesting State Party shall notify the requested State Party prior to the disclosure and, if so requested, consult with the requested State Party. If, in an exceptional case, advance notice is not possible, the requesting State Party shall inform the requested State Party of the disclosure without delay.*

*20. The requesting State Party may require that the requested State Party keep confidential the fact and substance of the request, except to the extent necessary to execute the request. If the requested State Party cannot comply with the requirement of confidentiality, it shall promptly inform the requesting State Party.*

*21. Mutual legal assistance may be refused:*

*(a) If the request is not made in conformity with the provisions of this article;*

*(b) If the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests;*

*(c) If the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or judicial proceedings under their own jurisdiction;*

*(d) If it would be contrary to the legal system of the requested State Party relating to mutual legal assistance for the request to be granted.*

*22. States Parties may not refuse a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.*

*23. Reasons shall be given for any refusal of mutual legal assistance.*

*24. The requested State Party shall execute the request for mutual legal assistance as soon as possible and shall take as full account as possible of any deadlines suggested by the requesting State Party and for which reasons are given, preferably in the request. The requested State Party shall respond to reasonable requests by the requesting State Party on progress of its handling of the request. The requesting State Party shall promptly inform the requested State Party when the assistance sought is no longer required.*

*25. Mutual legal assistance may be postponed by the requested State Party on the ground that it interferes with an ongoing investigation, prosecution or judicial proceeding.*

*26. Before refusing a request pursuant to paragraph 21 of this article or postponing its execution pursuant to paragraph 25 of this article, the requested State Party shall consult with the requesting State Party to consider whether assistance may be granted subject to such terms and conditions as it deems necessary. If the requesting State Party accepts assistance subject to those con-ditions, it shall comply with the conditions.*
*27. Without prejudice to the application of paragraph 12 of this article, a witness, expert or other person who, at the request of the requesting State Party, consents to give evidence in a proceeding or to assist in an investigation, prosecution or judicial proceeding in the territory of the requesting State Party shall not be prosecuted, detained, punished or subjected to any other restriction of his or her personal liberty in that territory in respect of acts, omissions or convictions prior to his or her departure from the territory of the requested State Party. Such safe conduct shall cease when the witness, expert or other person having had, for a period of fifteen consecutive days or for any period agreed upon by the States Parties from the date on which he or she has been officially informed that his or her presence is no longer required by the judicial authorities, an opportunity of leaving, has nevertheless remained voluntarily in the territory of the requesting State Party or, having left it, has returned of his or her own free will.*
*28. The ordinary costs of executing a request shall be borne by the re- quested State Party, unless otherwise agreed by the States Parties concerned. If expenses of a substantial or extraordinary nature are or will be required to fulfil the request, the States Parties shall consult to determine the terms and condi-tions under which the request will be executed, as well as the manner in which the costs shall be borne.*
*29. The requested State Party:*
*(a) Shall provide to the requesting State Party copies of government records, documents or information in its possession that under its domestic law are available to the general public;*
*(b) May, at its discretion, provide to the requesting State Party in whole, in part or subject to such conditions as it deems appropriate, copies of any government records, documents or information in its possession that under its domestic law are not available to the general public.*
*30. States Parties shall consider, as may be necessary, the possibility of concluding bilateral or multilateral agreements or arrangements that would serve the purposes of, give practical effect to or enhance the provisions of this article.*

### 6.6.5 Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime (the "Convention on Cybercrime") addresses the increasing importance of international cooperation in Articles 23 to 35.

#### General Principles for International Cooperation

Article 23 of the Council of Europe Convention on Cybercrime defines three general principles regarding international cooperation in cybercrime investigations among members.

***Article 23 – General principles relating to international co-operation***
*The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.*

First of all, members are supposed to provide cooperation in international investigation to the widest extent possible. This obligation reflects the importance of international cooperation in cybercrime investigations. In addition, Article 23 notes that the general principles do not only apply in cybercrime investigations, but in any investigation where evidence in electronic form needs to be collected. This covers cybercrime investigations as well as investigations in traditional cases. If the suspect in a murder case has used an e-mail service abroad, Article 23 would be applicable with regard investigations that are

necessary in regard to data stored by the host provider.[2351] The third principle notes that the provisions dealing with international cooperation do not substitute provisions of international agreements pertaining to mutual legal assistance and extradition or relevant provisions of domestic law pertaining to international cooperation. The drafters of the Convention on Cybercrime emphasized that mutual assistance should in general be carried out through the application of relevant treaties and similar arrangements for mutual assistance. As a consequence, the Convention on Cybercrime does not intend to create a separate general regime on mutual assistance. Therefore, only in those cases where the existing treaties, laws and arrangements do not already contain such provisions, each Party is required to establish a legal basis to enable the carrying out of international cooperation as defined by the Convention on Cybercrime.[2352]

### Extradition

The extradition of nationals remains one of the most difficult aspects of international cooperation.[2353] Requests for extradition very often lead to conflict between the need to protect the citizen and the need to support an ongoing investigation in a country abroad. Article 24 defines the principles of extradition. Unlike Article 23, the provision is limited to the offences mentioned in the Convention on Cybercrime and does not apply in cases that are minor (deprivation of liberty for a maximum period of at least one year[2354]). To avoid conflicts that could occur with the regard to the ability of the parties to make reservations, Article 24 is based on the principle of dual criminality.[2355]

***Article 24 – Extradition***

*1a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.*

*b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.*

*2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.*

*3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.*

*4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.*

*5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.*

*6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.*

*7a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.*

*b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.*

### General Principles of Mutual Assistance

With regard to mutual assistance, Article 25 complements the principles set out in Article 23. One of the most important regulations in Article 25 is paragraph 3, which highlights the importance of fast communication in cybercrime investigations.[2356] As pointed out previously, a number of cybercrime investigations at the national level fail because the investigations take too long and important data are therefore deleted before procedural measures to preserve them are undertaken.[2357] Investigations that require mutual legal assistance usually take even longer, due to the time-consuming formal requirements in the communications of law-enforcement agencies. The Convention on Cybercrime addresses this problem by highlighting the importance of enabling the use of expedited means of communication.[2358]

***Article 25 – General principles relating to mutual assistance***
*1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.*
*2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.*
*3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.*
*4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.*
*5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.*

In the course of cybercrime investigations carried out on a national level, links to offences related to another country may be discovered. If law-enforcement agencies, for example, investigate a child-pornography case, they may find information about paedophiles from other countries who have participated in the exchange of child pornography.[2359] Article 26 sets out the regulations that are necessary for law-enforcement agencies to inform foreign law-enforcement agencies without jeopardizing their own investigation.[2360]

***Article 26 – Spontaneous information***
*1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.*

*2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.*

As pointed out above, there are certain concerns related to the replacement of mutual legal assistance by spontaneous information. Information sharing will only be able to work if the state receiving the information is able to collect all relevant evidence on its own. In all other cases, formal cooperation is usually required in any event in order to ensure the chain of custody. In the debate on shifting international cooperation from formal requests to spontaneous information sharing, it is necessary to keep in mind that the formal process was developed to protect the integrity of a state as well the rights of the accused. Sharing of information should therefore not circumvent the dogmatic structure of mutual legal assistance.

One of the most important regulations of Article 26 relates to the confidentiality of information. Given that a number of investigations can only be carried out successfully if the offender is not aware of the investigations taking place, Article 26 enables the providing party to request confidentiality for the information transmitted. If the confidentiality cannot be granted, the providing party can refuse the information process.

### Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Like Article 25, Article 27 is based on the idea that mutual legal assistance should be carried out through application of relevant treaties and similar arrangements instead of solely referring to the Convention on Cybercrime. The drafters of the Convention on Cybercrime decided not to establish a separate mandatory mutual legal assistance regime within the Convention on Cybercrime.[2361] If other instruments are already in place, Articles 27 and 28 are not relevant within a concrete request. Only in those cases where other regulations are not applicable, Articles 27 and 28 provide a set of mechanisms that can be used to carry out mutual legal assistance requests.

The most important aspects regulated by Article 27 include the obligation to establish a designated contact point for mutual legal assistance requests[2362], requirements of direct communication between the contact points to avoid lengthy procedures[2363] and creation of a database of all contact points by the Secretary General of the Council of Europe.

In addition, Article 27 defines limitations with regard to requests for assistance. Parties to the Convention on Cybercrime can especially refuse cooperation with regard to political offences or if it considers that the cooperation could prejudice its sovereignty, security, public order or other essential interests.

The drafters of the Convention on Cybercrime saw the need on the one hand to enable the parties to refuse cooperation in certain cases but on the other hand pointed out that the parties should exercise the refusal of cooperation with restraint in order to avoid conflict with the principles set out previously.[2364] It is therefore especially important to define the term “other essential interests” in a narrow way. The Explanatory Report to the Convention on Cybercrime points out that this could be the case if the cooperation could lead to fundamental difficulties for the requested party.[2365] From the drafters’ perspective, concerns related to inadequate data-protection laws are not considered to be essential interests.[2366]

### Mutual assistance regarding provisional measures

Arts. 28-33 are a reflection of the procedural instruments of the Convention on Cybercrime.[2367] The Convention on Cybercrime contains a number of procedural instruments that are designed to improve investigations in Member States.[2368] With regard to the principle of national sovereignty[2369], these instruments can only be used for investigations at the national level.[2370] If investigators realize that evidence needs to be collected outside their territory, they need to request mutual legal assistance. In

addition to Article 18, each of the instruments established by Arts. 16-21 has a corresponding provision in Arts. 28-33 which enables law-enforcement agencies to apply the procedural instruments on request of a foreign law-enforcement agency.

| Procedural Instrument | Corresponding ML provision |
|---|---|
| Article 16 – Expedited preservation of stored computer data[2371] | Article 29 |
| Article 17 – Expedited preservation and partial disclosure of traffic data[2372] | Article 30 |
| Article 18 – Production order[2373] | None |
| Article 19 – Search and seizure of stored computer data[2374] | Article 31 |
| Article 20 – Real-time collection of traffic data[2375] | Article 33 |
| Article 21 – Interception of content data[2376] | Article 34 |

### Transborder access to stored computer data

In addition to purely mirroring procedural provisions, the drafters of the Convention on Cybercrime discussed under which circumstances law-enforcement agencies are allowed to access computer data that are neither stored in their territory nor under the control of a person in their territory. They were only able to agree on two case scenarios where an investigation should be carried out by one law-enforcement agency without the need to request mutual legal assistance.[2377] Further agreements were not possible[2378] and even the solution reached is still criticized by Member States of the Council of Europe.[2379]

The two cases where law-enforcement agencies are allowed to access data stored outside their territory are related to:

- publicly available information; and/or
- access with the consent of the person in control.

***Article 32 – Trans-border access to stored computer data with consent or where publicly available***
*A Party may, without the authorisation of another Party:*
*a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or*
*b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.*

Other forms of transborder access are not covered by Article 32, but nor are they precluded.[2380]

Article 32 notes that if the relevant data are publicly available, foreign law-enforcement agencies are allowed to access this information. An example of publicly available information is information made available on websites without access control (such as passwords). If investigators were not allowed – unlike any other user –to access these websites, this could seriously hinder their work. Therefore, this first situation addressed by Article 32 is widely accepted.

The second situation in which law-enforcement agencies are allowed to access stored computer data outside their territory is when the investigators have obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data. This authorization is heavily criticized.[2381]

One main concern is the fact that the provision in its current wording probably contradicts fundamental principles of international law.[2382] Based on international law, investigators have to respect national sovereignty during an investigation.[2383] They are especially not allowed to carry out investigations in another state without the consent of the competent authorities in that state. The decision whether such permission should be granted is not in the hands of an individual, but of the state authorities, since

interference with national sovereignty does not only affect the rights of the individual, but also state concerns. By ratifying the Convention on Cybercrime, countries partly dismiss the principle and allow other countries to carry out investigations affecting their territory.

Another concern is the fact that Article 32b does not define procedures for the investigation. Based on the text of the provision, it is not necessary for the same limitations to be applied that exist in domestic law with regard to comparable domestic investigations. Interestingly enough, such a restriction was included in the draft text of the Convention on Cybercrime presented in the beginning of 2000, but was removed in the 22nd draft.[2384]

By creating Article 32 sub-paragraph b, the drafters of the Convention on Cybercrime ultimately violated the dogmatic structure of the mutual legal assistance regime in this Convention. With Article 18, the drafters of the Convention on Cybercrime enabled investigators to order the submission of data in domestic investigations. If law-enforcement agencies were to be authorized to use this instrument in international investigations, it would have been sufficient to include it in the catalogue of instruments mentioned in the context of mutual legal assistance. However, the instrument cannot be applied in international investigations because the corresponding provision in Chapter 3 of the Convention on Cybercrime, dealing with international cooperation, is lacking. Instead of relinquishing the dogmatic structure by allowing foreign investigators to contact directly the person who has control over the data and ask for the submission of the data, the drafters could have simply implemented a corresponding provision in Chapter 3 of the Convention.[2385]

Transborder access to stored computer data was also discussed in Moscow at the 1999 G8 Ministerial Conference on Combating Transnational Organized Crimes.[2386] One of the outcomes of the meeting was a collection of principles regarding transborder access.[2387] This was in all likelihood the model for the regulation used by the drafters of the Convention on Cybercrime, and therefore shows similarities.

> *6. Transborder Access to Stored Data not Requiring Legal Assistance*
> *Notwithstanding anything in these Principles, a State need not obtain authorization from another State when it is acting in accordance with its national law for the purpose of:*
>
> *(a) accessing publicly available (open source) data, regardless of where the data is geographically located*
>
> *(b) accessing, searching, copying, or seizing data stored in a computer system located in another State, if acting in accordance with the lawful and voluntary consent of a person who has the lawful authority to disclose to it that data. The searching State should consider notifying the searched State, if such notification is permitted by national law and the data reveals a violation of criminal law or otherwise appears to be of interest to the searched State.*

The main difference is the notification procedure in 6 (b). The intention of the provision is intelligence sharing. However, with slight modifications, such a provision could ensure that affected states are aware of investigations taking place in their own territory. It would not prevent conflict with international law, but at least guarantee a certain degree of transparency.

### 24/7 Network of contacts

Cybercrime investigations often require immediate reaction.[2388] As explained above, this is especially the case when it comes to the traffic data that are necessary to identify a suspect, as they are often deleted within a rather short period of time.[2389] To increase the speed of international investigations, the Convention on Cybercrime highlights the importance of enabling the use of expedited means of communication in Article 25. In order to further improve the efficiency of mutual assistance requests, the drafters of the Convention on Cybercrime oblige the parties to designate a contact point for mutual assistance requests, who shall be available without time limitations.[2390] The drafters of the Convention on Cybercrime emphasized that establishment of the points of contact is one of the most important instruments provided by the Convention.[2391] However, a recent review of the use of 24/7 network points in countries that have ratified the Convention on Cybercrime shows that its use is very limited.

***Article 35 – 24/7 Network***

*1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:*

*a. the provision of technical advice;*

*b. the preservation of data pursuant to Articles 29 and 30;*

*c. the collection of evidence, the provision of legal information, and locating of suspects.*

*2a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.*

*b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.*

*3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.*

The idea of the 24/7 Network is based on the existing network for 24-hour contacts for International High-Tech and Computer-related Crime from the G8 Group of Nations.[2392] With the creation of a network of 24/7 contact points, the drafters of the Convention on Cybercrime aim to address the challenges of fighting cybercrime – especially those associated with the speed of data exchange processes[2393] and having an international dimension.[2394] The parties to the Convention on Cybercrime are obliged to establish such contact points and ensure that they are able to carry out certain immediate action, as well as maintain the service. As stated in Article 35 paragraph 3 of the Convention, this includes trained and equipped personnel.

With regard to the process of establishing the contact point and especially to the fundamental principles of this structure, the Convention on Cybercrime allows the Member States maximum flexibility. The Convention neither requires the creation of a new authority, nor defines to which of the existing authorities the contact point could or should be attached. The drafters of the Convention on Cybercrime further pointed out that the fact that the 24/7 network point is intended to provide technical as well as legal assistance will lead to various possible solutions regarding its implementation.

With regard to cybercrime investigations, the installation of the contact points has two main functions, namely speeding up communication by providing a single point of contact; and speeding up investigations by authorizing the contact point to carry out certain investigations right away. The combination of both functions has the potential to converge the speed of international investigations to the level reached within national investigations.

Article 32 of the Convention on Cybercrime defines the minimum required abilities of the network point. Apart from technical assistance and the provision of legal information, the main tasks of the contact point include the preservation of data, the collection of evidence and the locating of suspects.

In this context, it is again important to highlight that the Convention on Cybercrime does not prescribe which authority should be responsible for operating the 24/7 contact point. If the contact point is operated by an authority that has competence to order the preservation of data,[2395] and a foreign contact point requests such preservation, the measure can immediately be ordered by the local contact point. If the contact point is run by an authority that is not competent to order the preservation of data itself, it is important that the contact point shall have the ability to straight away contact the competent authorities to ensure that the measure is carried out immediately.[2396]

At the 2nd Meeting of the Cybercrime Convention Committee, it was explicitly pointed out that the participation in the 24/7 network of contacts does not require the signature or ratification of the Convention on Cybercrime.[2397]

In 2008, the Council of Europe published a study analysing the effectiveness of international cooperation against cybercrime.[2398] In 2009, a specific study on the functioning of 24/7 points of contact for cybercrime was undertaken.[2399] One result of the studies is that not all countries which have ratified the Convention on Cybercrime have created functioning 24/7 network points as required by the Convention. A second result is that countries which have established contact points often only use it for very limited purposes such as the preservation of traffic data.

### 6.6.6 International Cooperation in the Stanford Draft International Convention

The drafters of the Stanford Draft International Convention (the "Stanford Draft")[2400] recognized the importance of the international dimension of cybercrime and the related challenges. In order to address these challenges, they incorporated specific provisions that deal with international cooperation. The provisions cover the following topics:

- Article 6 – Mutual legal assistance
- Article 7 – Extradition
- Article 8 – Prosecution
- Article 9 – Provisional remedies
- Article 10 – Entitlements of an accused person
- Article 11 – Cooperation in law enforcement

This approach shows a number of similarities to the approach taken in the Council of Europe Convention on Cybercrime. The main difference is the fact that the regulations provided by the Convention on Cybercrime are stricter, more complex and more precisely defined compared to the Stanford Draft. As pointed out by the drafters of the Stanford Draft, the approach of the Convention on Cybercrime is more practical and therefore has some clear advantages in terms of actual application.[2401] The drafters of the Stanford Draft decided to follow a different approach, as they predicted that the implementation of new technology could lead to some difficulties. As a result, they only provided some general instructions without specifying them further.[2402]

## 6.7 Liability of Internet providers

**Bibliography (selected):** *Black*, Internet Architecture: An Introduction to IP Protocols, 2000; *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf; *Luotonen*, Web Proxy Servers, 1997; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Naumenko*, Benefits of Active Caching in the WWW, available at: www.epfl.ch/Publications/Naumenko/Naumenko99.pdf; *Schwartz*, Thinking outside the Pandora's box: Why the DMCA is unconstitutional under Article I, § 8 of the United States Constitution, Journal of Technology Law and Policy, Vol. 10, Issue 1, available at: http://grove.ufl.edu/~techlaw/vol10/issue1/schwartz.html; *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf; *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Walker*, Application of the DMCA Safe Harbor Provisions to Search Engines, Virginia Journal of Law and Technology, Vol. 9, 2004, available at:

www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003.

### 6.7.1 Introduction

Committing a cybercrime automatically involves a number of people and businesses, even if the offender acts alone. Due to the structure of the Internet, the transmission of a simple e-mail requires the service of a number of providers.[2403] In addition to the e-mail provider, the transmission involves access providers as well as routers who forward the e-mail to the recipient. The situation is similar for the downloading of movies containing child pornography. The downloading process involves the content provider who uploaded the pictures (for example on a website), the hosting provider who provided the storage media for the website, the routers who forwarded the files to the user, and finally the access provider who enabled the user to access the Internet.

Because of this involvement by multiple parties, Internet service providers have long since been at the centre of criminal investigations involving offenders who use the ISPs' services to commit an offence.[2404] One of the main reasons for this development is that, even when the offender is acting from abroad, the providers located within the country's national borders are a suitable subject for criminal investigations without violating the principle of national sovereignty.[2405]

The fact that, on the one hand, cybercrime cannot be committed without the involvement of providers, and, on the other hand, providers often do not have the ability to prevent these crimes, has led to the question whether the responsibility of Internet providers needs to be limited.[2406] The answer to the question is critical for economic development of the ICT infrastructure. Providers will only operate their services if they are able to avoid criminalization within their regular mode of operation. In addition, law-enforcement agencies also have a keen interest in this question. The work of law-enforcement agencies very often depends on cooperation of, and with, Internet providers. This raises some concern, since limiting the liability of Internet providers for acts committed by their users could have an impact on the ISPs' cooperation and support for cybercrime investigations, as well as on the actual prevention of crime.

### 6.7.2 The United States approach

There are different approaches taken to balance the need for actively involving providers in the investigations on the one hand, and limiting the risks of criminal liability for third parties action on the other.[2407] An example of a legislative approach can be found in 17 USC. §§ 517(a) and (b).

