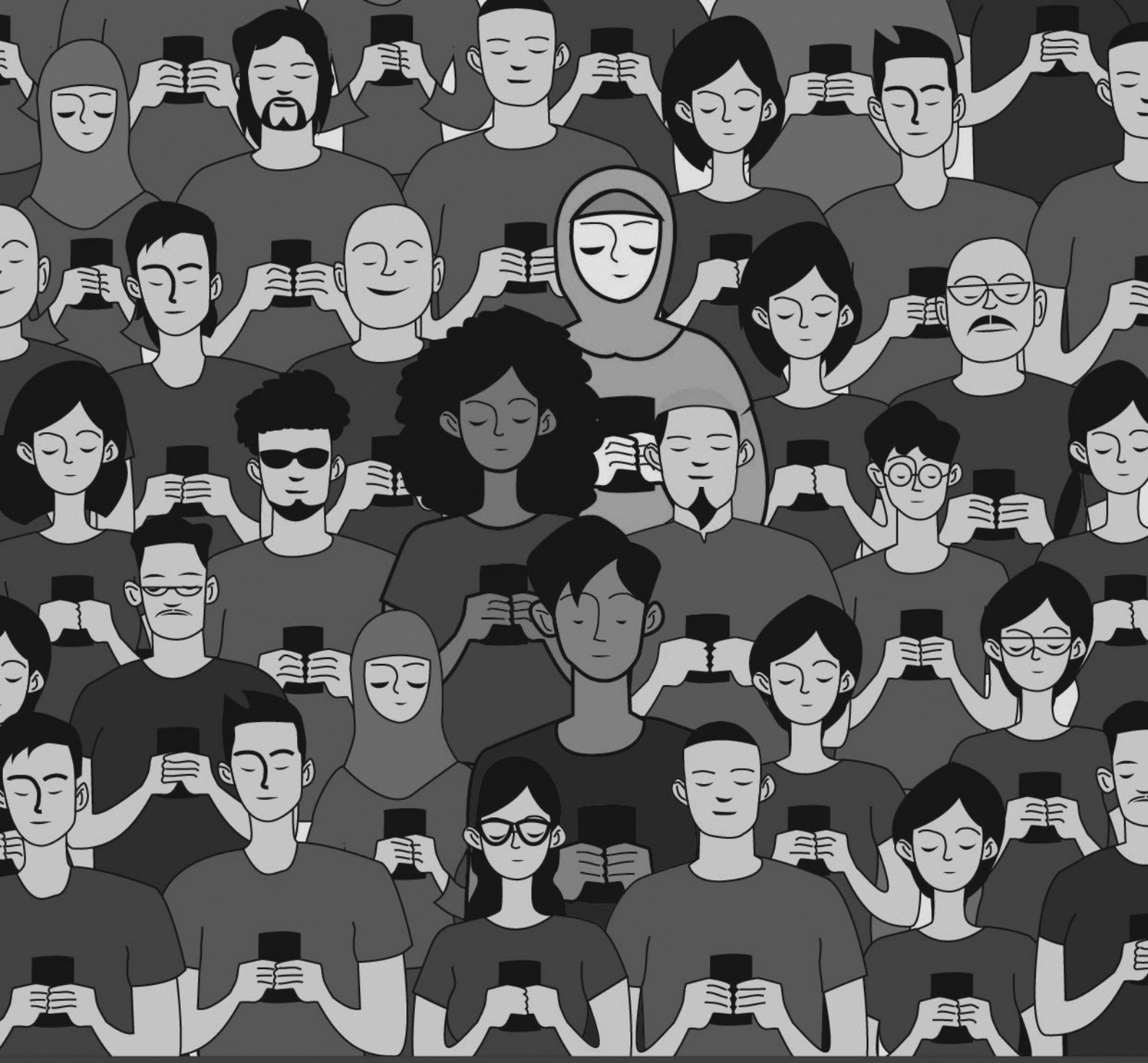


PENTINGNYA PENDEKATAN BERBASIS HAK ASASI MANUSIA DALAM LEGISLASI KEAMANAN SIBER

DDRN
Digital Democracy Resilience Network



PENTINGNYA PENDEKATAN BERBASIS HAK ASASI MANUSIA DALAM LEGISLASI KEAMANAN SIBER

DDRN
Digital Democracy Resilience Network

Pentingnya Pendekatan Berbasis Hak Asasi Manusia dalam Legislasi Keamanan Siber

Tim Penulis DDRN
Hafizh Nabiyyin (Koordinator)
Parasurama Pamungkas
Sekar Arum Jannah