***§ 512. Limitations on liability relating to material online***
***(a) Transitory Digital Network Communications***
*A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if –*

*(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;*

*(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;*

*(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;*

*(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and*

*(5) the material is transmitted through the system or network without modification of its content.*

***(b) System Caching***

*(1) Limitation on liability.– A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which –*

*(A) the material is made available online by a person other than the service provider;*

*(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and*

*(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A),*

*if the conditions set forth in paragraph (2) are met.*

*[…]*

This provision is based on the Digital Millennium Copyright Act (DMCA) which was signed into law in 1998.[2408] By creating a safe-harbour regime, DMCA excluded the liability of providers of certain services for copyright violations by third parties.[2409] In this context, it is first of all important to highlight that not all providers are covered by the limitation.[2410] The limitation of liability is only applicable to service providers[2411] and caching providers.[2412] In addition, it is important to point out that the liability is linked to certain requirements. With regard to service providers, the requirements are that:

- the transmission of the material was initiated by or at the direction of a person other than the service provider;
- the transmission is carried out through an automatic technical process without selection of the material by the service provider;
- the service provider does not select the recipients of the material;
- no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients.

Another example of a limitation of the responsibility of Internet providers can be found in 47 USC. § 230(c), which is based on the Communications Decency Act[2413]:

*§ **230. Protection for private blocking and screening of offensive material***

*[…]*

***(c) Protection for "Good Samaritan" blocking and screening of offensive material***

*(1) Treatment of publisher or speaker*

*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.*

*(2) Civil liability*

*No provider or user of an interactive computer service shall be held liable on account of –*

*(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or*

*(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).*

*[…]*

What both approaches, i.e. 17 USC. § 512(a) as well as 47 USC. § 230(c), have in common is that they focus on liability with regard to special groups of providers and special areas of law. The remaining part of

this chapter will therefore give an overview of the legislative approach adopted by the European Union, which follows a broader concept.

### 6.7.3 European Union Directive on Electronic Commerce

An example of a legislative approach to regulate the liability of Internet providers is the European Union's E-Commerce Directive.[2414] Faced with the challenges stemming from the international dimension of the Internet, the drafters of the Directive decided to develop legal standards that provide a legal framework for the overall development of the information society, and thereby support overall economic development as well as the work of law-enforcement agencies.[2415] The regulation regarding liability is based on the principle of graduated responsibility.

The Directive contains a number of provisions that limit the liability of certain providers.[2416] The limitations are linked to the different categories of services operated by the provider.[2417] In all other cases liability is not necessarily excluded, and unless liability is limited by other regulations, the actor is fully liable. The motivation of the Directive is to limit liability in those cases where the provider has only limited possibilities to prevent the crime. The reasons for the limited possibilities may be technical. The routers are for example – without a significant loss of speed – unable to filter the data passing through them and hardly able to prevent data-exchange processes. Hosting providers have the ability to remove data if they become aware of criminal activities. However, like the routers, the big hosting providers are unable to control all data stored on their servers.

Having regard to the varying ability to actually control criminal activities, the liability of hosting and access providers is different. In this respect, it needs to be taken into consideration that the balance of the Directive is based on current technical standards. At the moment no tools are available that can automatically detect unknown pornographic images. If technical development continues in this area it could become necessary to evaluate the technical ability of providers in the future and, if necessary, adjust the system.

### 6.7.4 Liability of access provider (European Union Directive on Electronic Commerce)

Article 12 to 15 define the degree of the limitation of liability of the different providers. Based on Article 12, the liability of access providers and router operators is completely excluded as long as they comply with the three conditions stipulated in Article 12. As a consequence, the access provider is in general not responsible for criminal offences committed by its users. This full exclusion of liability does not release the provider from the obligation to prevent further offences if ordered by a court or administrative authority.[2418]

***Section 4: Liability of intermediary service providers***
***Article 12***
***"Mere conduit"***
*1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:*

*(a) does not initiate the transmission;*

*(b) does not select the receiver of the transmission; and*

*(c) does not select or modify the information contained in the transmission.*

*2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.*
*3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.*

The approach is comparable to 17 USC. § 512(a).[2419] Both regulations aim to specify the liability of service providers and both regulations link the limitation of liability to similar requirements. The main difference is the fact that the application of Article 12 of the EU E-Commerce Directive is not limited to copyright violations but excludes liability with regard to any kind of offence.

### 6.7.5 Liability for caching (European Union Directive on Electronic Commerce)

The term "caching" is in this context used to describe the storage of popular websites on local storage media in order to reduce bandwidth and make access to data more efficient.[2420] One technique used to reduce bandwidth is the installation of proxy servers.[2421] Within this scope, a proxy server may service requests without contacting the specified server (the domain name entered by the user) by retrieving content saved on local storage media from a previous request. The drafters of the Directive recognized the economic importance of caching and decided to exclude liability for automatic temporary storage if the provider complies with the conditions stipulated in Article 13. One of the conditions is that the provider complies with widely recognized standards regarding the updating of the information.

***Article 13***
***"Caching"***
*1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:*

*(a) the provider does not modify the information;*

*(b) the provider complies with conditions on access to the information;*

*(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;*

*(d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and*

*(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.*

*2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.*

Article 13 of the European Union E-Commerce Directive is another example of similarities between the dogmatic structure of the US and European approaches. The EU approach is comparable to 17 USC. § 512(b).[2422] Both regulations aim to specify the liability of caching providers and both regulations link the limitation of liability to similar requirements. With regard to the liability of service providers[2423], the main difference between the two approaches is the fact that the application of Article 13 of the EU E-Commerce Directive is not limited to copyright violations but excludes liability with regard to any kind of offence.

### 6.7.6 Liability of Hosting Provider (European Union Directive)

Especially with regard to illegal content, the hosting provider has an important function within the perpetration of the offence. Offenders who are making illegal content available online do not generally store them on their own servers. Most websites are stored on servers that are made available by hosting providers. Anyone who would like to run a webpage can rent storage capacity from a hosting provider to store the website. Some providers even offer ad-sponsored webspace free of charge.[2424]

The identification of illegal content is a challenge for the hosting provider. Especially for popular providers with many websites, manual searches for illegal content on such a great number of websites would be

impossible. As a result, the drafters of the Directive decided to limit the liability of hosting providers. However, unlike in the case of the access provider, the liability of the host provider is not excluded. As long as the host provider has no actual knowledge of illegal activities or illegal content stored on its servers, it is not liable. Here, an assumption that illegal content could be stored on the servers is not considered equivalent to actually having knowledge of the matter. If the provider obtains concrete knowledge about illegal activities or illegal content, it can only avoid liability if it immediately removes the illegal information.[2425] Failure to react immediately will lead to liability of the hosting provider.[2426]

***Article 14***
***Hosting***
*1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:*

*(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or*

*(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.*

*2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.*
*3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.*

Article 14 is not only applicable for providers which limit their services to renting technical data-storage infrastructure. Popular Internet services like the auction platforms offer hosting services, too.[2427]

### 6.7.7 Liability of hosting provider (HIPCAR)

Another approach to the liability of hosting providers can be found in the legislative text developed by the beneficiary states within the HIPCAR initiative.[2428]

***Hosting Provider***
***30*** *(1) A hosting provider is not criminally liable for the information stored at the request of a user of the service, on condition that:*

*(a) the hosting provider expeditiously removes or disables access to the information after receiving an order from any public authority or court of law to remove specific illegal information stored; or*

*(b) the hosting provider, upon obtaining knowledge or awareness about specific illegal information stored by other ways than an order from a public authority, expeditiously informs a public authority to enable them to evaluate the nature of the information and if necessary issue an order to remove the content.*

*(2) Paragraph 1 shall not apply when the user of the service is acting under the authority or the control of the hosting provider.*
*(3) If the hosting provider is removing the content after receiving an order pursuant to paragraph 1 he is exempted from contractual obligations with his customer to ensure the availability of the service.*

Just like the European Union approach, Section II, Part V, 30(1)a. limits liability if the hosting provider expeditiously removes content after receiving an order from any public authority or court. Expeditiously in general means within less than 24 hours.[2429] The main difference from the EU approach can be found in Section II, Part V, 30(1)b. Unlike under the EU approach, the provider does not to determine whether content that comes to its attention is considered illegal. If it receives knowledge, its obligation is first of all

limited to informing the (designated) public authority about the potentially illegal content. The drafters of the provision decided that it is those authorities which should determine the nature of the provision and issue an order to remove the content.[2430] If the information is considered illegal the provider needs to remove it to avoid liability.

### 6.7.8 Exclusion of the obligation to monitor (European Union Directive on Electronic Commerce)

Before the Directive was implemented it was uncertain in some Member States whether the providers could be prosecuted based on a violation of the obligation to monitor users' activities. Apart from possible conflicts with data-protection regulations and secrecy of telecommunications, such an obligation would especially cause difficulties for hosting providers which store thousands of websites. To avoid these conflicts, the Directive excludes a general obligation to monitor transmitted or stored information.

> ***Article 15***
> ***No general obligation to monitor***
> *1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.*
> *2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.*

### 6.7.9 Liability for hyperlinks (Austrian ECC)

Hyperlinks play in important role on the Internet. They enable the provider of the hyperlink to guide the user to specific information available online. Instead of just offering technical details on how the information can be accessed (e.g. by providing the domain name of the website where the information is offered), the user can directly access the information by clicking on the active hyperlink. The hyperlink provides the command for the web browser to open the deposited Internet address.

During the drafting of the European Union Directive, the need for a regulation on hyperlinks was intensively discussed.[2431] The drafters decided not to oblige the Member States to harmonize their laws regarding liability for hyperlinks. Instead, they implemented a re-examination procedure to ensure that the need for proposals concerning the liability of providers of hyperlinks and location tool services was taken into consideration.[2432] Until regulation of liability for hyperlinks is amended in the future, the Member States are free to develop national solutions.[2433] Some EU countries have decided to address the liability of hyperlink providers in a dedicated provision.[2434] These countries have based the liability of hyperlink providers on the same principles that the Directive provides with regard the liability of hosting providers.[2435] This approach is the logical consequence of the comparable situation of host and hyperlink providers. In both cases, the providers are in control of the illegal content, or at least the link to the content.

An example is section 17 of the Austrian ECC:[2436]

> ***Sec. 17 ECC*** *(Austria) – Liability for hyperlinks*
> *(1) A provider who enables the access to information provided by third person by providing an electronic link is not liable for the information if he*
> *1. does not have actual knowledge of unlawful activity or information and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful; or*
> *2. upon obtaining such knowledge or awareness, acts expeditiously to remove the electronic link.*

### 6.7.10 Liability of search engines

Search-engine providers offer search services to identify documents of interest by specifying certain criteria. The search engine will search for relevant documents that match the criteria entered by the user. Search engines play an import role in the successful development of the Internet. Content that is made available on a website but is not listed in the search engine's index can only be accessed if the person wishing to access it knows the complete URL. *Introna/Nissenbaum* points out that "without much exaggeration one could say that to exist is to be indexed by a search engine".[2437]

As in the case of hyperlinks, the European Union Directive does not contain standards defining the liability of search-engine operators. Therefore, some EU countries have decided to address the liability of search-engine providers in a dedicated provision.[2438] Unlike in the case of hyperlinks, not all countries have based their regulation on the same principles.[2439] Spain[2440] and Portugal have based their regulations regarding the liability of search-engine operators on Article 14 of the Directive, while Austria[2441] has based the limitation of liability on Article 12.

> ***Sec. 14 ECC*** *(Austria) – Liability of search engine operators*
> *(1) A provider who makes available a search engine or other electronic tools to search for information provided by third party is not liable on condition that the provider:*
> *1. does not initiate the transmission;*
> *2. does not select the receiver of the transmission; and*
> *3. does not select or modify the information contained in the transmission*

[1360] For an overview of legal approaches, see also: ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 18 *et seq.*, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1361] *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 253 et seq; *Lindahl,* Deduction and Justification in the Law. Role of Legal Terms and Conditions, Ratio Juris, Vol. 17, Iss. 2, 2004, page 182 et seq.

[1362] *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 255.

[1363] Four definitions are included in Art. 1 and an additional provision was included in Art. 9, Council of Europe Convention on Cybercrime.

[1364] For more information related to legal approaches regulating the liability of access provider see below: § 6.7.4

[1365] With regard to the lawful interception of communication see below: § 6.5.9.

[1366] With regard to the liability of caching provider see below: § 6.7.5.

[1367] For more details related to different legal approaches to criminalize child pornography see below: § 6.2.8.

[1368] With regard to the criminalization of such conduct see below: § 6.2.7.

[1369] Art. 2(a) European Union Directive on combating the sexual abuse and sexual exploitation of children and child pornography, 2011/92/EU.

[1370] Art. 3(a) Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, ETS 201.

[1371] Sec. 3(3) HIPCAR Model Legislative Text on Cybercrime.

[1372] With regard to details of the criminalization see below: § 6.2.8.

[1373] For an overview of the legal age of consent and child pornography in selected countries, see: Prevention of Child Pornography, LC Paper No. CB(2)299/02-03(03), available at: www.legco.gov.hk/yr01-02/english/bc/bc57/papers/bc571108cb2-299-3e.pdf.

[1374] See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

[1375] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 104.

[1376] *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

[1377] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1378] Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model-Policy-Guidelines-and-Legislative-Text_Cybercrime.pdf.

[1379] Art. 2(c) European Union Directive on combating the sexual abuse and sexual exploitation of children and child pornography, 2011/92/EU.

[1380] Art. 20(2) Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, ETS 201.

[1381] With regard to different approaches to criminalize data interference see below: § 6.2.5.

[1382] Regarding the criminalization of data espionage/illegal data acquisition see below: § 6.2.3.

[1383] Art. 1(b) Council of Europe Convention on Cybercrime, ETS 185.

[1384] Art. 1(b) EU Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[1385] Art. 1 Draft ECOWAS Directive on Fighting Cyber Crime.

[1386] Sec. 3(5) HIPCAR Model Legislative Text on Cybercrime.

[1387] Sec.3 (7) HIPCAR Model Legislative Text.

[1388] *Stair/Reynolds/Reynolds*, Fundamentals of Information Systems, 2008, page 167; *Weik*, Computer science and communications dictionary, 2000, page 826; *Stair/Reynolds*, Principles of Information Systems, 2011, page 15.

[1389] Art. 1(a) Council of Europe Convention on Cybercrime, ETS 185.

[1390] Art. 1(a) EU Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. The Framework Decision uses the term „information" system instead of computer system.

[1391] Art. 1 Draft ECOWAS Directive on Fighting Cyber Crime.

[1392] Sec. 3(4) HIPCAR Model Legislative Text on Cybercrime.

[1393] Regarding attacks against critical infrastructure see above: § 1.2

[1394] Regarding the related challenges see above: § 3.2.14.

[1395] With regard to the legal response see below: § 6.5.11.

[1396] Draft African Union Convention on the Establishment of a credible Legal Framework for Cyber Security in Africa, Version 1, January 2011.

[1397] See below: § 6.2.15.

[1398] See Art. 10 (1)(a) HIPCAR Model Legislative Text on Cybercrime.

[1399] See below: § 6.2.6.

[1400] With regard to the liability of different types of provider see below: § 6.7.

[1401] Regarding the liability of search engines see below: § 6.7.10.

[1402] With regard to illegal interception, see below: § 6.2.4.

[1403] For more details related to the interference with computer data see below: § 6.2.5.

[1404] With regard to system interference see below: § 6.2.6.

[1405] See in this regard below: § 6.2.14.

[1406] See below: § 6.5.12.

[1407] Regarding the different legal approaches to seize evidence see below: § 6.5.6.

[1408] See in this regard Art. 19 (3) Council of Europe Convention on Cybercrime.

[1409] Sec. 3 Commonwealth Model Law on Computer and Computer-related Crime.

[1410] Sec. 3(17) HIPCAR Model Legislative Text on Cybercrime.

[1411] See below: § 6.5.9.

[1412] Art. 1 Council of Europe Convention on Cybercrime.

[1413] Sec. 3(18) HIPCAR Model Legislative Text on Cybercrime.

[1414] *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 *et seq.*

[1415] These range from the simple proof that technical protection measures can be circumvented, to the intent to obtain data stored on the victim computer. Even political motivations have been discovered. See: *Anderson*, Hacktivism and Politically Motivated Computer Crime, 2005, available at: www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf.

[1416] Regarding the independence of place of action and the location of the victim, see above § 3.2.7.

[1417] These can, for example, be passwords or fingerprint authorization. In addition, there are several tools available that can be used to circumvent protection measures. For an overview of potential tools, see *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

[1418] Regarding the supportive aspects of missing technical protection measures, see *Wilson*, Computer Attacks and Cyber Terrorism, Cybercrime & Security, IIV-3, page 5. The importance of implementing effective security measures to prevent illegal access is also highlighted by the drafters of the Convention on Cybercrime. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 45.

[1419] *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 729.

[1420] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 44. "The need for protection reflects the interests of organizations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner".

[1421] With regard to data espionage, see above, § 2.5.2 and below, § 6.1.3.

[1422] With regard to data interference, see above, § 2.5.4 and below, § 6.1.5.

[1423] *Sieber*, Informationstechnologie und Strafrechtsreform, page 49 *et seq.*

[1424] For an overview of the various legal approaches in criminalizing illegal access to computer systems, see *Schjolberg*, The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003, available at: www.mosstingrett.no/info/legal.html.

[1425] Art. 2 of the Convention on Cybercrime enables the Member States to keep those existing limitations that are mentioned in Art. 2, sentence 2. Regarding the possibility of limiting criminalization, see also: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 40.

[1426] An example of this is the German Criminal Code, which criminalized only the act of obtaining data (Section 202a). This provision was changed in 2007. The following text presents the old version:

> *Section 202a – Data Espionage*
> *(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.*
> *(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.*

[1427] This approach is not only found in national legislation, but was also recommended by Council of Europe Recommendation No. (89) 9.

[1428] For an overview of the various legal approaches in criminalizing illegal access to computer systems, see *Schjolberg*, The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003, available at: www.mosstingrett.no/info/legal.html.

[1429] Regarding the system of reservations and restrictions, see *Gercke*, The Convention on Cybercrime, Computer Law Review International, 2006, 144.

[1430] *Gercke*, Cybercrime Training for Judges, 2009, page 27, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1431] With regard to software tools that are designed and used to carry out such attacks, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf. With regard to Internet-related social engineering techniques, see the information offered by the anti-phishing working group, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

[1432] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

[1433] The relevance of attacks by insiders is highlighted by the 2007 CSI Computer Crime and Security Survey. The survey notes that 5 per cent of the respondents reported that 80-100 per cent of their losses were caused by insiders. Nearly 40 per cent of all respondents reported that between 1 per cent and 40 per cent of the losses related to computer and network crimes were caused by insiders. For more details, see: 2007 CSI Computer Crime and Security Survey, page 12, available at: www.gocsi.com/.

[1434] Reservations and restrictions are two possibilities of adjusting the requirements of the Convention to the requirements of individual national legal systems.

[1435] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

[1436] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1437] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1438] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self-defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1439] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47.

[1440] *Jones*, Council of Europe Convention on Cybercrime: Themes and Critiques, page 7.

[1441] See for example: World Information Technology And Services Alliance (WITSA), Statement On The Council Of Europe Draft Convention On Cybercrime, 2000, available at: www.witsa.org/papers/COEstmt.pdf. Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

[1442] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47, and Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62 (dealing with Article 4).

[1443] *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

[1444] This is especially relevant for phishing cases. See in this context: *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4.

[1445] *Gercke*, Cybercrime Training for Judges, 2009, page 28, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1446] Article 42 – Reservations: By a written notification addressed to the Secretary-General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

[1447] This limits the criminalization of illegal access to those cases where the victim used technical protection measures to protect its computer system. Access an unprotected computer system would therefore not be considered a criminal act.

[1448] The additional mental element/motivation enables Member States to undertake a more focused approach rather than implementing a criminalization of the mere act of hacking. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47, and Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62.

[1449] This enables Member States to avoid a criminalization of cases where the offender had physical access to the computer system of the victim and therefore did not need to perform an Internet-based attack.

[1450] Framework Decision on Attacks against Information Systems – 19 April 2002 – COM (2002) 173. For more details, see above: § 5.2.1.

[1451] Article 2 – Illegal access to information systems:
1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases that are not minor.
2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.

[1452] Model Law on Computer and Computer Related Crime, LMM(02)17, available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1453] See the explanation of the Council Framework Decision 2005/222/JHA, 1.6.

[1454] Council Framework Decision 2005/222/JHA (13).

[1455] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cybercrime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1456] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1457] See *Sofaer/Goodman/Cuellar/Drozdova and others*. A Proposal for an International Convention on Cybercrime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1458] In this context, "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

[1459] Standalone computer systems are covered by Art. 1, paragraph 3, of the Draft Convention because they "control programs". This does not require a network connection.

[1460] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1461] Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1462] The Explanatory Report points out that the provision intends to criminalize violations of the right of privacy of data communication. See the Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

[1463] See below: § 6.1.4.

[1464] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 730.

[1465] One key indication of the limitation of application is the fact that the Explanatory Report compares the solution in Art. 3 to traditional violations of the privacy of communication beyond the Internet, which do not cover any form of data espionage. *"The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights."* See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

[1466] See in this context especially a recent case from Hong Kong, People's Republic of China. See above: § 2.5.2.

[1467] ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1468] Regarding the challenges related to the use of encryption technology by offenders, see above: § 3.2.14; *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf; *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf; *Flamm*, Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography, available at: www.terrorismcentral.com/Library/Teasers/Flamm.html. Regarding the underlying technology, see: *Singh*, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

[1469] One of the consequences related to this aspect is the fact that limitation of the criminalization of illegal access to those cases where the victim of the attack secured the target computer system with technical protection measures could limit the application of such a provision, insofar as a large number of users do not have sufficient knowledge about the implementation of technical protection measures.

[1470] Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489 (1996). See in this context: *Chamblee*, Validity, Construction, and Application of Title I of Economic Espionage Act of 1996 (18 U.S.C.A. §§ 1831 *et seq.*), 177 A.L.R. Fed. 609 (2002); *Fischer*, An Analysis of the Economic Espionage Act of 1996, 25 Seton Hall Legis. J. 239 (2001).

[1471] *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81, page 986, available at: http://weblaw.usc.edu/why/students/orgs/lawreview/documents/Decker_Charlotte_81_5.pdf.

[1472] For details, see: US CCIPS, Prosecuting Intellectual Property Crimes, 3rd Edition, 2006, page 138 *et seq.* available at: www.justice.gov/criminal/cybercrime/ipmanual/04ipma.pdf.

[1473] *Loundy*, Computer Crime, Information Warfare, and Economic Espionage, 2009, page 55 *et seq.*; *Krotosi,* Identifying and Using Evidence Early To Investigate and Prosecute Trade Secret and Economic Espionage Act Cases, Economic Espionage and Trade Secrets, 2009, Vol. 75, No. 5, page 41 *et seq.* available at: www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf.

[1474] *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81, page 988, available at: http://weblaw.usc.edu/why/students/orgs/lawreview/documents/Decker_Charlotte_81_5.pdf.

[1475] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1476] The document is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1477] Explanatory Notes to the Model Legislative Text on Cybercrime, 2010. The document is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1478] This provision has recently been modified and now even criminalizes illegal access to data. The previous version of the provision has been used here, because it is better suited for demonstrating the dogmatic structure.

[1479] See *Hoyer* in SK-StGB, Sec. 202a, Nr. 3.

[1480] A similar approach of limiting criminalization to cases where the victim did not take preventive measures can be found in Art. 2, sentence 2, Convention on Cybercrime: *A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.* For more information, see above: § 6.1.1.

[1481] This provision is therefore an example for of a legislative approach that should not substitute for, but rather complement, self-protection measures.

[1482] See in this context for example a recent case in Hong Kong: *Watts,* Film star sex scandal causes internet storm in China, The Guardian, 12.02.2008, available at: www.guardian.co.uk/world/2008/feb/12/china.internet; *Tadros*, Stolen photos from laptop tell a tawdry tale, The Sydney Morning Herald, 14.02.2008, available at: www.smh.com.au/news/web/stolen-photos-from-laptop-tell-a-tawdry-tale/2008/02/14/1202760468956.html; *Pomfret*, Hong Kong's Edision Chen quits after sex scandal, Reuters, 21.02.2008, available at: www.reuters.com/article/entertainmentNews/idUSHKG36060820080221?feedType=RSS&feedName=entertainmentNews; *Cheng*, Edision Chen is a celebrity, Taipei Times, 24.02.2008, available at: www.taipeitimes.com/News/editorials/archives/2008/02/24/2003402707.

[1483] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

[1484] With regard to "phishing", see above: § 2.9.4 and below: § 6.1.15 and as well: *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Phishing, Computer und Recht, 2005, 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

[1485] Regarding the risks related to the use of wireless networks, see above: § 3.2.3. Regarding the difficulties in cybercrime investigations that include wireless networks, see *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime in Cybercrime & Security, IIA-2; *Urbas/Krone*, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: www.aic.gov.au/publications/tandi2/tandi329t.html.

[1486] Regarding the architecture of the Internet, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

[1487] Regarding the underlying technology and the security related issues, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: www.infodev.org/en/Document.18.aspx. With regard to the advantages of wireless networks for the development of ICT infrastructure in developing countries, see: The Wireless Internet Opportunity for Developing Countries, 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

[1488] The computer magazine ct reported in 2004 that field tests proved that more than 50 per cent of 1 000 wireless computer networks that were tested in Germany were not protected. See: www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/48182.

[1489] Regarding the impact of encryption of wireless communication, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: www.infodev.org/en/Document.18.aspx.

[1490] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1491] Regarding identity theft, see above: § 2.8.3 and below: § 6.1.16 and also: Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys, see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Lee*, Identity Theft Complaints Double in '02, New York Times, Jan. 22, 2003; *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf. For an approach to divide between four phases, see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[1492] In the United States, the SSN was created to keep an accurate record of earnings. Contrary to its original intentions, the SSN is today widely used for identification purposes. Regarding offences related to social-security numbers, see: *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350.

[1493] See: *Hopkins*, Cybercrime Convention: A Positive Beginning to a Long Road Ahead, Journal of High Technology Law, 2003, Vol. II, No. 1, page 112.

[1494] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

[1495] The Explanatory Report describes the technical means more in detail: "Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalization." Explanatory Report to the Council of Europe Convention on Cybercrime, No. 53.

[1496] Within this context, only interceptions made by technical means are covered by the provision – Article 3 does not cover acts of "social engineering".

[1497] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 730.

[1498] *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1499] See above: § 6.1.3.

[1500] "The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example) between two computer systems belonging to the same person, two computers communicating with one another or a computer and a person (e.g. through the keyboard)." Explanatory Report to the Council of Europe Convention on Cybercrime, No. 55.

[1501] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 53.

[1502] Covered by Article 3 is the interception of electronic emissions that are produced during the use of a computer. Regarding this issue, see Explanatory Report, No. 57: *"The creation of an offence in relation to "electromagnetic emissions" will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as "data" according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from a computer system is included as an offence under this provision"*, Explanatory Report to the Council of Europe Convention on Cybercrime, No. 57.

[1503] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

[1504] *Gercke*, Cybercrime Training for Judges, 2009, page 29, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1505] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 54.

[1506] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1507] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1508] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1509] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

[1510] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

[1511] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

[1512] Cookies are data sent by a server to a browser and then sent back each time the browser is used to access the server. Cookies are used for authentication, tracking and keeping user information. Regarding the functions of cookies and the controversial legal discussion, see: *Kesan/Shah*, Deconstruction Code, Yale Journal of Law & Technology, 2003-2004, Vol. 6, page 277 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=597543.

[1513] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

[1514] Model Law on Computer and Computer Related Crime" LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1515] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more

information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1516] The difficulty with offences against the integrity of data is that identification of these violations is often difficult to prove. Therefore, the Expert Group which drafted the Convention on Cybercrime identified the possibility of prosecuting violations regarding data interference by means of criminal law as a necessary strategic element in the fight against cybercrime. Explanatory Report to the Council of Europe Convention on Cybercrime, No. 60.

[1517] The 2007 Computer Economics Malware Report focuses on computer crime and analyses the impact of malware on the worldwide economy by summing up the estimated costs caused by attacks. It identified peaks in 2000 (USD 17.1 billion) and 2004 (USD 17.5 billion). For more information, see: 2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other malicious Code. A summary of the report is available at: www.computereconomics.com/article.cfm?id=1225.

[1518] A number of computer fraud scams are including the manipulation of data – e.g. the manipulation of bank-account files, transfer records or data on smart cards. Regarding computer related fraud scams, see above: § 2.8.1 and below: § 6.1.17.

[1519] Regarding the problems related to these gaps, see for example the LOVEBUG case, where a designer of a computer worm could not be prosecuted due to the lack of criminal law provisions related to data interference. See above: § 2.5.4 and: CNN, Love Bug virus raises spectre of cyberterrorism, 08.05.2000, http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; *Chawki*, A Critical Look at the Regulation of Cybercrime, www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 10, available at: http://media.hoover.org/documents/0817999825_1.pdf; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1520] A similar approach to Art. 4 of the Convention on Cybercrime is found in the EU Framework Decision on Attacks against Information Systems: Article 4 – Illegal data interference: "Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor".

[1521] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 60.

[1522] As pointed out in the Explanatory Report, the two terms overlap. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1523] Regarding the more conventional ways to delete files using Windows XP, see the information provided by Microsoft, available at: www.microsoft.com/windowsxp/using/setup/learnmore/tips/waystodelete.mspx.

[1524] Regarding the consequences for forensic investigations, see: *Casey*, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 *et seq.*, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[1525] See *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/05hb003.pdf.

[1526] The fact that the Explanatory Report mentions that the files are unrecognizable after the process does not give any further indication with regard to the interpretation of the term. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1527] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1528] A denial-of-service (DoS) attacks aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at:

www.cert.org/archive/pdf/DoS_trends.pdf. In 2000 a number of well-known US e-commerce businesses were targeted by DoS attacks. A full list is provided by *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

[1529] With regard to the criminalization of DoS attacks, see also below: § 6.1.6.

[1530] In addition, criminalization of DoS attacks is provided by Art. 5 of the Convention on Cybercrime. See below: § 6.1.6.

[1531] Apart from the input of malicious codes (e.g. viruses and trojan horses), it is likely that the provision could cover unauthorized corrections of faulty information as well.

[1532] *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf. Regarding the different recognized functions of malicious software, see above: § 2.5.4. Regarding the economic impact of malicious software attacks, see above: § 2.5.4.

[1533] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1534] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1535] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report states: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1536] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62: "The modification of traffic data for the purpose of facilitating anonymous communications (e.g., the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g., encryption), should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right." Regarding the liability of Remailer, see: *Du Pont*, The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

[1537] For further information, see *du Pont*, The Time Has Come For Limited Liability For Operators Of True Anonymity Remailers In Cyberspace: An Examination Of The Possibilities And Perils, Journal Of Technology Law & Policy, Vol. 6, Issue 2, page 176 *et seq.*, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

[1538] With regard to the possible difficulties to identify offenders who have made use of anonymous or encrypted information, the Convention leaves the criminalization of anonymous communications open to the parties to decide on – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62.

[1539] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[1540] For further information, see: *Gercke*, The EU Framework Decision on Attacks against Information Systems, Computer und Recht 2005, page 468 *et seq.*

[1541] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1542] Sec. 5 (Illegal access), Sec. 8 (Illegal interception) and Sec. 10 (Child pornography).

[1543] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cybercrime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf.
For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1544] ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 33, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1545] A denial-of-service (DoS) attack aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see above: § 2.5.4 and US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

[1546] For an overview of successful attacks against famous Internet companies, see: *Moore/Voelker/Savage*, Inferring Internet Denial-of-Service Activities, page 1, available at: www.caida.org/papers/2001/BackScatter/usenixsecurity01.pdf; CNN News, One year after DoS attacks, vulnerabilities remain, at: http://edition.cnn.com/2001/TECH/internet/02/08/ddos.anniversary.idg/index.html. *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

[1547] Regarding the possible financial consequences of lack of availability of Internet services due to attack, see: Campbell/Gordon/Loeb/Zhou, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, pages 431-448.

[1548] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. Regarding cyberterrorism, see above § 2.9.1 and *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, Cyberterrorism and Cybersecurity, available at: www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in *Arquilla/Ronfeld*t, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45 page 1033 *et seq.*; United States Department of State, Pattern of Global Terrorism, 2000, in: *Prados*, America Confronts Terrorism, 2002, 111 *et seq.*; *Lake*, 6 Nightmares, 2000, page 33 et *seq.*; *Gordon*, Cyberterrorism, available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; United States

National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, 2003, page 11 *et seq.* OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf; *Sofaer*, The Transnational Dimension of Cybercrime and Terrorism, pages 221-249.

[1549] The protected legal interest is the interest of operators as well as users of computer or communication systems being able to have them function properly. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 65.

[1550] *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1551] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

[1552] The Explanatory Report gives examples for implementation of restrictive criteria for serious hindering: "Each Party shall determine for itself what criteria must be fulfilled in order for the hindering to be considered "serious." For example, a Party may require a minimum amount of damage to be caused in order for the hindering to be considered serious. The drafters considered as "serious" the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g. by means of programs that generate "denial-of-service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system)" – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 67.

[1553] *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf. Although the connotation of "serious" does limit the applicability, it is likely that even serious delays to operations resulting from attacks against a computer system can be covered by the provision.

[1554] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

[1555] Examples are the use of networks (wireless or cable networks), bluetooth or infrared connection.

[1556] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61. Regarding the fact that the definition does not distinguish between the different ways how information can be deleted, see above: § 6.1.15. Regarding the impact of the different ways of deleting data on computer forensics, see: *Casey*, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 *et seq*., available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[1557] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1558] Apart from the input of malicious codes (e.g. viruses and trojan horses), it is therefore likely that the provision could cover unauthorized corrections of faulty information as well. .

[1559] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1560] "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: ITU Survey on Anti-Spam legislation worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. For more information, see above: § 2.5.g.

[1561] Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

[1562] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

[1563] Regarding legal approaches in the fight against spam, see above: § 6.1.l3.

[1564] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

[1565] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1566] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1567] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that*

*the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1568] See for example: World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

[1569] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 68: "The hindering must be "without right". Common activities inherent in the design of networks, or common operational or commercial practices are with right. These include, for example, the testing of the security of a computer system, or its protection, authorized by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such conduct is not criminalized by this article, even if it causes serious hindering."

[1570] Framework Decision on attacks against information systems – 19 April 2002 – COM (2002) 173.

[1571] Article 3 – Illegal system interference: "Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor".

[1572] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, § 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1573] Draft Convention on Cybercrime (Draft No. 19), European Committee On Crime Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), PC-CY (2000), 19, available at: www.iwar.org.uk/law/resources/eu/cybercrime.htm.

[1574] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/ documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1575] For an overview on hate speech legislation, see for example: the database provided at: www.legislationline.org. For an overview on other cybercrime-related legislation, see: the database provided at: www.cybercrimelaw.net.

[1576] Regarding the challenges of international investigation, see above: § 3.2.4 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1577] For details, see: *Wolters/Horn*, SK-StGB, Sec. 184, Nr. 2.

[1578] *Hoernle* in Muenchener Kommentar StGB, Sec. 184, No. 5.

[1579] Regarding the influence of pornography on minors, see: *Mitchell/Finkelhor/Wolak*, The exposure of youth to unwanted sexual material on the Internet – A National Survey of Risk, Impact, and Prevention, Youth & Society, Vol. 34, 2003, page 330 *et seq.*, available at: www.unh.edu/ccrc/pdf/Exposure_risk.pdf; *Brown*, Mass media influence on sexuality, Journal of Sex Research, February 2002, available at: http://findarticles.com/p/articles/mi_m2372/is_1_39/ai_87080439.

[1580] See Section 11 Subparagraph 3 Penal Code: "Audio and visual recording media, data storage media, illustrations and other images shall be the equivalent of writings in those provisions which refer to this subsection".

[1581] *Hoernle* in Muenchener Kommentar StGB, Sec. 184, No. 28.

[1582] The draft law was not in force by the time this publication was finalized.

[1583] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1584] Regarding the challenges of international investigation, see above: § 3.2.4. See also: *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1585] *Krone*, A Typology of Online Child Pornography Offending, Trends & Issues in Crime and Criminal Justice, No. 279; *Cox*, Litigating Child Pornography and Obscenity Cases, Journal of Technology Law and Policy, Vol. 4, Issue 2, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue2/cox.html#enIIB.

[1586] Regarding methods of distribution, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 10 *et seq.*, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729. Regarding the challenges related to anonymous communication, see above: § 3.2.14.

[1587] It has been reported that some websites containing child pornography register up to a million hits per day. For more information, see: *Jenkins*, Beyond Tolerance: Child Pornography on the Internet, 2001, New York University Press; *Wortley/Smallbone*, Child Pornography on the Internet, page 12, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

[1588] Regarding the challenges related to investigations involving anonymous communication technology, see above: § 3.2.l.

[1589] Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

[1590] *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999, page 68.

[1591] *Liu*, Ashcroft, Virtual Child Pornography and First Amendment Jurisprudence, UC Davis Journal of Juvenile Law & Policy, 2007, Vol. 11, page 6, available at: http://jjlp.law.ucdavis.edu/archives/vol-11-no-1/07%20Liu%2011.1.pdf.

[1592] *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999, page 69.

[1593] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 91.

[1594] *Akdeniz* in *Edwards/Waelde*, Law and the Internet: Regulating Cyberspace; *Williams* in *Miller*, Encyclopaedia of Criminology, page 7. Regarding the extent of criminalization, see: Child Pornography: Model Legislation & Global Review, 2006, available at: www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf. Regarding the discussion about the criminalization of child pornography and freedom of speech in the United States, see: *Burke*, Thinking Outside the Box: Child Pornography, Obscenity and the Constitution, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a11-Burke.pdf; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws in terms of the criminalization of child pornography.

[1595] Regarding differences in legislation, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 26, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

[1596] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 91.

[1597] *Walden*, Computer Crimes and Digital Investigations, 2006, page 144.

[1598] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 94.

[1599] Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse, ETS 201.

[1600] Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 135.

[1601] See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

[1602] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 95.

[1603] Regarding criminalization of the possession of child pornography in Australia, see: *Krone*, Does thinking make it so? Defining online child pornography possession offences, in "Trends & Issues in Crime and Criminal Justice", No. 299; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws regarding the criminalization of child pornography.

[1604] See: Child Pornography: Model Legislation & Global Review, 2006, page 2, available at: www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

[1605] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 98.

[1606] *Gercke*, Cybercrime Training for Judges, 2009, page 45, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_pdf.

[1607] Based on the National Juvenile Online Victimization Study, only 3 per cent of arrested Internet-related child-pornography possessors had morphed pictures. *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

[1608] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 102.

[1609] *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

[1610] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1611] Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1612] Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly Resolution 44/25 of 20 November 1989, entry into force 2 September 1990, in accordance with Article 49. Article 1. For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.

[1613] One example is the current German Penal Code. The term "child" is defined by law in Section 176 to which the provision related to child pornography refers: Section 176: "Whoever commits sexual acts on a person under fourteen years of age (a child) ...".

[1614] Council Framework Decision on combating the sexual exploitation of children and child pornography, 2004/68/JHA, available at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf.

[1615] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. 201, available at: http://conventions.coe.int.

[1616] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 104.

[1617] For an overview of the legal age of consent and child pornography in selected countries, see: Prevention of Child Pornography, LC Paper No. CB(2)299/02-03(03), available at: www.legco.gov.hk/yr01-02/english/bc/bc57/papers/bc571108cb2-299-3e.pdf.

[1618] See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

[1619] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1620] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1621] Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

[1622] *Gercke*, Cybercrime Training for Judges, 2009, page 46, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_pdf.

[1623] Regarding the challenges related to the use of encryption technology, see above: § 3.2.14. One survey on child pornography suggested that only 6 per cent of arrested child-pornography possessors used encryption technology. See: *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

[1624] See Explanatory Report to the Convention on the Protection of Children, No. 140.

[1625] The download is in general necessary to enable the display of the information on the website. Depending on the configuration of the browser, the information can be downloaded to cache and temp files or is just stored in the RAM memory of the computer. Regarding the forensic aspects of this download, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 180, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

[1626] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1627] Official Notes:
NOTE: The laws respecting pornography vary considerably throughout the Commonwealth. For this reason, the prohibition in the model law is limited to child pornography, which is generally the subject of an absolute prohibition in all member countries. However a country may wish to extend the application of this prohibition to other forms of pornography, as the concept may be defined under domestic law.
NOTE: The pecuniary penalty will apply to a corporation but the amount of the fine may be insufficient. If it is desired to provide a greater penalty for corporations, the last few lines of subsection (1) could read: "commits an offence punishable, on conviction:
(a) in the case of an individual, by a fine not exceeding [amount] or imprisonment for a period not exceeding [period]; or
(b) in the case of a corporation, by a fine not exceeding [a greater amount].

[1628] Official Note:
NOTE: Countries may wish to reduce or expand upon the available defences set out in paragraph 2, depending on the particular context within the jurisdiction. However, care should be taken to keep the defences to a minimum and to avoid overly broad language that could be used to justify offences in unacceptable factual situations.

[1629] See the preface to the Optional Protocol.

[1630] See Art. 2.

[1631] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1632] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1633] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1634] See in this regard: *Powell*, Paedophiles, Child Abuse and the Internet, 2007; *Eneman/Gillespie/Stahl*, Technology and Sexual Abuse: A Critical Review of an Internet Grooming Case, AISeL, 2010, available at: www.cse.dmu.ac.uk/~bstahl/index_html_files/2010_grooming_ICIS.pdf.

[1635] See: Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 155.

[1636] Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

[1637] Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 155.

[1638] Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 157.

[1639] Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 159.

[1640] International Mechanisms for Promoting Freedom of Expression, Joint Declaration, Challenges to Freedom of Expression in the New Century, by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2001.

[1641] For an overview of hate speech legislation, see the database provided at: www.legislationline.org.

[1642] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1643] Regarding the criminalization of hate speech in Europe, see: *Blarcum*, Internet Hate Speech, The European Framework and the Emerging American Haven, Washington and Lee Law Review, 2007, page 781 *et seq.* available at: http://law.wlu.edu/ deptimages/Law%20Review/62-2VanBlarcum.pdf. Regarding the situation in Australia, see: *Gelber/Stone*, Hate Speech and Freedom of Speech in Australia, 2007.

[1644] Vienna Summit Declaration, 1993, available at: www.coe.int/t/dghl/monitoring/ecri/archives/other_texts/2-vienna/plan_of_action/plan_of_action_vienna_summit_EN.asp.