Editor:
Anton Muhajir

Penata Letak:
Daeng Ipul

Koalisi Organisasi Masyarakat Sipil
Jejaring Resiliensi Demokrasi Digital (DDRN)
Oktober 2025

Laporan ini menggunakan lisensi Creative Commons Attribution-NonCommercial 4.0 (CC BY-NC 4.0). Anda bebas untuk untuk mendistribusikan, mencampur ulang, mengadaptasi, dan membuat materi dalam media atau format apa pun hanya untuk tujuan nonkomersial, dan hanya selama atribusi diberikan kepada pencipta. Informasi lebih lanjut di https://creativecommons.org/licenses/by-nc/4.0/

DAFTAR ISI

KATA PENGANTAR 1

Memadukan Keamanan dan Hak Asasi Manusia di Ruang Digital: Sebuah Keharusan Strategis— 1

RINGKASAN EKSEKUTIF 3

PENDAHULUAN 4

METODOLOGI 7

KERANGKA KONSEPTUAL 8

4.1. Keamanan Siber— 8

4.2. Keamanan Tradisional— 9

4.3. Pendekatan Berbasis HAM ***(Human-centric Approach)***— 10

PEMBAHASAN 13

5.1. Urgensi Pembentukan RUU KKS— 13

5.2. Komparasi Pendekatan Keamanan dan Ketahanan Siber di Tingkat Regional dan Internasional— 16

5.3. Catatan Kritis atas Draf Rancangan UU KKS— 22

5.3.1. Reorientasi Tujuan Keamanan Siber dan Pelindungan Individu—— 22

5.3.2. Mendudukkan Kembali Ketahanan Siber dan Pertahanan Siber —— 24

5.3.3. Mengeluarkan Kewenangan TNI dalam Penegakkan Hukum pada Tindak Pidana Nonmiliter —— 26

5.3.4. Harmonisasi Legislasi Keamanan dan Ketahanan Siber dengan Kejahatan Siber—— 27

5.3.5. Mengakomodasi Model Multipemangku Kepentingan —— 29

5.3.6. Harmonisasi Tata Kelola Kecerdasan Artifisial dengan RUU Keamanan dan Ketahanan Siber—— 30

5.4. Pentingnya Pendekatan Berbasis HAM dalam Legislasi Keamanan Siber— 32

KESIMPULAN 39

REKOMENDASI 40

DAFTAR PUSTAKA 42



KATA PENGANTAR

Memadukan Keamanan dan Hak Asasi Manusia di Ruang Digital: Sebuah Keharusan Strategis

Indonesia sedang berada pada titik balik penting dalam membangun kedaulatan digitalnya. Dengan lebih dari 229 juta pengguna internet dan ekonomi digital yang terus melesat, ruang siber telah menjadi tulang punggung kemajuan bangsa. Namun, di balik peluang besar ini, ancaman siber yang kian canggih dan sistematis—dari serangan *ransomware* terhadap infrastruktur vital hingga kebocoran data masif—telah menempatkan keamanan dan ketahanan siber sebagai isu strategis yang tidak bisa ditunda.

Dalam konteks inilah, riset ini hadir. Sebagai pihak yang telah lama terlibat dalam advokasi tata kelola internet dan kebijakan digital, kami dari Koalisi Organisasi Masyarakat Sipil Jejaring Resiliensi Demokrasi Digital (DDRN) melihat bahwa Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) memiliki potensi besar untuk menjadi landmark regulasi. Namun, potensi itu hanya akan terwujud jika pendekatan yang diambil tidak semata-mata bersifat *state-centric*, tetapi juga *human-centric*—menempatkan warga sebagai subjek yang dilindungi, bukan hanya objek yang dikendalikan.