[1645] Recommendation No. 1275 on the fight against racism, xenophobia, anti-Semitism and intolerance.

[1646] Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4: "The committee drafting the Convention discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention."

[1647] Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

[1648] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1649] Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

[1650] Regarding the list of states that signed the Additional Protocol, see above: § 5.2.1.

[1651] Regarding the difficulties related to the jurisdiction and the principle of freedom of expression, see also: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: www.coe.int/t/e/human_rights/ecri/1-EComputerLawReviewInternational/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ComputerLawReviewInternational(2000)27.pdf.

[1652] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at: www.uncjin.org/Documents/EighthCongress.html; Schjolberg/Hubbard, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1653] Regarding the challenges of international investigation, see above: § 3.2.5 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1654] Regarding possible reservations, see: *Blarcum*, Internet Hate Speech, The European Framework and the Emerging American Haven, Washington and Lee Law Review, 2007, page 792.

[1655] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

[1656] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

[1657] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

[1658] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 29.

[1659] Regarding the definition of "distributing" and "making available", see § 6.1.8 above.

[1660] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 34.

[1661] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1662] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 36.

[1663] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention

on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1664] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1665] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1666] Regarding legislation on blasphemy, as well as other religious offences, see: Preliminary Report On The National Legislation In Europe Concerning Blasphemy, Religious Insults And Inciting Religious Hatred, 2007, available at: www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf.

[1667] International Mechanisms for Promoting Freedom of Expression, Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2006.

[1668] See above: § 6.1.9, as well as Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

[1669] The draft law was not in force at the time this publication was finalized.

[1670] Prevention of Electronic Crimes Ordinance 2007, available at: www.upesh.edu.pk/net-infos/cyber-act08.pdf .

[1671] Prevention of Electronic Crimes Ordinance, 2007, published in the Gazette of Pakistan, Extraordinary, Part-I, dated 31 December 2007, available at: www.na.gov.pk/ordinances/ord2008/elect_crimes_10042008.pdf.

[1672] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1673] Regarding the difficulties related to jurisdiction and the principle of freedom of expression, see also: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: www.coe.int/t/e/human_rights/ecri/1-EComputerLawReviewInternational/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ComputerLawReviewInternational(2000)27.pdf.

[1674] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1675] Regarding the challenges of international investigation, see above: § 3.2.6 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1676] The 2005 e-gaming data report estimates total Internet gambling revenues as USD 3.8 billion in 2001 and USD 8.2 billion in 2004. For more details, see: www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm. Regarding the number of licensed Internet websites related to Internet gambling in selected countries, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 52, available at: www.gao.gov/new.items/d0389.pdf. Regarding the total numbers of Internet gambling websites, see: *Morse*, Extraterritorial Internet Gambling: Legal Challenges and Policy Opinion, page 7, available at: http://law.creighton.edu/pdf/4/morsepublication2.pdf.

[1677] For an overview of different national Internet gambling legislation, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 45 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf.

[1678] Regarding the situation in the People's Republic of China, see for example: Online Gambling challenges China's gambling ban, available at: www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

[1679] Regarding addiction, see: *Shaffer*, Internet Gambling & Addiction, 2004, available at: www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Griffiths/Wood*, Lottery Gambling and Addiction; An Overview of European Research, available at: www.european-lotteries.org/data/info_130/Wood.pdf; *Jonsson/Andren/Nilsson/Svensson/Munck/Kindstedt/Rönnberg*, Gambling addiction in Sweden – the characteristics of problem gamblers, available at: www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, www.ncpgambling.org/media/pdf/eapa_flyer.pdf.

[1680] See the decision from the German Federal Court of Justice (BGH), published in BGHST 11, page 209.

[1681] See *Thumm*, Strafbarkeit des Anbietens von Internetglueckspielen gemaess § 284 StGB, 2004.

[1682] Examples of equipment in Internet-related cases could include servers, as well as Internet connections. Internet service providers which do not know that their services are abused by offenders to run illegal gambling operations are thus not responsible, as they may lack intention.

[1683] For details, see: *Hoyer*, SK-StGB, Sec. 284, Nr. 18. As mentioned previously, criminalization is limited to those cases where the offender is intentionally making the equipment available.

[1684] This is especially relevant with regard to the location of the server.

[1685] Avoiding the creation of safe havens is a major intention of harmonization processes. The issue of safe havens has been addressed by a number of international organizations. UN General Assembly Resolution 55/63 states that: "*States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies*". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "*There must be no safe havens for those who abuse information technologies*".

[1686] With regard to the principle of sovereignty, changing the location of a server can have a great impact on the ability of law-enforcement agencies to carry out an investigation. National Sovereignty is a fundamental principle in International Law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[1687] Regarding the challenges related to the international dimension and the independence of place of action and the location of the crime scene, see above: §§ 3.2.6 and 3.2.7.

[1688] For details, see: *Hoyer*, SK-StGB, Sec. 285, Nr. 1.

[1689] Regarding the vulnerability of Internet gambling to money laundering, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 5, 34 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf.

[1690] Regarding other recent approaches in the United States, see: *Doyle*, Internet Gambling: A Sketch of Legislative Proposals in the 108th Congress, CRS Report for Congress No. RS21487, 2003, available at: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-4047: *Doyle*, Internet Gambling: Two Approaches in the 109th Congress, CRS Report for Congress No. RS22418, 2006, available at: www.ipmall.info/hosted_resources/crs/RS22418-061115.pdf.

[1691] For an overview of the law, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm; *Shaker*, America's Bad Bet: How the Unlawful Internet Gambling Enforcement act of 2006 will hurt the house, Fordham Journal of Corporate & Financial Law, Vol. XII, page 1183 *et seq.*, available at: http://law.fordham.edu/publications/articles/600flspub8956.pdf.

[1692] *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm.

[1693] *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm.

[1694] Based on Sec. 5366, criminalization is limited to the acceptance of financial instruments for unlawful Internet gambling.

[1695] General Agreement on Trade in Services (GATS) – with regard to the United States Unlawful Internet Gambling Enforcement Act especially Articles XVI (dealing with Market Access) and XVII (dealing with National Treatment) could be relevant.

[1696] See: EU opens investigation into US Internet gambling laws, EU Commission press release, 10.03.2008, available at: http://ec.europa.eu/trade/issues/respectrules/tbr/pr100308_en.htm; *Hansen*, EU investigates DOJ internet gambling tactics, The Register, 11.03.2008, available at: www.theregister.co.uk/2008/03/11/eu_us_internet_gambling_probe/.

[1697] See above: § 3.2.l.

[1698] See above: § 3.2.2.

[1699] See, for example: Freedom of Expression, Free Media and Information, Statement of Mr McNamara, US delegation to OSCE, October 2003, available at: http://osce.usmission.gov/archive/2003/10/FREEDOM_OF_EXPRESSION.pdf; *Lisby*, No Place in the Law: Criminal Libel in American Jurisprudence, 2004, available at: http://www2.gsu.edu/~jougcl/projects/40anniversary/criminallibel.pdf. Regarding the development of the offence, see: *Walker*, Reforming the Crime of Libel, New York Law School Law Review, Vol. 50, 2005/2006, page 169, available at: www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf; Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: www.article19.org/pdfs/standards/definingdefamation.pdf; *Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts, Washington University Law Review, 2006, page 1157 *et seq.*, available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 *et seq.*, available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol. 84, 2006, page 1187 *et seq.*, available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

[1700] See, for example, the Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 10 December 2002. For more information, see: www.osce.org/documents/rfm/2004/10/14893_en.pdf. See in addition the statement of the representative on Freedom of the Media, Mr Haraszti, at the fourth Winder Meeting of the OSCE Parliamentary Assembly on 25 February 2005.

[1701] Regarding various regional approaches to criminalization of defamation, see: *Greene* (eds), It's a Crime: How Insult Laws Stifle Press Freedom, 2006, available at: www.wpfc.org/site/docs/pdf/It's_A_Crime.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf.

[1702] For more details, see: the British Crime Survey 2006/2007 published in 2007, available at: www.homeoffice.gov.uk/rds/pdfs07/hosb1107.pdf.

[1703] See: Crime Statistic Germany (Polizeiliche Kriminalstatistik), 2006, available at: www.bka.de/pks/pks2006/download/pks-jb_2006_bka.pdf.

[1704] The full version of the Criminal Defamation Amendment Bill 2002 is available at: www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02_P.pdf. For more information about the Criminal Defamation Amendment Bill 2002, see the Explanatory Notes, available at: www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02Exp_P.pdf

[1705] The full text of the Criminal Code of Queensland, Australia is available at: www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/CriminCode.pdf.

[1706] The provider Postini published a report in 2007 that identifies up to 75 per cent spam e-mail, see: www.postini.com/stats/. The Spam-Filter-Review identifies up to 40 per cent spam e-mails, see: http://spam-filter-review.toptenreviews.com/spam-statistics.html. The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails are spam. See: www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf.

[1707] For more information on the phenomenon, see above: § 2.6.7. For a precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[1708] Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

[1709] See ITU Survey on Anti-Spam Legislation Worldwide, 2005, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[1710] Regarding the availability of filter technology, see: *Goodman,* Spam: Technologies and Politics, 2003, available at: http://research.microsoft.com/~joshuago/spamtech.pdf. Regarding user-oriented spam prevention techniques, see: *Rotenberg/Liskow*, ITU WSIS Thematic Meeting On Countering Spam Consumer Perspectives On Spam: Challenges And Challenges, available at: www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

[1711] Spam Issues in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1712] See Spam Issues in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1713] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 37, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1714] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69: "The sending of unsolicited e-mail, for commercial or other purposes, may cause nuisance to its recipient, in particular when such messages are sent in large quantities or with a high frequency ("spamming"). In the opinion of the drafters, such conduct should only be criminalised where the communication is intentionally and seriously hindered. Nevertheless, Parties may have a different approach to hindrance under their law, e.g. by making particular acts of interference administrative offences or otherwise subject to sanction. The text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered – partially or totally, temporarily or permanently – to reach the threshold of harm that justifies sanction, administrative or criminal, under their law."

[1715] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1716] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1717] The document available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1718] Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1719] Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1720] Regarding the US legislation on spam, see: *Sorkin*, Spam Legislation in the United States, The John Marshall Journal of Computer & Information Law, Vol. XXII, 2003; *Warner*, Spam and Beyond: Freedom, Efficiency, and the Regulation of E-mail Advertising, The John Marshall Journal of Computer & Information Law, Vol. XXII, 2003; *Alongi*, Has the US conned Spam, Arizona Law Review, Vol. 46, 2004, page 263 *et seq.*, available at: www.law.arizona.edu/Journals/ALR/ALR2004/vol462/alongi.pdf; Effectiveness and Enforcement of the CAN-SPAM Act: Report to Congress, 2005, available at: www.ftc.gov/reports/canspam05/051220canspamrpt.pdf.

[1721] For more details about the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM act 2003), see: www.spamlaws.com/f/pdf/pl108-187.pdf.

[1722] See: *Hamel,* Will the CAN-SPAM Act of 2003 Finally Put a Lid on Unsolicited E-mail?, New Eng. Law Review, 39, 2005, 196 *et seq.* 325, 327 (2001)).

[1723] For more details, see: *Bueti,* ITU Survey on Anti-Spam legislation worldwide 2005, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[1724] For more information, see: *Wong,* The Future Of Spam Litigation After Omega World Travel v. Mummagraphics, Harvard Journal of Law & Technology, Vol. 20, No. 2, 2007, page 459 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v20/20HarvJLTech459.pdf.

[1725] Websense Security Trends Report 2004, page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security –

Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

[1726] One example of this misuse is the publication of passwords used for access control. Once published, a single password can grant access to restricted information to hundreds of users.

[1727] One example is the 2001 EU Framework Decision combating fraud and counterfeiting of non-cash means of payment.

[1728] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 71: "To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offences under Articles 2 – 5. In this respect the provision builds upon recent developments inside the Council of Europe (European Convention on the legal protection of services based on, or consisting of, conditional access – ETS N° 178) and the European Union (Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access) and relevant provisions in some countries".

[1729] With the definition of "distributing" in the Explanatory Report ('Distribution' refers to the active act of forwarding data to others – Explanatory Report, No. 72), the drafters of the Convention restrict devices to software. Although the Explanatory Report is not definitive in this matter, it is likely that it covers not only software devices, but hardware tools as well.

[1730] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

[1731] See, in this context: *Biancuzzi*, The Law of Full Disclosure, 2008, available at: www.securityfocus.com/print/columnists/466.

[1732] Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society:
*Article 6 – Obligations as to technological measures*
*1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.*
*2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:*
*(a) are promoted, advertised or marketed for the purpose of circumvention of, or*
*(b) have only a limited commercially significant purpose or use other than to circumvent, or*
*(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.*

[1733] See for example one approach in the US legislation:
18 USC. § 1029 ( Fraud and related activity in connection with access devices)
*(a) Whoever -*
*(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;*
*(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;*
*(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;*
*(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;*
*(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000*;
*(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of -*
*(A) offering an access device*; *or*
*(B) selling information regarding or an application to obtain an access device*;
*(7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services*;
*(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver*;

*(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or*
*(10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device; shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.*
*(b)*
*(1) Whoever attempts to commit an offense under subsection (a) of this section shall be subject to the same penalties as those prescribed for the offense attempted.*
*(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both. […]*

[1734] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

[1735] This approach could lead to broad criminalization. Therefore Art. 6, Subparagraph 3 of the Convention on Cybercrime enables states to make a reservation and limit criminalization to the distribution, sale and making available of devices and passwords.

[1736] Art. 6, Subparagraph 3 of the Convention on Cybercrime enables states to make a reservation and limit criminalization to the distribution, sale and making available of devices and passwords.

[1737] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

[1738] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72: "This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices".

[1739] Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001, on the harmonization of certain aspects of copyright and related rights in the information society.

[1740] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 73: The drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This was considered to be too narrow. It could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances. The alternative to include all devices even if they are legally produced and distributed, was also rejected. Only the subjective element of the intent of committing a computer offence would then be decisive for imposing a punishment, an approach which in the area of money counterfeiting also has not been adopted. As a reasonable compromise the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices.

[1741] Regarding the US approach to address the issue, see for example 18 USC. § 2512 (2):
*(2) It shall not be unlawful under this section for –*
*(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or*
*(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.*

[1742] *Gercke*, Cybercrime Training for Judges, 2009, page 39, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1743] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 76: "Paragraph 2 sets out clearly that those tools created for the authorised testing or the protection of a computer system are not covered by the provision. This concept is already contained in the expression 'without right'. For example, test-devices ('cracking-devices') and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be 'with right'."

[1744] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 731.

[1745] See, for example, the World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

[1746] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1747] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 76.

[1748] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report points out: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1749] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 77.

[1750] For more information, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 78.

[1751] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1752] Expert Group's suggestion for an amendment:
Paragraph 3:
A person who possesses more than one item mentioned in subparagraph (i) or (ii), is deemed to possess the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6,7 or 8 unless the contrary is proven.
Official Note: S*ubsection 3 is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context.*

[1753] Canada's suggestion for an amendment:
Paragraph 3:
(3) Where a person possesses more than [number to be inserted] item(s) mentioned in subparagraph (i) or (ii), a court may infer that the person possesses the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8, unless the person raises a reasonable doubt as to its purpose.
Official Note: S*ubsection 3 is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context.*

[1754] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1755] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1756] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1757] "Draft thereby makes criminal the knowing and deliberate effort to cause illegal attacks through such distribution, but not discussions of computer vulnerability intended for evaluating." See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1758] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1759] See *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.88.

[1760] See for example: *Austria*, Forgery in Cyberspace: The Spoof could be on you, University of Pittsburgh School of Law, Journal of Technology Law and Policy, Vol. IV, 2004, available at: http://tlp.law.pitt.edu/articles/Vol5-Austria.pdf.

[1761] See for example 18 USC. § 495:
Whoever falsely makes, alters, forges, or counterfeits any deed, power of attorney, order, certificate, receipt, contract, or other writing, for the purpose of obtaining or receiving, or of enabling any other person, either directly or indirectly, to obtain or receive from the United States or any officers or agents thereof, any sum of money; or
Whoever utters or publishes as true any such false, forged, altered, or counterfeited writing, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited; or
Whoever transmits to, or presents at any office or officer of the United States, any such writing in support of, or in relation to, any account or claim, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited –
Shall be fined under this title or imprisoned not more than ten years, or both.
Or Sec. 267 German Penal Code:
Section 267 Falsification of Documents
(1) Whoever, for the purpose of deception in legal relations, produces a counterfeit document, falsifies a genuine document or uses a counterfeit or a falsified document, shall be punished with imprisonment for not more than five years or a fine.
(2) An attempt shall be punishable.
(3) In especially serious cases the punishment shall be imprisonment from six months to ten years. An especially serious cases exists, as a rule, if the perpetrator:
1. acts professionally or as a member of a gang which has combined for the continued commission of fraud or falsification of documents;
2. causes an asset loss of great magnitude;
3. substantially endangers the security of legal relations through a large number of counterfeit or falsified documents; or
4. abuses his powers or his position as a public official.
(4) Whoever commits the falsification of documents professionally as a member of a gang which has combined for the continued commission of crimes under Sections 263 to 264 or 267 to 269, shall be punished with imprisonment from one year to ten years, in less serious cases with imprisonment from six months to five years.

[1762] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 82.

[1763] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 81: "The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception."

[1764] See Art. 1 (b) Convention on Cybercrime.

[1765] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 84.

[1766] For example, by filling in a form or adding data to an existing document.

[1767] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 84.

[1768] With regard the definition of "alteration" in Art. 4, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1769] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

[1770] With regard the definition of "suppression" in Art. 4, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1771] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

[1772] With regard the definition of "deletion", see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1773] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

[1774] If only part of a document is deleted the act might also be covered by the term "alteration".

[1775] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1776] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1777] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1778] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 85.

[1779] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1780] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1781] See, for example: *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006, available at: http://edition.cnn.com/2006/US/05/18/identity.theft/; Identity Fraud, NY Times Topics, available at: http://topics.nytimes.com/top/reference/timestopics/subjects/i/identity_fraud/index.html; *Stone*, US Congress looks at identity theft, International Herald Tribune, 22.03.2007, available at: www.iht.com/articles/2007/03/21/business/identity.php.

[1782] See, for example, the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

[1783] See, for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Peeters*, Identity Theft Scandal in the US: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm.

[1784] Regarding the phenomenon of identity theft, see above: § 2.8.3.

[1785] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cybercrime, COM (2007) 267.

[1786] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cybercrime, COM (2007) 267.

[1787] *Gercke*, Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, Document No: E/CN.15/2009/CRP.13, page 8 *et seq.*

[1788] *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

[1789] This is not the case if the scam is based solely on synthetic data. Regarding the relevance of synthetic data, see: *McFadden*, Synthetic identity theft on the rise, Yahoo Finance, 16.05.2007, available at: http://biz.yahoo.com/brn/070516/21861.html?.v=1=1 ; ID Analytics, www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf.

[1790] The reason for the success is the fact that the provisions focus on the most relevant aspect of phase 1: transfer of the information from the victim to the offender.

[1791] Examples of acts that are not covered include the illegal access to a computer system in order to obtain identity related information.

[1792] One of the most common ways the information obtained is used is fraud. See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[1793] Furthermore, it is uncertain whether the provisions criminalize possession if the offender does not intend to use the data but to sell them. Prosecution could in this case in general be based on fact that 18 USC. § 1028 not only criminalizes possession with the intent to use it to commit a crime, but also to aid or abet any unlawful activity.

[1794] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1795] Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1796] See also: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, page 29, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

[1797] Similar provisions are included in the Commonwealth Model Law and the Stanford Draft International Convention. For more information about the Commonwealth model law, see: Model Law on Computer and Computer Related Crime, LMM(02)17. The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf. For more information about the Stanford Draft International Convention, see: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror,

page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1798] See above: § 6.1.1.

[1799] See above: § 6.1.4.

[1800] See above: § 6.1.5.

[1801] *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[1802] See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[1803] See above: § 2.8.1.

[1804] Regarding the criminalization of computer-related fraud in the UK, see: *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.50 *et seq.*

[1805] One example of this is Section 263 of the German Penal Code that requires the falsity of a person (mistake). The provision does not therefore cover the majority of computer-related fraud cases:

> *Section 263 Fraud*
> *(1) Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another, by provoking or affirming a mistake by pretending that false facts exist or by distorting or suppressing true facts, shall be punished with imprisonment for not more than five years or a fine.*

[1806] A national approach that is explicitly address computer-related fraud is 18 USC. § 1030:

> *Sec. 1030. Fraud and related activity in connection with computers*
> *(a) Whoever -*
> *(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it*;
> *(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -*
> *(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 USC. 1681 et seq.)*;
> *(B) information from any department or agency of the United States*; *or*
> *(C) information from any protected computer if the conduct involved an interstate or foreign communication*;
> *(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States*;
> *(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period*;

[1807] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

[1808] The drafters highlighted that the four elements have the same meaning as in the previous articles: "To ensure that all possible relevant manipulations are covered, the constituent elements of 'input', 'alteration', 'deletion' or 'suppression' in Article 8(a) are supplemented by the general act of 'interference with the functioning of a computer program or system' in Article 8(b). The elements of 'input, alteration, deletion or suppression' have the same meaning as in the previous articles." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

[1809] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

[1810] With regard to the definition of "alteration" in Art. 4, see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1811] With regard to the definition of "suppression" in Art. 4, see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1812] With regard to the definition of "deletion", see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1813] As a result, not only data-related offences, but also hardware manipulations, are covered by the provision.