Riset ini menguraikan dengan rinci mengapa pendekatan berbasis HAM justru akan memperkuat efektivitas keamanan siber nasional. Beberapa poin kritis yang diangkat—seperti pentingnya mendefinisikan ulang ketahanan siber (*cyber resilience*) yang lebih luas dari sekadar pertahanan siber (*cyber defense*), perlunya mengharmonisasikan kewenangan lembaga, serta pengaturan yang jelas tentang peran Badan Siber dan Sandi Negara (BSSN)—disajikan dengan argumen teknis dan komparasi global yang relevan. Penguatan kapasitas teknis dan koordinasi BSSN harus diimbangi dengan mekanisme akuntabilitas dan transparansi, agar kepercayaan publik—yang merupakan fondasi dari ketahanan siber—dapat terbangun secara organik.

Riset ini juga menjadi pengingat kolektif bahwa dalam demokrasi, keamanan dan hak asasi manusia bukanlah dua hal yang dipertentangkan, melainkan dua sisi dari koin yang sama. Legislasi yang baik adalah yang mampu menciptakan keseimbangan: melindungi kedaulatan tanpa mengabaikan privasi, mencegah ancaman tanpa membungkam kebebasan berekspresi, dan melibatkan seluruh pemangku kepentingan—mulai dari pemerintah, aparat penegak hukum, sektor swasta, hingga komunitas teknis dan masyarakat sipil.

Kami menyampaikan apresiasi setinggi-tingginya kepada tim penulis DDRN yang telah menyusun riset yang komprehensif dan visioner ini. Semoga kontribusi pemikiran ini dapat diterima sebagai bahan pertimbangan yang konstruktif bagi pemerintah dan DPR dalam menyempurnakan RUU KKS. Mari kita bersama-sama wujudkan ruang digital Indonesia yang tidak hanya aman dan berdaulat, tetapi juga adil, inklusif, dan menghormati martabat setiap warganya.

Bali, Hari Pahlawan, 10 November 2025

Unggul Sagena
Koordinator Koalisi Organisasi Masyarakat Sipil Jejaring Resiliensi Demokrasi Digital (DDRN)

1. RINGKASAN EKSEKUTIF

Peran teknologi dan pertumbuhan internet di Indonesia memiliki peran signifikan dalam dimensi ekonomi, sosial, politik, dan budaya. Menyadari peluang serta tantangannya, maka perlu upaya mendorong pengaturan keamanan siber. Sejalan dengan hal ini, pemerintah menginisiasi Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) yang masuk dalam Program Legislasi Nasional (Prolegnas) Prioritas Tahun 2026. Dengan adanya perancangan regulasi yang komprehensif terkait keamanan siber, Indonesia akan menjadi negara di Asia Tenggara yang memiliki undang-undang (UU) keamanan siber selain Filipina, Singapura, Thailand, Vietnam, dan Malaysia.

Tulisan ini menelaah substansi dan proses perancangan UU tersebut dan mengidentifikasi beberapa catatan kritis mengenai reorientasi peraturan yang didasarkan pada pendekatan hak-hak individu, kejelasan definisi antara ketahanan siber dan pertahanan siber, tumpang tindih kewenangan Tentara Nasional Indonesia (TNI) dalam melakukan penyidikan tindak pidana di ruang siber, harmonisasi legislasi keamanan dan ketahanan siber dengan kejahatan siber, serta urgensi penguatan model tata kelola multipemangku kepentingan. Perspektif ini diharapkan dapat memberikan landasan untuk menganalisis keseimbangan antara kepentingan keamanan nasional dan perlindungan hak-hak sipil di ruang digital sebagaimana yang diatur dalam RUU KKS di Indonesia.

2. PENDAHULUAN

Indonesia merupakan negara dengan tingkat keterhubungan internet tinggi. Pada tahun 2025, Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa angka penetrasi internet mencapai 80,66 persen atau sekitar 229,4 juta pengguna internet dari total populasi Indonesia. Pulau Jawa menjadi kawasan dengan tingkat penetrasi internet tertinggi, diikuti Kalimantan, Sumatera, serta Bali dan Nusa Tenggara.[1] Pemanfaatan internet serta kemajuan teknologi informasi di berbagai aspek memiliki potensi untuk mendorong potensi ekonomi digital, memfasilitasi pertukaran informasi, dan meningkatkan partisipasi publik dalam proses demokrasi. Namun, hal ini juga diiringi oleh kekhawatiran mengenai risiko ancaman di ruang digital.