[1814] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 87.

[1815] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 88.

[1816] "The offence has to be committed "intentionally". The general intent element refers to the computer manipulation or interference causing loss of property to another. The offence also requires a specific fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another."

[1817] The drafters of the Convention point out that these acts are not meant to be included in the offence established by Article 8 – Explanatory Report to the Council of Europe Convention on Cybercrime, No. 90.

[1818] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1819] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 90.

[1820] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1821] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1822] Regarding the ongoing transition process, see: OECD Information Technology Outlook 2006, Highlights, page 10, available at: www.oecd.org/dataoecd/27/59/37487604.pdf.

[1823] For more information on the effects of digitization on the entertainment industry, see above: § 2.7.1.

[1824] The technology that is used is called digital rights management – DRM. The term digital rights management (DRM) is used to describe several technologies used to enforce pre-defined policies controlling access to software, music, movies or other digital data. One of the key functions is copy protection, which aims to control or restrict the use and access to digital media content on electronic devices with such technologies installed. For further information, see:

*Cunard/Hill/Barlas*, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

[1825] Regarding the technical approach to copyright protection, see: *Persson/Nordfelth*, Cryptography and DRM, 2008, available at: www.it.uu.se/edu/course/homepage/security/vt08/drm.pdf.

[1826] For details see above: § 2.7.1.

[1827] Examples are 17 USC. § 506 and 18 USC. § 2319:
*Section 506. Criminal offenses*
*(a) Criminal Infringement. —- Any person who infringes a copyright willfully either –*
*(1) for purposes of commercial advantage or private financial gain, or*
*(2) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000, shall be punished as provided under section 2319 of title 18, United States Code. For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement.*
*[...]*
*Section 2319. Criminal infringement of a copyright*
*(a) Whoever violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsections (b) and (c) of this section and such penalties shall be in addition to any other provisions of title 17 or any other law.*
*(b) Any person who commits an offense under section 506(a)(1) of title 17 –*
*(1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than $2,500;*
*(2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and*
*(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.*
*(c) Any person who commits an offense under section 506(a)(2) of title 17, United States Code –*
*(1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of $2,500 or more;*
*(2) shall be imprisoned not more than 6 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and*
*(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000.*
*(d)(1) During preparation of the presentence report pursuant to Rule 32(c) of the Federal Rules of Criminal Procedure, victims of the offense shall be permitted to submit, and the probation officer shall receive, a victim impact statement that identifies the victim of the offense and the extent and scope of the injury and loss suffered by the victim, including the estimated economic impact of the offense on that victim.*
*(2) Persons permitted to submit victim impact statements shall include –*
*(A) producers and sellers of legitimate works affected by conduct involved in the offense;*
*(B) holders of intellectual property rights in such works; and*
*(C) the legal representatives of such producers, sellers, and holders.*
*(e) As used in this section –*
*(1) the terms "phonorecord" and "copies" have, respectively, the meanings set forth in section 101 (relating to definitions) of title 17; and*
*(2) the terms "reproduction" and "distribution" refer to the exclusive rights of a copyright owner under clauses (1) and (3) respectively of section 106 (relating to exclusive rights in copyrighted works), as limited by sections 107 through 122, of title 17.*
Regarding the development of legislation in the United States, see: *Rayburn*, After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html.

[1828] Regarding the international instruments, see: *Sonoda*, Historical Overview of Formation of International Copyright Agreements in the Process of Development of International Copyright Law from the 1830s to 1960s, 2006, available at: www.iip.or.jp/e/summary/pdf/detail2006/e18_22.pdf; *Okediji*, The International Copyright System: Limitations, Exceptions and Public Interest Considerations for Developing Countries, 2006, available at: www.unctad.org/en/docs/iteipc200610_en.pdf. Regarding international approaches to anti-circumvention laws, see:

*Brown*, The evolution of anti-circumvention law, International Review of Law, Computer and Technology, 2006, available at: www.cs.ucl.ac.uk/staff/I.Brown/anti-circ.pdf.

[1829] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 109.

[1830] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 110: "With regard to paragraph 1, the agreements referred to are the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and the World Intellectual Property Organisation (WIPO) Copyright Treaty. With regard to paragraph 2, the international instruments cited are the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the World Intellectual Property Organisation (WIPO) Performances and Phonograms Treaty. The use of the term "pursuant to the obligations it has undertaken" in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention."

[1831] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 111: "The use of the term "pursuant to the obligations it has undertaken" in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention."

[1832] Explanatory Report to the Council of Europe Convention on Cybercrime, Nos. 16 and 108.

[1833] *Article 61:*

> *Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale. Remedies available shall include imprisonment and/or monetary fines sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding gravity. In appropriate cases, remedies available shall also include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale.*

[1834] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 113.

[1835] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 114.

[1836] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report points out: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1837] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 115. In addition, the drafters pointed out: The absence of the term "without right" does not *a contrario* exclude application of criminal law defences, justifications and principles governing the exclusion of criminal liability associated with the term "without right" elsewhere in the Convention.

[1838] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention

on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1839] See: *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1840] See: *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1841] See, for example, Art. 5 of the Convention on Cybercrime.

[1842] Convention on Cybercrime, ETS 185.

[1843] Council of Europe Convention on the Prevention of Terrorism, ETS 196.

[1844] Council of Europe Convention on the Prevention of Terrorism, ETS 196.

[1845] EU Framework Decision on Combating Terrorism, COM (2007) 650.

[1846] EU Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

[1847] EU Framework Decision 2008/919/JHA of 28 November 2008, No. 4.

[1848] The intention of the drafters to cover online and offline activities was highlighted several times. See, for example: EU Framework Decision 2008/919/JHA of 28 November 2008, No. 11. "These forms of behavior should be equally punishable in all Member States irrespective of whether they are committed through the Internet or not."

[1849] Regarding the motivation, see: *Russell*, A History of the United Nations Charter, 1958.

[1850] *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 57.

[1851] *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 59.

[1852] *Mani*, Basic Principles of Modern International Law: A Study of the United Nations Debates on the Principles of International Law Concerning Friendly Relations and Co-operation among States, 1993, page 263 *et seq.*

[1853] *Bond*, Peacetime foreign Data Manipulations as one Aspect of Offensive Information Warfare, 1996.

[1854] *Brownlie*, International Law and the Use of Force, 1993, page 362.

[1855] *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 80.

[1856] *Solce*, The Battlefield of Cyberspace: The inevitable new military branch – the cyber force, Alb. Law Journal of Science and Technology, Vol. 18, page 304.

[1857] *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 57.

[1858] *Albright/Brannan/Waldrond*, Did Stuxnet Take out 1 000 Centrifuges at the Nataz Enrichment Plant?, Preliminary Assessment, Institute for Science and International Security, 2010.

[1859] Regarding proliferation concerns, see: *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 58.

[1860] With regard to the development, see: *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3, page 28 *et seq.*; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

[1861] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No.5.

[1862] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, page 6.

[1863] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[1864] Regarding the admissibility and reliability of digital images, see: *Witkowski*, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law & Policy, page 267 *et seq.*

[1865] *Harrington*, A Methodology for Digital Forensics, T.M. Cooley J. Prac. & Clinical L., 2004, Vol. 7, page 71 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004, page 14. Regarding the legal frameworks in different countries, see: *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Wang*, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Makulilo*, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 76; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 213.

[1866] See: *Richtel*, Live Tracking of Mobile Phones Prompts Court Fight on Privacy, The New York Times, 10.12.2005, available at: www.nytimes.com/2005/12/10/technology/10phone.html?pagewanted=print10dec2005. Regarding the legal implications, see: *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38, page 1324 *et seq.*, available at www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__law_review/documents/web_copytext/ecm_pro_059784.pdf.

[1867] For a case where search-engine requests were used as evidence in a murder case, see: *Jones*, Murder Suspect's Google Search Spotlighted in Trial, Informationweek.com, 11.11.2005, available at: www.informationweek.com/news/internet/search/showArticle.jhtml?articleID=173602206.

[1868] The Council of Europe Convention on Cybercrime therefore contains a provision that clarifies that the procedural instruments in the Convention shall not only be applicable with regard to cybercrime-related offences, but also to "other criminal offences committed by means of a computer system" and "the collection of evidence in electronic form of a criminal offence" (Art. 14).

[1869] *Casey*, Digital Evidence and Computer Crime, 2004, page 9.

[1870] Regarding the need for formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2.

[1871] Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq.*

[1872] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 3. Regarding the early discussion about the use of printouts, see: *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970, page 291 *et seq.*

[1873] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Casey*, Digital Evidence and Computer Crime, 2004, page 11; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, page 1.

[1874] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historical development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.

[1875] *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286. With more reference to national law: *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 213; *Vaciago*, Digital Evidence, 2012, Chapter I.1 (with an overview about the discussion about digital evidence in different jurisdictions).

[1876] Police and Criminal Evidence Code (PACE).

[1877] *Casey*, Digital Evidence and Computer Crime, 2004, page 12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm.

[1878] Regarding the different models of cybercrime investigation, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

[1879] This includes the development of investigation strategies.

[1880] The second phase covers, in particular, the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[1881] See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, No. 2, page 3.

[1882] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 532.

[1883] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

[1884] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

[1885] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

[1886] This includes, for example, the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

[1887] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

[1888] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process within forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

[1889] Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

[1890] *Vaciago*, Digital Evidence, 2012, Chapter II.

[1891] *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/EFE47BD9-A897-6585-5EAB032ADF89EDCF.pdf.

[1892] Regarding geo-recognition, see: *Friedland/Sommer*; Cybercasing the Joint: On the Privacy Implications of Geo-Tagging, available at: www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf; *Strawn*, Expanding the Potential for GPS Evidence Acquisition, Small Scale Digital Device Forensics Journal, 2009, Vol. 3, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V3_1_Strawn.pdf; *Zdziarski*, iPhone Forensics, 2008, available at: www.esearchbook.com/files/4/eSearchBook.1224255173.iPhone%20Forensics.pdf.

[1893] See *Liberatore/Erdely/Kerle/Levine/Shields*, Forensic investigation of peer-to-peer file sharing networks, Digital Investigations, 2010, page 95 *et seq.*, available at: www.dfrws.org/2010/proceedings/2010-311.pdf.

[1894] Regarding the use of metadata for investigations, see: *Luque*, Logical Level Analysis of Unix Systems in: Handbook of Computer Crime Investigations: Forensic Tools and Technology, 2001; *Cohen*, Digital Still Camera Forensics, Small Scale Digital Device Forensics Journal, 2007, Vol. 1, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V1_1_Cohen.pdf.

[1895] *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286.

[1896] *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217. Regarding the challenges of witnesses as a source of evidence, see: *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Heaton-Armstrong/Shepherd/Wolchover*, Analysing Witness Testimony: Psychological, Investigative and Evidential Perspective, 2002.

[1897] *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

[1898] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 19.

[1899] Regarding the liability of digital investigations, see: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, No. 2.

[1900] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161.

[1901] *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

[1902] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[1903] Daubert v. Merrell Dow Pharmaceutical, Inc. (1993) 113 S. Ct. 2786, available at: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=509&invol=579.

[1904] *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No. 3, page 1.

[1905] The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217.

[1906] Regarding the status of national legislation, see for example: The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

[1907] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

[1908] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

[1909] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 85; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 41 *et seq.*

[1910] *Casey*, Digital Evidence and Computer Crime, 2004, page 15.

[1911] *Talleur*, Digital Evidence: The Moral Challenge, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, page 1 *et seq.*, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E398D-0CAD-4E8D-CD2Dpage 38F31AF079F9.pdf; With a strong call for courts looking at experts in forensic investigations: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[1912] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf. Criteria for Admissibility of Expert Opinion, Utah Law Review, 1978, page 546 *et seq.*

[1913] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

[1914] See *Casey*, Digital Evidence and Computer Crime, 2004, page 16; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39.

[1915] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217.

[1916] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[1917] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[1918] See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.

[1919] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 92.

[1920] *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

[1921] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[1922] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[1923] *Menezes*, Handbook of Applied Cryptography, 1996, page 361.

[1924] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[1925] *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

[1926] For an overview of the different techniques, see: *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Cristopher*, Computer Evidence: Collection and Preservation, 2006.

[1927] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[1928] *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/EFE47BD9-A897-6585-5EAB032ADF89EDCF.pdf.

[1929] *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

[1930] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[1931] *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

[1932] Regarding the design of courtrooms, see: *Youngblood*, Courtroom Design, 1976; *Smith/Larson*, Courtroom design, 1976.

[1933] Scientific Evidence Review: Admissibility of Expert Evidence, ABA, 2003, page 159 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004, page 169; *Nilsson*, Digital Evidence in the Courtroom, 2010; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12, Issue 1.

[1934] *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

[1935] See *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 538.

[1936] Regarding the need for a formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol. 3, No. 2, page 2.

[1937] *Casey*, Digital Evidence and Computer Crime, 2004, page 20.

[1938] *Gercke*, Impact of Cloud Computing on the work of law-enforcement agencies, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*

[1939] *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 218.

[1940] *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286.

[1941] See in this context: *Nikali*, The Substitution of Letter Mail in Targeted Communication, 2007, available at: http://hsepubl.lib.hse.fi/pdf/diss/a136.pdf.

[1942] See in this context *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Hayes*, Forensic Handwriting Examination, 2006.

[1943] *Houck/Siegel*, Fundamentals of Forensic Science, 2010, page 512 *et seq.*; FBI Handbook of Crime Scene Forensics, 2008, page 111 *et seq.*; *Hilton*, Identification of the Work from an IBM Selectric Typewriter, Journal of Forensic Sciences, 1962, Vol. 7, Issue 3, page 286 *et seq.*; *Miller*, An Analysis of the Identification Value of Defects in IBM Selectric Typewriters, American Academy of Forensic Science annual meeting, presented paper, Ohio, 1983; *Koppenhaver*, Forensic Document Examination: Principles and Practice, 2007, page 207 *et seq.*

[1944] *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mail: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

[1945] *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mail: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

[1946] *Meghanathan/Allam/Moore*, Tools and Techniques for Network Forensics, International Journal of Network Security and its Applications, 2009, Vol. 1, No. 1, page 16 *et seq.*, available at: http://airccse.org/journal/nsa/0409s2.pdf.

[1947] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

[1948] Regarding approaches to link a suspect to stored computer records, see for example: *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 165.

[1949] Regarding the obligation to register prior to the use of public Internet terminals in Italy, see: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, CRi 2006, page 94.

[1950] See: *Richtel*, Live Tracking of Mobile Phones Prompts Court Fight on Privacy, The New York Times, 10.12.2005, available at: www.nytimes.com/2005/12/10/technology/10phone.html?pagewanted=print10dec2005. Regarding the legal implications, see: *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38, page 1324 *et seq.*, available at www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__law_review/documents/web_copytext/ecm_pro_059784.pdf.

[1951] Regarding a case where search-engine requests were used as evidence in a murder case, see: *Jones*, Murder Suspect's Google Search Spotlighted in Trial, Informationweek.com, 11.11.2005, available at: www.informationweek.com/news/internet/search/showArticle.jhtml?articleID=173602206.

[1952] Regarding the extent of commercial child pornography, see: IWF 2007 Annual and Charity Report, page 7.

[1953] See *Schnabel,* The Mikado Principle, Datenschutz und Datensicherheit, 2006, page 426 *et seq.*

[1954] *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 206.

[1955] Regarding the legitimacy principle, see: *Grans/Palmer*, Australian Principles of Evidence, 2005, page 10.

[1956] *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 219.

[1957] *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 207.

[1958] *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80.

[1959] *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208.

[1960] Regarding necessary procedures, see: *Chawki*, The Digital Evidence in the Information Era, available at: www.droit-tic.com/pdf/digital_evid.pdf; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

[1961] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[1962] *Menezes*, Handbook of Applied Cryptography, 1996, page 361.

[1963] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[1964] See in this context also: *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208.

[1965] Regarding the consequences of the fruit of the poisonous tree doctrine for computer-crime investigations, see: *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, 2005, Vol. 119, page 563.

[1966] *Kenneally*, UCLA Journal of Law and Technology, 2005, Vol. 9, Issue 2; *Keane*, Modern Law of Evidence, 2005, page 27.

[1967] Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006, pages 331-332 and *Omychund v Barker* (1744) 1 Atk 21 at 49; *Robinson Bros (Brewers) Ltd v. Houghton and Chester-le-Street Assessment Committee* [1937] 2 KB 445 at 468, [1937] 2 All ER 298 at 307, CA, per Scott LJ.

[1968] Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006, pages 331-332.

[1969] *Springsteen v Masquerade Music Ltd* [2001] EWCA Civ 563, [2001] EMLR 654. The primary evidence rule was in any event inapplicable to recordings on film or tape, which may be proven by copies under common law (*Kajala v Noble* (1982) 75 Cr App Rep 149, DC; R v. Wayte (1982) 76 Cr App Rep 110, CA) and if lost or destroyed their contents may be proven by oral evidence from persons who have previously viewed or heard them (*Taylor v Chief Constable of Cheshire* [1987] 1 All ER 225, 84 Cr App Rep 191, DC). Also, see now the Criminal Justice Act 2003 s 133; and para 1464 post.

[1970] Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, pages 565-566; *Permanent Trustee Co of New South Wales v Fels* [1918] AC 879, PC.

[1971] Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, pages 565-566; The admission of documentary copies is subject to the Civil Evidence Act 1995: see PARA 808 *et seq.*

[1972] *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

[1973] *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

[1974] With regard to different exemptions, see: *Nemeth*, Law of Evidence: A Primer for Criminal Justice, 2007, page 144 *et seq.*; Best Evidence Rule, California Law Review Commission, 1996, available at: www.clrc.ca.gov/pub/Printed-

Reports/REC-BestEvidenceRule.pdf; *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

[1975] For further reference, see: *Eltgroth*, Best Evidence and the Wayback Machine, Fordham Law Review, 2009, 193, available at: http://law.fordham.edu/assets/LawReview/Eltgroth_October_2009.pdf.

[1976] With regard to European common law countries (UK, Ireland), this development was especially supported by EU Directive 1999/93/EC. See also Sec. 4 and 6 of the Commonwealth model law on electronic evidence.

[1977] *Munday*, Evidence, 2007, page 380; *Allen*, Practical Guide to Evidence, 2008, page 189.

[1978] Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, page 567.

[1979] Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, page 567 and *R v Sharp* [1988] 1WLR 7, HL; *R v Kearley* [1992] 2 AC 228, [1992] 2 All ER 345. HL. See also Civil Evidence Act 1995 ss1-7.

[1980] Per Lord Havers in *R v Sharp* [1988] 1 WLR 7 and per Lords Ackner and Oliver in R v Kearley [1992] 2 All ER 345 at 363 and 366 respectively. The rule also extends to out-of-court statements of otherwise admissible opinion.

[1981] *Keane*, Modern Law of Evidence, 2005, pages 246-266.

[1982] *Dennis*, The Law of Evidence, 2002, Chapters 16-17.
*Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 242.

[1983] *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 246.

[1984] Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006.

[1985] See in this context, for example, Part II of the Irish Criminal Evidence Act 1992.

[1986] R v Dodson [1984] 1 WLR 971, 79 CrApp Rep 220, CA (photographic evidence); R v Maqsud Ali [1966] 1 QB 688, 49 Cr App Rep 230, CCA (tape recorded conversation); R v Wood (1982) 76 Cr App Rep 23, CA; Castle v Cross [1984] 1 WLR 1372, DPP v McKeown [1997] 1 All ER 737, 2 Cr App Rep 155, HL (computer evidence).

[1987] A "statement" is now defined as any representation of fact or opinion made by a person by whatever means; and it includes a representation made in a sketch, photo or other pictorial form: Criminal Justice Act 2003 ss 115(2), 134 (2).

[1988] See in this context, for example, the Statue of Liberty case, [1968] 1 W.L.R. 739.

[1989] *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 246.

[1990] *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208 *et seq.*

[1991] *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 220.

[1992] *Insa/Lazaro*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 214; *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 205.

[1993] Model Law on Electronic Evidence (LMM(02)12.

[1994] Singapore Evidence Act, Section 35.

[1995] Canada Uniform Electronic Evidence Act.

[1996] See above.

[1997] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. For more information, see: *Dumortier*, The European Directive 1999/93/EC on a Community Framework for Electronic Signatures, in Lodder/Kaspersen, eDirectives, 2000, page 33 *et seq.*, available at: www.law.kuleuven.be/icri/publications/58The%20European%20Directive%201999.pdf.

[1998] *Kenneally*, UCLA Journal of Law and Technology, 2005, Vol. 9, Issue 2; *Keane*, Modern Law of Evidence, 2005, page 27.

[1999] *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

[2000] *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

[2001] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, § 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[2002] United Nations Report oft he International Law Commission, Fifty-eigth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm

[2003] *Valesco*, Jurisdictional Aspects of Cloud Computing, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf

[2004] For a general overview see: *Kohl*, Jurisdiction and the Internet: Regulatory Competence over Online Activity, 2007; *Zittrain*, Jurisdiction, Internet Law Series, 2005;

[2005] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

[2006] National sovereignty is a fundamental principle in international law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[2007] *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 5, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf.

[2008] *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 6; *Van Dervort*, International Law and Organizations: An Introduction, 1998, page 254.

[2009] *Van Dervort*, International Law and Organizations: An Introduction, 1998, page 254.

[2010] International Court of Justice, Case of S.S."Lotus", Series A – No. 10, 1927, available at: www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf.

[2011] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.html; Dunn/Krishna-Hensel/Mauer (eds), The Resurgence of the State, Trends and Progress in Cyberspace Governance, 2007, page 69.

[2012] *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 8, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf.

[2013] For an overview about relevant case examples for conflicts see: *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 10 et seq.

[2014] *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 21.

[2015] See in this regard for example: *Ali/Ragothaman/Bhagavathula/Pendse*, Security Issues in Airplane Data Networks, available at: http://soar.wichita.edu/dspace/bitstream/handle/10057/398/GRASP-4.pdf?sequence=1; The Developments in Satellite Hardware, Satellite Executive Briefing, Vol. 3, No. 12, 2010, available at: www.satellitemarkets.com/pdf/aug10.pdf.

[2016] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

[2017] See *Krizek*, Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice, Boston University International Law Journal, 1988, page 337 et seq; *Cameron*, Protective Principle of International Criminal Jurisdiction, 1994.

[2018] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

[2019] *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 72. Regarding the use of the principle within the US see for example United States v. Gallaxy Sports.

[2020] See in this regard below: § 6.2.8.

[2021] *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 72.

[2022] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

[2023] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

[2024] See: *Kobrick*, The Ex Post Facto Prohibition and the Exercise of Universal Jurisdiction over International Crimes, Columbia Law Review, Vol 87, 1987, page 1523 et seq; Regarding the discussion about scope and application of the principle of universal jurisdiction within the UN see the information provided by the Sixth Committee, available at: www.un.org/en/ga/sixth/64/UnivJur.shtml.

[2025] For an overview about the implementation of the principle in European countries see: Universal Jurisdiction in Europe – The State of the Art, Human Rights Watch, 2006, available at: www.hrw.org/sites/default/files/reports/ij0606web.pdf.

[2026] See above: §§ 4.5.4 and 6.1.

[2027] This was also highlighted by the drafters of the Council of Europe Convention on Cybercrime, which contains a set of essential investigation instruments. The drafters of the report point out: "Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132. Regarding the substantive criminal law provisions related to cybercrime, see above: § 6.1.

[2028] Regarding the elements of an anti-cybercrime strategy, see above: § 4. Regarding user-based approaches in the fight against cybercrime, see: *Görling*, The Myth Of User Education, 2006, at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See also the comment made by *Jean-Pierre Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

[2029] Due to the protocols used in Internet communication and worldwide accessibility, there is very little need for a physical presence at the place where a service is physically offered. Due to this independence of place of action and the crime site, many criminal offences related to the Internet are transnational crimes. Regarding the independence of place of action and the result of the offence, see above: § 3.2.7.

[2030] Regarding the challenges of fighting cybercrime, see above: § 3.2.

[2031] The pure fact that the offender is acting from a different country can result in additional challenges for law-enforcement agencies' investigations even if similar substantive criminal law provisions and procedural law instruments are in place in both countries. In these cases, the investigation nevertheless requires international cooperation between the authorities in both countries, which in general is more time consuming compared to investigations concentrating on a single country.

[2032] See in this context also: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 134.

[2033] For an overview of the current status of the implementation of the Convention on Cybercrime and its procedural law provisions in selected countries, see the country profiles made available on the Council of Europe website: www.coe.int/cybercrime/.

[2034] See Articles 15-21 of the Council of Europe Convention on Cybercrime.

[2035] See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, No. 2, page 3.

[2036] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21.

[2037] *Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4, available at: www.acpr.gov.au/pdf/ACPR_CC3.pdf. Regarding the need for standardization, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Hall/Davis*, Towards Defining the Intersection of Forensic and Information Technology, International Journal of Digital Evidence, Vol. 4, Issue 1; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Forensics, International Journal of Digital Evidence, Vol. 3, Issue 2.

[2038] *Patel/Ciarduain*, The impact of forensic computing on telecommunication, IEEE Communications Magazine, Vol. 38, No. 11, 2000, page 64.

[2039] For an overview of different kinds of evidence that can be collected by computer forensic experts, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

[2040] *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 538.

[2041] For an overview of different forensic investigation techniques related to the most common technologies, see: *Carney/Rogers*, The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction, International Journal of Digital Evidence, Vol. 2, Issue 4; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf; *Urnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, Vol. 5, Issue 1; *Marsico/Rogers*, iPod Forensics, International Journal of Digital Evidence, Vol. 4, Issue 2; *Gupta/Mazumdar*; Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol, International Journal of Digital Evidence, Vol. 2, Issue 4; Hidden Disk Areas: HPA and DCO, International Journal of Digital Evidence, Vol. 5, Issue 1; *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, Vol. 4, Issue 1; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233; *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

[2042] *Harrison/Heuston/Morrissey/Aucsmith/Mocas/Russelle*, A Lesson Learned Repository for Computer Forensics, International Journal of Digital Evidence, Vol. 1, Issue 3.

[2043] Regarding the different models of Cybercrime investigations, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

[2044] This includes the development of investigation strategies.

[2045] The second phase covers especially the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[2046] With regard to developments, see: *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3, page 28 *et seq.*; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology

Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

[2047] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

[2048] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

[2049] *Vaciago*, Digital Evidence, 2012, Chapter II.1; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 220.

[2050] For guidelines on how to carry out the seizure of computer equipment, see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory, available at: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[2051] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

[2052] Regarding investigation techniques, see: *Casey*, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 204, page 283 *et seq.*

[2053] *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, No. 1.

[2054] *Howard*, Don't Cache out your Case: Prosecuting Child Pornography Possession Laws Based on Images located in Temporary Internet Files, Berkeley Technology Law Journal, 2004, Vol. 19, page 1227 *et seq.*; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 54.

[2055] See below: § 6.3.8.

[2056] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 171.

[2057] Regarding the challenges of encryption, see § 3.2.14 as well as *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, Issue 3.

[2058] Regarding possible counter strategies for law enforcement, see: *Haldeman/Schoen/Heninger* and other, Lest we Remember: Cold Boot Attacks on Encryption keys, 2008, available at: http://citp.princeton.edu/memory.

[2059] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[2060] *Vaciago*, Digital Evidence, 2012, Chapter II.1.

[2061] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 43; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 59.

[2062] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

[2063] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

[2064] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

[2065] *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, No. 3.

[2066] *Goodman*, Why the Police don't care about Computer Crime, Harvard Journal of Law & Technology, 1997, Vol. 10, No. 3, page 473; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38; *Gercke*, Challenges related to the Fight against Cybercrime, Multimedia und Recht, 2008, page 297.

[2067] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process in forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

[2068] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the forensic software magic lantern, developed as a keylogger used by law enforcement in the US, see: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3; *Green*, FBI Magic Lantern reality check, The Register, 03.12.2001, available at: www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/; *Salkever*, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.2001, available at: www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; *Abreu*, FBI confirms "Magic Lantern" project exists, 2001, available at: www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

[2069] Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security – available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

[2070] *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law & Technology, 2005, Vol. 9, No. 2.

[2071] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 52.

[2072] For an overview of the debate, see: *Gercke*, The Role of Internet Service Providers in the Fight Against Child Pornography Computer Law Review International, 2009, page 65 *et seq.*

[2073] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 15.

[2074] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 24.

[2075] See *Callanan/Gercke*, Study on the Cooperation between service providers and law enforcement against cybercrime – Toward common best-of-breed guidelines?, 2008, available at: www.coe.int/cybercrime/.

[2076] For more information about the Guidelines, see: *Gercke,* The Council of Europe Guidelines for the Cooperation between LEAs and ISPs against Cybercrime, Computer Law Review International, 2008, page 97 *et seq.*

[2077] See Guidelines for the cooperation of law enforcement and internet service providers against cybercrime, No. 29.

[2078] See Guidelines for the cooperation of law enforcement and internet service providers against cybercrime, No. 30.

[2079] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

[2080] Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

[2081] Regarding the impact on tracing offenders, see: *Nicoll*, Concealing and Revealing Identity on the Internet in *Nicoll/Prins/Dellen*, Digital Anonymity and the Law, Tensions and Dimensions, 2003, page 99 *et seq.*

[2082] *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, 2002, Vol. 1, No. 3.

[2083] For more information about CIPAV, see: *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007, available at: www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV for the first time, Heise Security News, 19.07.2007, available at: www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950; *Poulsen*, FBI's Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007, available at: www.wired.com/politics/law/news/2007/07/fbi_spyware; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008, available at: www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007, available at: http://news.zdnet.com/2100-1009_22-6197405.html; *Popa*, FBI Fights against terrorists with computer viruses,

19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.

2084 *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, No. 4.

2085 For more information, see: *Crumbley/Heitger/Smith*, Forensic and Investigative Accounting, 2005, § 14.12; *Caloyannides*, Privacy Protection and Computer Forensics, 2004, page 149.

2086 The term "phishing" describes an act that is carried out to make targets disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, The criminalization of Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide: Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

2087 *Casey*, Digital Evidence and Computer Crime, 2004, page 19.

2088 For more information, see: Spiegel Online, Fahnder ueberpruefen erstmals alle deutschen Kreditkarten, 08.01.2007, available at: www.spiegel.de/panorama/justiz/0,1518,457844,00.html.

2089 *Goodman*, Why the Police don't care about Computer Crime, Harvard Journal of Law & Technology, 1997, Vol. 10, No. 3, page 472.

2090 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

2091 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 90, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

2092 Regarding the need for a formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol. 3, No. 2, page 2.

2093 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208 *et seq.*

2094 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

2095 A denial-of-service (DoS) attacks aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

2096 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 64, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

2097 For further information, see: *Provos/Honeyman*, Hide and Seek: An Introduction to Steganography, available at: http://niels.xtdnet.nl/papers/practical.pdf; *Kharrazi/Sencar/Memon*, Image Steganography: Concepts and Practice, available at: http://isis.poly.edu/~steganography/pubs/ims04.pdf; Labs, Developments in Steganography, available at: http://web.media.mit.edu/~jrs/jrs_hiding99.pdf; *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.

2098 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9.

2099 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

2100 Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

2101 With regard to the criminalization of illegal devices, see below: § 6.1.15..

[2102] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

[2103] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

[2104] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 29.

[2105] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

[2106] Regarding the ability to manipulate the time information and the response in forensic investigations, see: *Gladyshev/Patel*, Formalizing Event Time Bounding in Digital Investigations, International Journal of Digital Evidence, 2005, Vol. 4, No. 1. Regarding dynamic time analysis, see: *Weil*, Dynamic Time & Date Stamp Analysis, International Journal of Digital Evidence, 2002, Vol. 1, No. 2.

[2107] *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

[2108] *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

[2109] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

[2110] See *Casey*, Digital Evidence and Computer Crime, 2004, page 16; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39.

[2111] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[2112] *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

[2113] For an overview of the different techniques, see: *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Cristopher*, Computer Evidence: Collection and Preservation, 2006.

[2114] Regarding the related procedural instrument, see: Art. 19, paragraph 3 Convention on Cybercrime.

[2115] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 12.

[2116] *Talleur*, Digital Evidence: The Moral Challenge, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, page 1 *et seq.*, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E398D-0CAD-4E8D-CD2D38F31AF079F9.pdf. With a strong call for courts looking at experts in forensic investigations: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[2117] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

[2118] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 62.

[2119] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 85; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 41 *et seq.*

[2120] See *Gercke*, Convention on Cybercrime, Multimedia und Recht. 2004, page 801, for further reference.

[2121] Taylor, The Council of Europe Cybercrime Convention – A civil liberties perspective, available at http://crime-research.org/library/CoE_Cybercrime.html; Cybercrime: Lizenz zum Schnueffeln Financial Times Germany, 31.8.2001; Statement of the Chaos Computer Club, available at www.ccc.de.

[2122] See *Breyer,* Council of Europe Convention on Cybercrime, DUD, 2001, 595 *et seq.*

[2123] Regarding the possibilities of making reservations, see Article 42 of the Convention on Cybercrime:
Article 42
By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

[2124] See above: § 5.2.1.

[2125] "Although Parties are obligated to introduce certain procedural law provisions into their domestic law, the modalities of establishing and implementing these powers and procedures into their legal system, and the application of the powers and procedures in specific cases, are left to the domestic law and procedures of each Party. These domestic laws and procedures, as more specifically described below, shall include conditions or safeguards, which may be provided constitutionally, legislatively, judicially or otherwise. The modalities should include the addition of certain elements as conditions or safeguards that balance the requirements of law enforcement with the protection of human rights and liberties. As the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 145.

[2126] "There are some common standards or minimum safeguards to which Parties to the Convention must adhere. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 145.

[2127] For the transformation of safeguards for Internet-related investigation techniques, see: *Taylor*, The Scope of Government Access to Copies of Electronic Communication Stored with Internet Service Providers: A Review of Legal Standards, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/taylor.pdf.

[2128] This is especially relevant with regard to the protection of the suspect of an investigation.

[2129] See: Article 37 – Accession to the Convention.
1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

[2130] ABA International Guide to Combating Cybercrime, page 139.

[2131] "Interception of telephone conversations represent[s] a serious interference with private life and correspondence and must accordingly be based upon a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated" – Case of Kruslin v. France, Application No. 11801/85.

[2132] "The requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly", Case of Malone v. United Kingdom, Application No. 8691/79.

[2133] "Powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only insofar as strictly necessary for safeguarding the democratic institutions", Case of Klass and others v. Germany, Application No. 5029/71.

[2134] "The expression "in accordance with the law", within the meaning of Article 8 § 2 (Art. 8-2), requires firstly that the impugned measure should have some basis in domestic law", Case of Kruslin v. France, Application No. 11801/85.

[2135] "Furthermore, tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject", Case of Doerga v. The Netherlands, Application No. 50210/99.

[2136] "It also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and compatible with the rule of law", Case of Kruslin v. France, Application No. 11801/85.
"Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence." Case of Malone v. United Kingdom, Application No. 8691/79.

[2137] "The cardinal issue arising under Article 8 (Art. 8) in the present case is whether the interference so found is justified by the terms of paragraph 2 of the Article (Art. 8-2). This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions", Case of Klass and others v. Germany, Application No. 5029/71.

[2138] "Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislation and jurisprudence, that the power or procedure shall be proportional to the nature and circumstances of the offence. Other States will apply related principles of their law, such as limitations on overbreadth of production orders and reasonableness requirements for searches and seizures." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.

[2139] The list is not concluding. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.

[2140] "National legislatures will have to determine, in applying binding international obligations and established domestic principles, which of the powers and procedures are sufficiently intrusive in nature to require implementation of particular conditions and safeguards." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 147.

[2141] See below: § 6.2.9

[2142] See below: § 6.2.10.

[2143] "Also, the explicit limitation in Article 21 that the obligations regarding interception measures are with respect to a range of serious offences, determined by domestic law, is an explicit example of the application of the proportionality principle." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.
"Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 230.

[2144] See below: § 6.3.4.

[2145] See below: § 6.3.7.

[2146] As explained in more detail below, Art. 16 does not oblige the provider to transfer the relevant data to the authorities. It only authorizes the law-enforcement agencies to prevent the deletion of the relevant data. The advantage of separation of the obligation to preserve the data and the obligation to disclose them is the fact that it is possible to require different conditions for their application.

[2147] A definition of the term "subscriber information" is provided in Art. 18 Subparagraph 3 of the Convention on Cybercrime.

[2148] A definition of the term "computer data" is provided in Art. 1 of the Convention on Cybercrime.

[2149] As described more in detail below, the differentiation between "computer data" and "subscriber information" in Art. 18 of the Convention on Cybercrime enables the signatory states to develop graded safeguards with regard to the production order.

[2150] "Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 155. Regarding the identification of suspects by IP-based investigations, see: *Gercke*, Preservation of User Data, DUD 2002, page 577 *et seq.*

[2151] *Gercke*, Preservation of User Data, DUD 2002, 578.

[2152] The cost issue was especially raised within the discussion on data retention legislation in the EU. See, for example: E-communications service providers remain seriously concerned with the agreement reached by European Union Justice Ministers to store records of every e-mail, phone call, fax and text message, Euroispa press release, 2005, available at: www.ispai.ie/EUROISPADR.pdf; See as well: ABA International Guide to Combating Cybercrime, page 59.

[2153] Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

[2154] The discussion already took place at the beginning of 2000. In a G8 Meeting in Tokyo experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding implementation of a data retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible." Report of the Workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001. A similar discussion took place during the negotiation of the Convention on Cybercrime. The drafters explicitly pointed out that the Convention does not establish a data retention obligation. See Explanatory Report to the Convention on Cybercrime, No. 151, available at: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

[2155] Regarding The Data Retention Directive in the European Union, see: *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law, 2007, Vol. 8, No.1, available at: http://eprints.law.duke.edu/archive/00001602/01/8_Chi._J._Int'l_L._233_(2007).pdf; *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq.*

[2156] Art. 6 Periods of Retention
Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.
Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

[2157] See: Preface 11 of the European Union Data Retention Directive: "Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive."

[2158] Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

[2159] See, for example: Draft Bill to amend title 18, United States Code, to protect youth from exploitation by adults using the Internet, and for other purposes – Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act (SAFETY) of 2007, available at: www.govtrack.us/congress/bill.xpd?bill=h110-837. Regarding the current situation in the US, see: ABA International Guide to Combating Cybercrime, page 59.

[2160] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

[2161] However, it is recommended that states consider the establishment of powers and procedures to actually order the recipient of the order to preserve the data, as quick action by this person can result in the more expeditious implementation of the preservation measures in particular cases. Explanatory Report to the Convention on Cybercrime, No. 160.

[2162] *Gercke*, Cybercrime Training for Judges, 2009, page 63, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[2163] See: *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 803.

[2164] "Preservation" requires that data which already exists in a stored form be protected from anything that would cause its current quality or condition to change or deteriorate. Explanatory Report to the Convention on Cybercrime, No. 159.

[2165] Explanatory Report, No. 152.

[2166] Regarding the advantages of a system of graded safeguards, see above: § 6.3.3.

[2167] "The reference to 'order or similarly obtain' is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive (e.g. from police or prosecutor)". See Explanatory Report to the Convention on Cybercrime, No. 160.

[2168] The drafters of the Convention on Cybercrime tried to approach the problems related to the need for immediate action from law-enforcement agencies on the one hand and the importance of ensuring safeguards on the other in a number of ways. Another example for the approach is related to the production order (Art. 18). The drafters suggested that the requirements for the handout of data to law-enforcement agencies could be adjusted in relation to the categories of data. See Explanatory Report to the Convention on Cybercrime, No. 174: "The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases."

[2169] *Gercke*, Cybercrime Training for Judges, 2009, page 64, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[2170] An IP address does not necessary immediately identify the offender. If law-enforcement agencies know the IP address an offender used to commit an offence, this information only enables them to identify the connection used to log on to the Internet. If a group of people had access to this connection (e.g. in an Internet café), further investigations are necessary to identify the offender.

[2171] If the offender is using services that do not require a registration or if the subscriber information provided by the user is not verified, Art. 18 Subparagraph 1b) will not enable the law-enforcement agencies to immediately identify the offender. Art. 18 Subparagraph 1b) is therefore especially relevant with regard to commercial services (like providing Internet access, commercial e-mail or hosting services).

[2172] *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

[2173] "Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination." See Explanatory Report to the Convention on Cybercrime, No. 167.

[2174] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[2175] Official Note: As noted in the expert group report, in some countries it may be necessary to apply the same standard for production orders as is used for a search warrant because of the nature of the material that may be produced. In other countries it may be sufficient to employ a lower standard because the production process is less invasive than the search process.

Official Note: Countries may wish to consider whether subparagraph c is appropriate for inclusion in domestic law because while it may be of great practical use, it requires the processing and compilation of data by court order, which may not be suitable for some jurisdictions.

[2176] The Commonwealth Model Law contains an alternative provision:
"Sec. 16: If a magistrate is satisfied on the basis of an *ex parte* application by a police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify:
(a) the service providers; and
(b) the path through which the communication was transmitted."

[2177] For an introduction to data retention, see: *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq.*; *Blanchette/Johnson*, Data retention and the panoptic society: The social benefits of forgetfulness, available at: http://polaris.gseis.ucla.edu/blanchette/papers/is.pdf.

[2178] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[2179] See, for example: Briefing for the Members of the European Parliament on Data Retention, available at: www.edri.org/docs/retentionletterformeps.pdf; CMBA, Position on Data retention: GILC, Opposition to data retention continues to grow, available at: www.vibe.at/aktionen/200205/data_retention_30may2002.pdf. Regarding the concerns relating to violation of the European Convention on Human Rights, see: *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq.*

[2180] See: Heise News, 13 000 determined to file suit against data retention legislation, 17.11.2007, available at: www.heise.de/english/newsticker/news/99161/from/rss09.

[2181] Case C-275/06.

[2182] See: Advocate General Opinion – 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top. The court usually but not invariably follows the adviser's conclusion.

[2183] In a G8 meeting in Tokyo, experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding an implementation of a data-retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible." Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001.