Di konteks kawasan, Indo-Pasifik termasuk Asia Tenggara di dalamnya, memiliki posisi strategis dan potensi ekonomi digital masif yang menjadikannya sebagai arena persaingan geopolitik. Sebagai contoh, sengketa wilayah di Laut China Selatan yang membuat Tiongkok dan Filipina sebagai *claimant states* terlibat dalam konfrontasi militer.[2] Hal ini memengaruhi arsitektur keamanan di tingkat kawasan dan nasional pada negara-negara di Asia Tenggara yang saat ini ancaman keamanan tidak lagi hanya diartikan secara konvensional, tetapi bergeser ke bentuk-bentuk nonmiliter seperti serangan siber, atau bahkan mengombinasikan keduanya.[3]

Indonesia sendiri menyadari bahaya ancaman siber sebagaimana tercantum dalam beberapa dokumen pertahanan. Menurut UU Nomor 3 Tahun 2002 tentang Pertahanan Negara, pertahanan negara bertujuan untuk menjaga dan melindungi keutuhan dan kedaulatan negara dari ancaman militer dan nonmiliter, termasuk ancaman siber. Ancaman siber bersifat multifaset yang mengombinasikan beragam taktik, teknik, dan aktor dalam mengeksploitasi kerentanan di ruang digital. Serangan ini dapat menyasar infrastruktur kritis, institusi pemerintahan, serta sistem pertahanan dan militer. Dampaknya bersifat multidimensi, mencakup gangguan terhadap objek vital nasional dan kerugian ekonomi yang berpotensi mengancam stabilitas dan keamanan nasional. Misalnya di tahun 2024, serangan siber dalam bentuk *ransomware* telah melumpuhkan Pusat Data Nasional Sementara (PDNS) yang berdampak pada gangguan

1 *Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), Survei Internet APJII 2025,* online.

2 *Nuurrianti Jalli dan Angel Martinez, "Artificial Intelligence is Intensifying South China Sea Disputes in the Philippines," Fulcrum, 25 Februari 2025,* online.

3 *Kementerian Pertahanan Republik Indonesia, "Kabainstrahan Kemhan Buka FGD tentang Rumusan Ancaman Peperangan Hibrida," 16 Agustus 2023,* online.

pelayanan di 282 instansi di tingkat kementerian lembaga serta pemerintah provinsi, kabupaten, dan kota.

Namun, ancaman siber yang terus berkembang membuat operasi ancaman siber mengalami pergeseran, tidak hanya menyasar kepada infrastruktur keamanan nasional atau sektor kritis, tetapi juga berkaitan dengan hak atas privasi dan keamanan individu di ruang digital. Sejumlah insiden siber di Indonesia juga terjadi dalam bentuk kebocoran data sensitif. PT Kereta Api Indonesia (PT KAI) misalnya, menjadi salah satu sasaran peretasan yang membuat bocornya puluhan ribu data pribadi pengguna dan karyawannya.[4] Selain itu, data milik Badan Intelijen Strategis (BAIS) TNI dan Pusat Indonesia *Automatic Fingerprint Identification System* Kepolisian Negara Republik Indonesia (INAFIS Polri) diduga mengalami kebocoran yang memuat data pribadi mengenai anggota instansi.[5]

Indonesia sudah memiliki beberapa regulasi yang mengatur ruang digital dan keamanan data seperti UU Informasi dan Transaksi Elektronik (UU ITE) beserta aturan-aturan turunannya dan UU Pelindungan Data Pribadi (UU PDP). Selain itu, terdapat dua peraturan keamanan siber yang tercantum dalam Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Perpres IIV) dan Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Nasional Keamanan Siber dan Manajemen Krisis (Perpres Stranas KSMK) yang mencakup sektor pemerintahan, energi, transportasi, finansial, kesehatan, teknologi informasi, komunikasi, pangan, dan pertahanan.[6] Pemerintah Indonesia juga membentuk Badan Siber dan Sandi Negara (BSSN) melalui Peraturan Presiden Nomor 133 Tahun 2017. Peraturan tersebut memandatkan BSSN sebagai badan yang bertanggung jawab dalam keamanan siber. Namun, Indonesia belum memiliki payung hukum dalam bentuk UU yang dapat mengoordinasikan beberapa peraturan sektoral berkaitan dengan keamanan siber yang telah ada. Berangkat dari kebutuhan mendesak tersebut, pada tahun 2019, pemerintah menginisiasi penyusunan RUU KKS. Meski pembahasannya sempat terhenti, RUU KKS ditetapkan masuk ke dalam salah satu Prolegnas Prioritas tahun 2026.