[2184] Regarding the challenges for law-enforcement agencies related to the use of means of anonymous communication, see above: § 3.2.12.

[2185] Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

[2186] An example of an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorization. In addition, he is obliged to request identification from his customers prior to the use of his services. Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[2187] See: *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 91, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf.

[2188] Regarding the impact of use of anonymous communication technology on the work of law-enforcement agencies, see above: § 3.2.12.

[2189] Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[2190] Regarding protection of the use of anonymous means of communication by the United States constitution, see: *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 82, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf.

[2191] A detailed overview of the elements of search procedures is provided by the ABA International Guide to Combating Cybercrime, 123 *et seq.* For more information on computer-related search and seizure, see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 *et seq.*; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 *et seq.* Regarding remote live search and possible difficulties with regard to the principle of chain of custody, see: *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law and Technology Vol. 9, Issue 2, 2005, available at: www.lawtechjournal.com/articles/2005/05_051201_Kenneally.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

[2192] Regarding the involvement of computer forensic experts in investigations, see above: § 6.3.2.

[2193] Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

[2194] See below: § 6.3.12.

[2195] Apart from the fact that direct access enables the law-enforcement agencies to examine the physical condition of storage media, physical access to a computer system is the only way to ensure that the files on the suspect's computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

[2196] See Explanatory Report to the Convention on Cybercrime, No. 184.

[2197] "However, in a number of jurisdictions stored computer data per se will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data." Explanatory Report to the Convention on Cybercrime, No. 184. Regarding the special demands with regard to computer-related search and seizure procedures, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

[2198] Explanatory Report, No. 184.

[2199] Regarding the difficulties of online search procedures, see below: § 6.3.12.

[2200] See in this context: *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80.

[2201] Regarding the requirements in the US, see for example: *Brenner*, Michigan Telecommunications and Technology Law Review, 2001-2002, Vol. 8, page 41 *et seq.*; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

[2202] "However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. There are several reasons for this: first, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record." Explanatory Report to the Convention on Cybercrime, No. 187.

[2203] *Gercke*, Cybercrime Training for Judges, 2009, page 69, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[2204] *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

[2205] The importance of being able to extend the search to connected computer systems was already addressed by Council of Europe Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning problems of

criminal procedural law connected with information technology that was adopted by the Committee of Ministers on 11.09.1995 at the 543rd meeting of the Ministers Deputies. The text of the recommendation is available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf.

[2206] In this context, it is important to keep in mind the principle of national sovereignty. If the information is stored on a computer system outside the territory, an extension of the search order could violate this principle. The drafters of the Convention on Cybercrime therefore pointed out: "Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be in its territory"– Explanatory Report to the Convention on Cybercrime, No. 193. With regard to this issue, see also: New Jersey Computer Evidence Search and Seizure Manual, 2000, page 12, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[2207] For guidelines how to carry out the seizure of computer equipment, see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory, available at: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[2208] Regarding the classification of the act of copying the data, see: *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 *et seq.*

[2209] "Since the measures relate to stored intangible data, additional measures are required by competent authorities to secure the data; that is, 'maintain the integrity of the data', or maintain the 'chain of custody' of the data, meaning that the data which is copied or removed be retained in the State in which they were found at the time of the seizure and remain unchanged during the time of criminal proceedings. The term refers to taking control over or the taking away of data". Explanatory Report to the Convention on Cybercrime, No. 197.

[2210] This principle also applies with regard to the seizure of hardware. Compared to maintaining the integrity of copied data it is often easier to maintain the integrity of data on a storage device.

[2211] See above: § 2.6.

[2212] One possibility to prevent access to the information without deleting it is the use of encryption technology.

[2213] See in this context: *Williger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, Vol. 10, Issue 5.

[2214] The fact that law-enforcement agencies are able to access certain data stored outside the country through a computer system in their territory does not automatically legalize the access. See Explanatory Report to the Convention on Cybercrime, No. 195. "This article does not address 'transborder search and seizure', whereby States could search and seize data in the territory of other States without having to go through the usual channels of mutual legal assistance. This issue is discussed below at the Chapter on international co-operation." Two cases of transborder access to stored computer data are regulated in Art. 32 Convention on Cybercrime:
Article 32 – Trans-border access to stored computer data with consent or where publicly available
A Party may, without the authorisation of another Party:
a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

[2215] "It addresses the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted." Explanatory Report to the Convention on Cybercrime, No. 200.

[2216] "A means to order the co-operation of knowledgeable persons would help in making searches more effective and cost efficient, both for law enforcement and innocent individuals affected. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data." Explanatory Report to the Convention on Cybercrime, No. 201.

[2217] Explanatory Report to the Convention on Cybercrime, No. 202.

[2218] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[2219] Official Note: If the existing search and seizure provisions contain a description of the content of the warrant, either in a section or by a form, it will be necessary to review those provisions to ensure that they also include any necessary reference to computer data.

[2220] Official Note: A country may wish to add a definition of "assist" which could include providing passwords, encryption keys and other information necessary to access a computer. Such a definition would need to be drafted in accordance with its constitutional or common law protections against self-incrimination.

[2221] Regarding the motivation of the drafters, see Explanatory Report to the Convention on Cybercrime, No. 171.

[2222] "A "production order" provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability." Explanatory Report to the Convention on Cybercrime, No. 171.

[2223] Explanatory Report to the Convention on Cybercrime, No. 173.

[2224] "At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement." Explanatory Report to the Convention on Cybercrime, No. 173.

[2225] Regarding the possibilities to hinder IP-based investigations by using means of anonymous communication, see above: § 3.2.12.

[2226] If the providers offer their service free of charge, they do often either require an identification of the user nor do at least not verify the registration information.

[2227] See above: § 6.3.5.

[2228] Explanatory Report to the Convention on Cybercrime, No. 172.

[2229] This can be, for example, information that was provided on a classic registration form and kept by the provider as paper records.

[2230] The Explanatory Report even points out that the parties to the Convention can adjust their safeguards with regard to specific data within each of the categories. See Explanatory Report to the Convention on Cybercrime, No. 174: "Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases."

[2231] For example, the requirement of a court order.

[2232] The differentiation between the real-time collection of traffic data (Art. 20) and the real-time collection of content data (Art. 21) shows that the drafters of the Convention realized the importance of separating instruments with different impact.

[2233] See below: § 6.3.9.

[2234] See below: § 6.3.10.

[2235] Art. 21 of the Convention on Cybercrime obliges the signatory states to implement the possibility to intercept content data only with regard to serious offences ("Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law"). On the contrary, Art. 20 of the Convention on Cybercrime is not limited to serious offences. "Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 230.

[2236] Regarding the advantages of a graded system of safeguards, see above: § 6.3.3.

[2237] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[2238] Official Note: As noted in the expert group report, in some countries it may be necessary to apply the same standard for production orders as is used for a search warrant because of the nature of the material that may be produced. In other countries it may be sufficient to employ a lower standard because the production process is less invasive than the search process.
Official Note: Countries may wish to consider whether subparagraph c is appropriate for inclusion in domestic law because while it may be of great practical use, it requires the processing and compilation of data by court order, which may not be suitable for some jurisdictions.

[2239] Regarding the legislation on legal interception in Great Britain, Canada, South Africa, United States (New York) and Israel, see: Legal Opinion on Intercept Communication, 2006, available at: www.law.ox.ac.uk/opbp/OPBP%20Intercept%20Evidence%20Report.pdf.

[2240] In these cases, other technical solutions for surveillance need to be evaluated. Regarding possible physical surveillance techniques, see: *Slobogin*, Technologically-assisted physical surveillance: The American Bar Association's Tentative Draft Standards, Harvard Journal of Law & Technology, Vol. 10, Nr. 3, 1997, page 384 *et seq.*

[2241] Regarding the interception of VoIP to assist law-enforcement agencies, see: *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[2242] Regarding the interception of VoIP to assist law-enforcement agencies, see: ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 48, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.htm; *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[2243] In particular, lack of technical preparation of Internet providers to collect the relevant data in real time.

[2244] Explanatory Report to the Convention on Cybercrime, No. 205.

[2245] ABA International Guide to Combating Cybercrime, page 125.

[2246] ABA International Guide to Combating Cybercrime, page 125.

[2247] The "origin" refers to a telephone number, Internet protocol (IP) address or similar identification of a communications facility to which a service provider renders services. Explanatory Report to the Convention on Cybercrime, No. 30.

[2248] "In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation.

Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive." See: Explanatory Report to the Convention on Cybercrime, No. 29. Regarding the importance of traffic data in cybercrime investigations, see also: ABA International Guide to Combating Cybercrime, page 125; *Gercke*, Preservation of User Data, DUD 2002, 577 *et seq.*

[2249] "In general, the two possibilities for collecting traffic data in paragraph 1(a) and (b) are not alternatives. Except as provided in paragraph 2, a Party must ensure that both measures can be carried out. This is necessary because if a service provider does not have the technical ability to assume the collection or recording of traffic data (1(b)), then a Party must have the possibility for its law enforcement authorities to undertake themselves the task (1(a))." Explanatory Report to the Convention on Cybercrime, No. 223.

[2250] The Convention does not define technical standards regarding the design of such an interface. Explanatory Report to the Convention on Cybercrime, No. 220.

[2251] Explanatory Report to the Convention on Cybercrime, No. 223.

[2252] "The article [Art. 20] does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems." Explanatory Report to the Convention on Cybercrime, No. 221.

[2253] See above: § 3.2.12.

[2254] Tor is a software that enables users to protect against traffic analysis. For more information about the software, see: http://tor.eff.org/.

[2255] An example of an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorization. In addition, he is obliged to request an identification from his customers prior to the use of his services. Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[2256] This advantage is also relevant for remote forensic investigations. See below: § 6.3.12.

[2257] Such obligation might be legal or contractual.

[2258] Explanatory Report to the Convention on Cybercrime, No. 226.

[2259] Regarding the key intention, see Explanatory Report on the Convention on Cybercrime No. 16: "The Convention aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation."

[2260] The drafters of the Convention point out that the signatory states should limit the use of the right to make reservations in this context: Explanatory Report to the Convention on Cybercrime, No. 213.
Regarding the possibilities of making reservations, see Art. 42 Convention on Cybercrime:
Article 42
By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No. other reservation may be made.

[2261] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers,* Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade

and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[2262] One possibility to prevent law-enforcement agencies from analysing the content exchanged between two suspects is the use of encryption technology. Regarding the functioning of encryption procedures, see: *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

[2263] Regarding the impact of encryption technology on computer forensic and criminal investigations, see: *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding legal solutions designed to address this challenge, see below: § 6.3.11.

[2264] *Schneier*, Applied Cryptography, page 185.

[2265] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[2266] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[2267] *Schneier*, Applied Cryptography, page 185.

[2268] Regarding practical approaches to recover encrypted evidence, see: *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at:

[2269] The issue is, for example, addressed by Recommendation No. R (95) of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with information, 11 September 1995: "14. Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary" and the G8 in the 1997 Meeting in Denver: "To counter, inter alia, the use of strong encryption by terrorists, we have endorsed acceleration of consultations and adoption of the OECD guidelines for cryptography policy and invited all states to develop national policies on encryption, including key, management, which may allow, consistent with these guidelines. Lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies."

[2270] For more information, see: *Koops*, The Crypto Controversy. A Key Conflict in the Information Society, Chapter 5.

[2271] The need for such authorization is mentioned, for example, in principle 6 of the 1997 Guidelines for Cryptography Policy: "National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible."

[2272] This topic was discussed in the deliberations of the US District Court of New Jersey in the case United States v. Scarfo. The District Court decided that the federal wiretapping law and the Fourth Amendment allow law-enforcement agencies to make use of a software to record keystrokes on a suspect's computer (keylogger) in order to intercept a passphrase to an encrypted file (if the system does not operate while the computer is communicating with other computers). See: www.epic.org/crypto/scarfo/opinion.html.

[2273] Export limitations on encryption software capable of processing strong keys are not designed to facilitate the work of law-enforcement agencies in the country. The intention of such regulations is to prevent the availability of the technology outside the country. For detailed information on import and export restrictions with regard to encryption technology, see: http://rechten.uvt.nl/koops/cryptolaw/index.htm.

[2274] The limitation of the import of such powerful software is even characterized as "misguided and harsh to the privacy rights of all citizens". See, for example: The Walsh Report – Review of Policy relating to Encryption Technologies 1.1.16 available at: www.efa.org.au/Issues/Crypto/Walsh/walsh.htm.

[2275] See: *Lewis*, Encryption Again, available at: www.csis.org/media/csis/pubs/011001_encryption_again.pdf.

[2276] The key escrow system was promoted by the United States Government and implemented in France for a period in 1996. For more information, see: Cryptography and Liberty 2000 – An International Survey of Encryption Policy, available at: http://www2.epic.org/reports/crypto2000/overview.html#Heading9.

[2277] See: *Diehl*, Crypto Legislation, Datenschutz und Datensicherheit, 2008, page 243 *et seq.*

[2278] "To counter, inter alia, the use of strong encryption by terrorists, we have endorsed acceleration of consultations and adoption of the OECD guidelines for cryptography policy and invited all states to develop national policies on encryption, including key, management. which may allow, consistent with these guidelines. lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies", www.g7.utoronto.ca/summit/1997denver/formin.htm.

[2279] See, for example: Antigua and Barbuda, Computer Misuse Bill 2006, Art. 25, available at: www.laws.gov.ag/bills/2006/computer-misuse-bill-2006.pdf; Australia, Cybercrime Act, Art. 12, available at: http://scaleplus.law.gov.au/html/comact/11/6458/pdf/161of2001.pdf; Belgium, Wet van 28 november 2000 inzake informaticacriminaliteit, Art. 9 and Code of Criminal Procedure, Art. 88, available at: http://staatsbladclip.zita.be/staatsblad/wetten/2001/02/03/wet-2001009035.html; France, Loi pour la confiance dans l'économie numérique, Section 4, Art. 37, available at: www.legifrance.gouv.fr/affichTexte.do;jsessionid=B78A2A8ED919529E3B420C082708C031.tpdjo12v_3?cidTexte=JORFTEXT000000801164&dateTexte=20080823; United Kingdom, Regulation of Investigatory Powers Act 2000, Art. 49, available at: www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1; India, The Information Technology Act, 2000, Art. 69, available at: www.legalserviceindia.com/cyber/itact.html; Irland, Electronic Commerce Act, 2000, Art. 27, available at: www.irlgov.ie/bills28/acts/2000/a2700.pdf; Malaysia, Communications and Multimedia Act, Section 249, available at: www.msc.com.my/cyberlaws/act_communications.asp; Morocco, Loi relative à l'échange électronique de données juridiques, Chapter III, available at: http://droitmaroc.wordpress.com/2008/01/29/loi-n%C2%B0-53-05-relative-a-lechange-electronique-de-donnees-juridiques-integrale/; Netherlands, Wet op de inlichtingen en veiligheidsdiensten 2002, Art. 89, available at www.legalserviceindia.com/cyber/itact.html; South Africa, Regulation of Interception of Communications and Provisions of Communications-Related Information Act, Art. 21, available at: www.info.gov.za/gazette/acts/2002/a70-02.pdf; Trinidad and Tobago, The Computer Misuse Bill 2000, Art. 16, available at: www.ttcsweb.org/articles/computer-laws/computer-misuse-act-2000/compbill.pdf.

[2280] An example can be found in Sec. 69 of the Indian Information Technology Act 2000: "Directions of Controller to a subscriber to extend facilities to decrypt information.(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. (2) The subscriber or any person in-charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information." For more information about the Indian Information Technology Act 2000, see: *Duggal*, India's Information Technology Act 2000, available under: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002090.pdf.

[2281] For general information on the Act, see: *Brown/Gladman*, The Regulation of Investigatory Powers Bill – Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses, available at: www.fipr.org/rip/RIPcountermeasures.htm; *Ward*, Campaigners hit by decryption law, BBC News, 20.11.2007, available at: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm; ABA International Guide to Combating Cybercrime, page 32.

[2282] For an overview of the regulation, see: *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

[2283] Regarding the discussion of protection against self-incrimination under United States law, see for example: *Clemens*, No Computer Exception to the Constitution: The First Amendment Protects Against Compelled Production of an Encrypted Document or Private key, UCLA Journal of Law and Technology, Vol. 8, Issue 1, 2004; *Sergienko*, Self Incrimination and Cryptographic Keys, Richmond Journal of Law & Technology, 1996, available at: www.richmond.edu/jolt/v2i1/sergienko.html; *O'Neil*, Encryption and the First Amendment, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art1.pdf; *Fraser*, The Use of Encrypted, Coded and Secret Communication is an "Ancient Liberty" Protected by the United States Constitution, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art2.pdf; *Park*, Protecting the Core Values of the First Amendment in an age of New Technology: Scientific Expression vs. National Security, Virginia Journal of Law and

Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art3.pdf; Hearing before the Subcommittee on the Constitution, Federalism, and Property Rights of the Committee on the Judiciary, United States Senate, 150 Congress, Second Session on Examining the Use of Encryption, available at: www.loc.gov/law/find/hearings/pdf/00139296461.pdf.

Regarding the discussion in Europe on self-incrimination, in particular with regard to the European Convention on Human Rights (ECHR), see: *Moules*, The Privilege against self-incrimination and the real evidence, The Cambridge Law Journal, 66, page 528 *et seq.*; *Mahoney*, The Right to a Fair Trail in Criminal Matters under Art. 6 ECHR, Judicial Studies Institute Journal, 2004, page 107 *et seq.*; *Birdling*, Self-incrimination goes to Strasbourg: O'Halloran and Francis vs. United Kingdom, International Journal of Evidence and Proof, Vol. 12, Issue 1, 2008, page 58 *et seq.*; Commission of the European Communities, Green Paper on the Presumption of Innocence, COM (2006) 174, page 7, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0174:FIN:EN:pdf.

[2284] Regarding the situation in the US, see: *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

[2285] In this context, see also: *Walker*, Encryption, and the Regulation of Investigatory Powers Act 2000, available at: www.bileta.ac.uk/01papers/walker.html.

[2286] *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

[2287] Regarding possibilities to circumvent the obligations, see: *Ward*, Campaigners hit by decryption law, BBC News, 20.11.2007, available at: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm.

[2288] A detailed overview of the elements of search procedures as well as the challenges of carrying them out is provided by the ABA International Guide to Combating Cybercrime, 123 *et seq.* For more information on computer-related search and seizure, see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 *et seq.*; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 *et seq.*

[2289] Regarding the threat that the suspect could manipulate or delete evidence and the related obligation to keep information about an ongoing investigation based on Art. 20 confidential, see above: § 6.3.9.

[2290] There are disadvantages related to remote investigations. Apart from the fact that direct access enables law-enforcement agencies to examine the physical condition of storage media, physical access to a computer system it is the only way to ensure that the files on the suspect's computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

[2291] Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

[2292] See: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf; *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3, available at: http://assets.opencrs.com/rpts/RL32706_20070926.pdf; *Green*, FBI Magic Lantern reality check, The Register, 03.12.2001, available at: www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/; *Salkever*, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.200, available at:

www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; *Abreu*, FBI confirms "Magic Lantern" project exists, 2001, available at: www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

[2293] See: *McCullagh*; FBI remotely installs spyware to trace bomb threat, News.com, 18.07.2007, available at: www.news.com/8301-10784_3-9746451-7.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf; Secret online search warrant: FBI uses CIPAV for the first time, Heise News, 19.07.2007, available at: www.heise-security.co.uk/news/92950.

[2294] Computer and Internet protocol address verifier.

[2295] A copy of the search warrant is available at: http://blog.wired.com/27bstroke6/files/timberline_affidavit.pdf. Regarding the result of the search, see: www.politechbot.com/docs/fbi.cipav.sanders.search.warrant.071607.pdf. For more information about CIPAV, see: *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007, available at: www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV for the first time, Heise Security News, 19.07.2007, available at: www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950; *Poulsen*, FBI's Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007, available at: www.wired.com/politics/law/news/2007/07/fbi_spyware; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008, available at: www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007, available at: http://news.zdnet.com/2100-1009_22-6197405.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.

[2296] Regarding the discussion in Germany, see: The German government is recruiting hackers, Forum for Incident Response and Security Teams, 02.12.2007, available at: www.first.org/newsroom/globalsecurity/179436.html; Germany to bug terrorists' computers, The Sydney Morning Herald, 18.11.2007, available at: www.smh.com.au/news/World/Germany-to-bug-terrorists-computers/2007/11/18/1195321576891.html; *Leyden*, Germany seeks malware "specialists" to bug terrorists, The Register, 21.11.2007, available at: www.theregister.co.uk/2007/11/21/germany_vxer_hire_plan/; Berlin's Trojan, Debate Erupts over Computer Spying, Spiegel Online International, 30.08.2007, available at: www.spiegel.de/international/germany/0,1518,502955,00.html.

[2297] See: Tagesspiegel, Die Ermittler sufen mit, 8.12.2006, available at: www.tagesspiegel.de/politik/;art771,1989104.

[2298] For an overview, see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 *et seq.*

[2299] The search function was the focus of the decision of the German Supreme Court in 2007. See: Online police searches found illegal in Germany, 14.02.2007, available at: www.edri.org/edrigram/number5.3/online-searches.

[2300] Regarding investigations involving VoIP, see: *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[2301] See: *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf. Keylogging is the focus of the FBI software "magic lantern". See: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3, available at: http://assets.opencrs.com/rpts/RL32706_20070926.pdf. See also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[2302] This is the focus of the US investigation software CIPAV. Regarding the functions of the software, see the search warrant, available at: http://blog.wired.com/27bstroke6/files/timberline_affidavit.pdf.

[2303] Regarding these functions, see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 *et seq.*

[2304] Regarding the possible ways of infecting a computer system by spyware, see: The spying game: how spyware threatens corporate security, Sophos white paper, 2005, available at: www.cehs.usu.edu/facultyandstaff/security/sophos-spyware-wpus.pdf.

[2305] With regard to the efficiency of virus scanners and protection measures implemented in the operating systems, it is likely that the functioning of a remote forensic software would require the cooperation of software companies. If software companies agree to prevent detection of remote forensic software, this could result in serious risks for computer security. For more information, see: *Gercke*, Computer und Recht 2007, page 249.

[2306] If the offender stores illegal content on an external storage device that is not connected to a computer system, the investigators will in general not be able to identify the content if they only have access to the computer system via remote forensic software.

[2307] Regarding the importance of maintaining integrity during a forensic investigation, see: *Hosmer*, Providing the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[2308] National sovereignty is a fundamental principle in international law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[2309] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[2310] Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[2311] See above: § 3.2.12.

[2312] Based on Art. 7, "anyone running an establishment open to the public or any kind of private association where devices or terminals, which can be used for electrnic data transmission or other communications, are made available to the public, to customers or members" is obliged to require a licence from local authorities and identify persons using the service. For more information, see: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq*.

[2313] Decree 144/2005, 27 July 2005 ("Decreto-legge"). Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article, Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[2314] For more details, see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*

[2315] *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 95.

[2316] Regarding the related challenges, see: *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2, page 6 *et seq.*

[2317] International Mechanisms for Promoting Freedom of Expression, Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2005.

[2318] *Büllingen/Gillet/Gries/Hillebrand/Stamm*, Situation and Perspectives of Data Retention in an international comparison (Stand und Perspectiven der Vorratsdatenspeichung im internationalen Vergleich), 2004, page 10, available at: www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf.

[2319] *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

[2320] Regarding the transnational dimension of cybercrime, see: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289, available at: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[2321] See above: § 3.2.7.

[2322] See *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 451 *et seq.*, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page xvii, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[2323] See, in this context: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[2324] *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2, page 156, available at: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

[2325] *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141.

[2326] The need to speed up the process of international cooperation is pointed out in the Explanatory Report. See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

[2327] Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

[2328] The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and, the Protocol against the Smuggling of Migrants by Land, Sea and Air and the Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition.

[2329] Inter-American Convention on Mutual Assistance in Criminal Matters, 1992, Treaty Series, OAS, No. 75. The text of the Convention and a list of signatures and ratifications is available at: www.oas.org/juridico/english/sigs/a-55.html.

[2330] European (Council of Europe) Convention on Mutual Assistance in Criminal Matters, 1959, ETS 30.

[2331] Council of Europe Convention on Cybercrime, ETS 185.

[2332] See in this context the UN Model Treaty on Mutual Legal Assistance, 1999, A/RES/45/117; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[2333] A full list of agreements is available at: www.ag.gov.au/www/agd/agd.nsf/page/Extradition_and_mutual_assistanceRelationship_with_other_countries.

[2334] Second Meeting of Ministers of Justice or of Misters or Attorney General of the American on Cybercrime, Background Documents on the Developments on Cyber Crime in the Framework of the REMJAS and the OAS, 1999, Chapter III, available at: www.oas.org/juridico/english/cybGE_IIIrep3.pdf.

[2335] See in this regard: *Pop*, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science, 2008, page 160 *et seq.*; *Stowell*, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931, page 262; Recueil Des Cours, Collected Courses, Hague Academy of International Law, 1976, page 119.

[2336] Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.pdf.

[2337] *Choo,* Trends in Organized Crime, 2008, page 273.

[2338] *Brenner*, Organized Cybercrime, North Carolina Journal of Law & Technology, 2002, Issue 4, page 27.

[2339] See, for example: Great Britain Crown Prosecution Service, Convictions for internet rape plan, Media release, 01.12.2006.

[2340] *Choo,* Trends in Organized Crime, 2008, page 273.

[2341] For further details, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[2342] According to the report of the expert meeting held between 8 and 10 October 2008, there are certain states which require special provisions in their internal law to allow such spontaneous information, while others can transmit information spontaneously without such internal provisions in force: see CTOC/COP/2008/18 page 5.

[2343] For details about the intention of the drafters, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 226, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[2344] For details, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 225, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[2345] See, for example, Art. 29 and Art. 35 Convention on Cybercrime.

[2346] The directory is available at: www.unodc.org/compauth/en/index.html. Access requires registration and is reserved for competent national authorities.

[2347] The directory indicates the central authority responsible for receiving the MLA request, languages accepted, channels of communication, contact points, fax and e-mails, specific requests of the receiving states and sometimes even extracts from domestic legislation of that state.

[2348] See CTOC/COP/2008/18, paragraph 27.

[2349] See Art. 25, paragraph 3 of the Convention on Cybercrime.

[2350] The software is available at: www.unodc.org/mla/index.html.

[2351] See Explanatory Report to the Convention on Cybercrime, No. 243. The Member States have the possibility to limit the international cooperation with regard to certain measures (extradition, real time collection of traffic data and the interception of content data).

[2352] If, for example, two countries involved in a cybercrime investigation already have bilateral agreements in place that contain the relevant instruments, those agreements will remain a valid basis for the international cooperation

[2353] Regarding the difficulties with the dual criminality principle, see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 *et seq.*, available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

[2354] The Explanatory Report clarifies that the determination of the covered offences does not depend on the actual penalty imposed in the particular cases. See: Explanatory Report to the Convention on Cybercrime, No. 245.

[2355] Regarding the dual criminality principle, see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 *et seq.*, available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

[2356] See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

[2357] See above: § 3.2.10.

[2358] See Explanatory Report to the Convention on Cybercrime, No. 256.

[2359] This information often leads to successful international investigations. For an overview of large-scale international investigations related to child pornography, see: *Krone*, International Police Operations Against Online Child Pornography, Trends and Issues in Crime and Criminal Justice, No. 296, page 4, available at: www.ecpat.se/upl/files/279.pdf.

[2360] Similar instruments can be found in other Council of Europe conventions. For example, Article 10 of the Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and Article 28 of the Criminal Law Convention on Corruption. Council of Europe conventions are available at: www.coe.int.

[2361] See Explanatory Report to the Convention on Cybercrime, No. 262.

[2362] Regarding the 24/7 network points of contact, see below: § 6.4.12.

[2363] See Explanatory Report to the Convention on Cybercrime, No. 265: "Initially, direct transmission between such authorities is speedier and more efficient than transmission through diplomatic channels. In addition, the establishment of an active central authority serves an important function in ensuring that both incoming and outgoing requests are diligently pursued, that advice is provided to foreign law enforcement partners on how best to satisfy legal requirements in the requested Party, and that particularly urgent or sensitive requests are dealt with properly."

[2364] See Explanatory Report to the Convention on Cybercrime, No. 268.

[2365] See Explanatory Report to the Convention on Cybercrime, No. 269. "Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests), furnishing the specific data sought by the requesting Party would raise difficulties so fundamental as to be considered by the requested Party to fall within the essential interests ground of refusal."

[2366] See Explanatory Report to the Convention on Cybercrime, No. 269.

[2367] See above: § 6.3.

[2368] The most important instruments established by the Convention on Cybercrime are: Expedited preservation of stored computer data (Art. 16), Expedited preservation and partial disclosure of traffic data (Art. 17), Production order (Art. 18), Search and seizure of stored computer data (Art. 19), Real-time collection of traffic data (Art. 20), Interception of content data (Art. 21).

[2369] National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[2370] An exemption is Art. 32 of the Convention on Cybercrime – See below. Regarding the concerns related to this instrument, see: Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2: " […] Russian Federation (had a positive approach towards the Convention but further consideration would have to be given to Article 32b in particular in the light of experience gained from the use of this Article).

[2371] See above: § 6.3.4.

[2372] See above: § 6.3.4.

[2373] See above: § 6.3.7.

[2374] See above: § 6.3.6.

[2375] See above: § 6.3.9.

[2376] See above: § 6.3.10.

[2377] See Explanatory Report to the Convention on Cybercrime, No. 293.

[2378] "The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules." See Explanatory Report to the Convention on Cybercrime, No. 293.

[2379] See below in this chapter.

[2380] See Explanatory Report to the Convention on Cybercrime, No. 293.

[2381] Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2.

[2382] See: Challenges and Best Practices in Cybercrime Investigation, 2008, available at: www.unafei.or.jp/english/pdf/PDF_rms/no79/15_P107-112.pdf.

[2383] National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[2384] For more information, see: A Draft Commentary on the Council of Europe Convention, October 2000, available at: www.privacyinternational.org/issues/cybercrime/coe/analysis22.pdf.

[2385] In this context, it is necessary to point out a difference between Art. 32 and Art. 18. Unlike Art. 18, Art. 32 does not enable a foreign law-enforcement agency to order the submission of the relevant data. It can only seek permission.

[2386] Communiqué of the Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Moscow, 19-20 October 1999.

[2387] Principles on Transborder Access to Stored Computer Data, available at: www.justice.gov/criminal/cybercrime/g82004/99TransborderAccessPrinciples.pdf.

[2388] The need to speed up the process of international cooperation is pointed out in the Explanatory Report. See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

[2389] See above: § 6.3.4.

[2390] Availability 24 hours a day and 7 days a week is especially important with regard to the international dimension of cybercrime, as requests can potentially come from any time zone in the world. Regarding the international dimension of cybercrime and the related challenges, see above: § 3.2.6.

[2391] See Explanatory Report to the Convention on Cybercrime, No. 298.

[2392] Regarding the activities of the G8 in the fight against cybercrime, see above: § 5.1.1. For more information on the 24/7 Network, see: *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 484, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.

[2393] See above: § 3.2.10.

[2394] See above: § 3.2.6.

[2395] Regarding the question of which authorities should be authorized to order the preservation of data, see above: § 6.3.4.

[2396] Explanatory Report to the Convention on Cybercrime, No. 301.

[2397] Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 5 (35).

[2398] *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf

[2399] The Functioning of 24/7 points of contact for cybercrime, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf.

[2400] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at:

http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[2401] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[2402] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[2403] Regarding the network architecture and the consequences with regard to the involvement of service providers, see: *Black*, Internet Architecture: An Introduction to IP Protocols, 2000; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003, available at: http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html.

[2404] See in this context: *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf.

[2405] National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[2406] For an introduction to the discussion, see: *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.,* available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

[2407] In the decision Recording Industry Association Of America v. Charter Communications, Inc., the United States Court of Appeals for the eighth circuit described (by referring to House Report No. 105-551(II) at 23 (1998)) the function of the United States DMCA by pointing out the balance. In the opinion of the court, DMCA has "two important priorities: promoting the continued growth and development of electronic commerce and protecting intellectual property rights."

[2408] Regarding the history of DMCA and pre-DMCA case law in the United States, see: *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Salow*, Liability Immunity for Internet Service Providers – How is it working?, Journal of Technology Law and Policy, Vol. 6, Issue 1, 2001, available at: http://grove.ufl.edu/~techlaw/vol6/issue1/pearlman.html.

[2409] Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf; *Schwartz*, Thinking outside the Pandora's box: Why the DMCA is unconstitutional under Article I, § 8 of the United States Constitution, Journal of Technology Law and Policy, Vol. 10, Issue 1, available at: http://grove.ufl.edu/~techlaw/vol10/issue1/schwartz.html.

[2410] Regarding the application of DMCA to search engines, see: *Walker*, Application of the DMCA Safe Harbor Provisions to Search Engines, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf.

[2411] 17 USC. § 512(a)

[2412] 17 USC. § 512(b)

[2413] Regarding the Communications Decency Act, see: *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf;

[2414] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') – Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union e-commerce regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*, available at: www.law.du.edu/ilj/online_issues_folder/pappas.7.15.03.pdf.

[2415] See *Lindholm/Maennel*, Computer Law Review International 2000, 65.

[2416] Art. 12 – Art. 15 EU of the E-Commerce Directive.

[2417] With the number of different services covered, the E-Commerce Directive aims for a broader regulation than 17 USC. § 517(a). Regarding 17 USC. § 517(a).

[2418] See Art. 12 paragraph 3 of the E-Commerce Directive.

[2419] The provision was implemented by DMCA (Digital Millennium Copyright Act). Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

[2420] Regarding traditional caching as well as active caching, see: *Naumenko*, Benefits of Active Caching in the WWW, available at: www.epfl.ch/Publications/Naumenko/Naumenko99.pdf.

[2421] For more information on proxy servers, see: *Luotonen*, Web Proxy Servers, 1997.

[2422] The provision was implemented by DMCA (Digital Millennium Copyright Act). Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

[2423] See above: § 6.5.4.

[2424] Regarding the impact of free webspace on criminal investigations, see: *Evers*, Blogging sites harbouring cybercriminals, CNET News, 26.07.2005, available at: http://news.zdnet.co.uk/security/0,1000000189,39210633,00.htm.

[2425] This procedure is called "notice and takedown".

[2426] The hosting provider is quite often in a difficult situation. On the one hand, it needs to react immediately to avoid liability; on the other hand, it has certain obligations to its customers. If it removes legal information that was just at first sight illegal, this could lead to claims for indemnity.

[2427] By enabling their customers to offer products, they provide the necessary storage capacity for the required information.

[2428] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[2429] See the Explanatory Note to the HIPCAR cybercrime model legislative text available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[2430] See the Explanatory Note to the HIPCAR cybercrime model legislative text available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[2431] *Spindler*, Multimedia und Recht 1999, page 204.

[2432] Art. 21 – Re-examination

> 1. Before 17 July 2003, and thereafter every two years, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, accompanied, where necessary, by proposals for adapting it to legal, technical and economic developments in the field of information society services, in particular with respect to crime prevention, the protection of minors, consumer protection and to the proper functioning of the internal market.
> 2. In examining the need for an adaptation of this Directive, the report shall in particular analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services, 'notice and take down'

procedures and the attribution of liability following the taking down of content. The report shall also analyse the need for additional conditions for the exemption from liability, provided for in Articles 12 and 13, in the light of technical developments, and the possibility of applying the internal market principles to unsolicited commercial communications by electronic mail.

[2433] *Freytag*, Computer und Recht 2000, page 604; *Spindler*, Multimedia und Recht 2002, page 497.

[2434] Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

[2435] See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

[2436] § 17 – Ausschluss der Verantwortlichkeit bei Links

(1) Ein Diensteanbieter, der mittels eines elektronischen Verweises einen Zugang zu fremden Informationen eröffnet, ist für diese Informationen nicht verantwortlich, sofern er von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder, sobald er diese Kenntnis oder dieses Bewusstsein erlangt hat, unverzüglich tätig wird, um den elektronischen Verweis zu entfernen.

[2437] *Introna/Nissenbaum*, Sharping the Web: Why the politics of search engines matters, page 5, available at: www.nyu.edu/projects/nissenbaum/papers/searchengines.pdf.

[2438] Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

[2439] See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

[2440] Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) – Artículo 17. Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda (Spain)
1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que: a) No. tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o b) si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.
Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere la letra a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.
2. La exención de responsabilidad establecida en el apartado primero no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.

[2441] Ausschluss der Verantwortlichkeit bei Suchmaschinen
§ 14. (1) Ein Diensteanbieter, der Nutzern eine Suchmaschine oder andere elektronische Hilfsmittel zur Suche nach fremden Informationen bereitstellt, ist für die abgefragten Informationen nicht verantwortlich, sofern er
1. die Übermittlung der abgefragten Informationen nicht veranlasst,
2. den Empfänger der abgefragten Informationen nicht auswählt und
3. die abgefragten Informationen weder auswählt noch verändert.
(2) Abs. 1 ist nicht anzuwenden, wenn die Person, von der die abgefragten Informationen stammen, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

**Office of the Director**
**Telecommunication Development Bureau (BDT)**
Place des Nations
CH-1211 Geneva 20
Email: mailto:bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax.: +41 22 730 5484

**Deputy to the Director and Administration and Operations Coordination Department (DDR)**
Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5784
Fax: +41 22 730 5484

**Infrastructure Enabling Environmnent and E-Applications Department (IEE)**
Email: bdtiee@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

**Innovation and Partnership Department (IP)**
Email: bdtip@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

**Project Support and Knowledge Management Department (PKM)**
Email: bdtpkm@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

# Africa

## Ethiopia
**International Telecommunication Union (ITU)**
**Regional Office**
P.O. Box 60 005
Gambia Rd. Leghar ETC Bldg 3rd Floor
Addis Ababa – Ethiopia
E-mail: itu-addis@itu.int
Tel.: +251 11 551 49 77
Tel.: +251 11 551 48 55
Tel.: +251 11 551 83 28
Fax.: +251 11 551 72 99

## Cameroon
**Union internationale des télécommunications (UIT)**
**Bureau de zone**
Immeuble CAMPOST, 3ème étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroun
E-mail: itu-yaounde@itu.int
Tel.: + 237 22 22 92 92
Tel.: + 237 22 22 92 91
Fax.: + 237 22 22 92 97

## Senegal
**Union internationale des télécommunications (UIT)**
**Bureau de zone**
Immeuble Fayçal, 4ème Etage
19, Rue Parchappe x Amadou Assane Ndoye
Boîte postale 50202 Dakar RP
Dakar – Sénégal
E-mail: itu-dakar@itu.int
Tel.: +221 33 849 77 20
Fax.: +221 33 822 80 13

## Zimbabwe
**International Telecommunication Union (ITU)**
**Area Office**
TelOne Centre for Learning
Corner Samora Machel and Hampton Road
P.O. Box BE 792
Belvedere Harare, Zimbabwe
E-mail: itu-harare@itu.int
Tel.: +263 4 77 59 41
Tel.: +263 4 77 59 39
Fax. +263 4 77 12 57

# Americas

## Brazil
**International Telecommunication Union (ITU)**
**Regional Office**
SAUS Quadra 06 Bloco "E"
11 andar – Ala Sul
Ed. Luis Eduardo Magalhães (AnaTel.) –
CEP 70070-940 – Brasilia – DF – Brasil
E-mail: itubrasilia@itu.int
Tel.: +55 61 2312 2730
Tel.: +55 61 2312 2733
Tel.: +55 61 2312 2735
Tel.: +55 61 2312 2736
Fax.: +55 61 2312 2738

## Barbados
**International Telecommunication Union (ITU)**
**Area Office**
United Nations House
Marine Gardens
Hastings – Christ Church
P.O. Box 1047
Bridgetown – Barbados
E-mail: itubridgetown@itu.int
Tel.: +1 246 431 0343/4
Fax.: +1 246 437 7403

## Chile
**Unión Internacional de Telecomunicaciones (UIT)**
**Oficina de Representación de Área**
Merced 753, Piso 4
Casilla 50484 – Plaza de Armas
Santiago de Chile – Chile
E-mail: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax.: +56 2 632 6154

## Honduras
**Unión Internacional de Telecomunicaciones (UIT)**
**Oficina de Representación de Área**
Colonia Palmira, Avenida Brasil
Edificio COMTELCA/UIT 4 Piso
P.O. Box 976
Tegucigalpa – Honduras
E-mail: ituteguciglapa@itu.int
Tel.: +504 2 201 074
Fax. +504 2 201 075

# Arab States

## Egypt
**International Telecommunication Union (ITU)**
**Regional Office**
c/o National Telecommunications Institute Bldg (B 147)
Smart Village – Km 28
Cairo – Alexandria Desert Road
6th October Governorate – Egypt
E-mail: itucairo@itu.int
Tel.: +20 2 35 37 17 77
Fax.: +20 2 35 37 18 88

# Asia and the Pacific

## Thailand
**International Telecommunication Union (ITU)**
**Regional Office**
3rd Floor Building 6,
TOT Public Co., Ltd
89/2 Chaengwattana Road, Laksi
Bangkok 10210 – Thailand
Mailing address:
P.O. Box 178, Laksi Post Office
Bangkok 10210, Thailand
E-mail: itubangkok@itu.int
Tel.: +66 2 574 8565/9
Tel.: +66 2 574 9326/7
Fax.: +66 2 574 9328

## Indonesia
**International Telecommunication Union (ITU)**
**Area Office**
Sapta Pesona Building, 13th floor
Jl. Merdeka Barat No. 17
Jakarta 10110 – Indonesia
Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta – Indonesia
E-mail: itujakarta@itu.int
Tel.: +62 21 381 35 72
Tel.: +62 21 380 23 22
Tel.: +62 21 380 23 24
Fax.: +62 21 389 05 521

# CIS countries

## Russian Federation
**International Telecommunication Union (ITU)**
**Area Office**
4, building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation
Mailing address:
P.O. Box 25 – Moscow 105120
Russian Federation
E-mail: itumoskow@itu.int
Tel.: +7 495 926 60 70
Fax. +7 495 926 60 73

# Europe

## Switzerland
**International Telecommunication Union ( ITU) Europe Unit EUR**
**Telecommunication Development Bureau BDT**
Place des Nations
CH-1211 Geneva 20 – Switzerland
E-mail: eurregion@itu.int
Tel.: +41 22 730 5111



International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

Printed in Switzerland
Geneva, 2012

09/2012