Regulasi di ruang siber kerap kali mengaburkan batas antara kepentingan keamanan nasional dan perlindungan hak asasi manusia (HAM). Upaya untuk menyeimbangkan keduanya menghadirkan peluang sekaligus tantangan. Di satu sisi, langkah-langkah keamanan siber yang

4 *Dani Aswara, "Kaleidoskop 2024: 6 Serangan Siber Besar di Indonesia," Tempo, 31 Desember 2024,* online.

5 *Willy Medi Christian Nababan, "Data Bais TNI-Inafis Polri Bobol, Dokumen Rahasia, Nama, Foto, NRP, dan Kesatuan Pun Terkuak," Kompas, 26 Juni 2024,* online.

6 *Sekretaris Kabinet, "President Jokowi Issues Presidential Regulation on Protection for Vital Information Infrastructure," 15 Juni 2022,* online.

komprehensif sangat dibutuhkan guna merespons ancaman yang terus berkembang. Namun, di sisi lain, pendekatan yang terlalu represif berisiko menimbulkan pelanggaran terhadap hak-hak individu, seperti hak atas privasi dan kebebasan berekspresi.[7] Hal ini semakin relevan jika melihat berbagai insiden serangan siber di Indonesia yang tidak hanya menyasar lembaga pemerintah dan sektor pertahanan, tetapi juga mengeksploitasi kelemahan data pribadi masyarakat sebagai pengguna teknologi dalam kehidupan sehari-hari.

Merespons perkembangan legislasi keamanan siber nasional, Digital Democracy Resilience Network (DDRN) merumuskan beberapa catatan kritis dan menggarisbawahi pentingnya pendekatan berbasis HAM dalam kerangka hukum tersebut. Fokus keamanan siber yang selama ini bertumpu pada perlindungan negara mendorong pendiri dan direktur Citizen Lab, Professor Ronald Deibert untuk mengeksplorasi kemungkinan pendekatan yang lebih berorientasi pada manusia dalam konsep keamanan siber. Definisi keamanan siber umumnya masih terbatas pada perlindungan institusi negara seperti militer, intelijen, dan aparat penegak hukum. Menanggapi kecenderungan yang bersifat *state-centric* tersebut, Diebert menawarkan perspektif alternatif melalui pendekatan *human-centric*, yang menempatkan individu, tanpa memandang asal negara atau kewarganegaraan, sebagai pusat perhatian dalam strategi keamanan siber. Ia menekankan bahwa pendekatan ini seharusnya menjadi landasan utama karena mencerminkan prinsip-prinsip modern dalam penegakan HAM. Dalam konteks digital, hak-hak tersebut mencakup kebebasan memperoleh informasi, kebebasan berpendapat dan berpikir, serta hak untuk berserikat.

7 *Robb Shawe, "Cybersecurity and Human RIghts: Navigating the Balance between Security and Freedom in the Digital Era," Journal of Information Technology and Integrity, 2025.*

3. METODOLOGI

Penelitian ini ditulis menggunakan pendekatan kualitatif untuk menguraikan lanskap ruang siber di Indonesia serta memahami substansi dari RUU KKS yang dianalisis melalui kerangka HAM untuk mengetahui dampak potensial terhadap kebebasan berpendapat dan partisipasi masyarakat sipil dalam proses demokrasi. Adapun metode pengumpulan data dalam penulisan penelitian ini mencakup studi pustaka, analisis dokumen, dan diskusi kelompok terarah.

Studi pustaka dilakukan untuk menghimpun data sekunder melalui bacaan serta informasi yang tersedia secara publik. Analisis dokumen yang dimaksud ialah mengulas secara sistematis dokumen-dokumen yang relevan meliputi naskah akademik RUU KKS sebagai rujukan utama serta dokumen pendukung lainnya. Diskusi kelompok terarah mengundang pemangku kepentingan kunci seperti pemerintah, ahli kebijakan, dan organisasi masyarakat sipil. Diskusi ini bertujuan menggali temuan-temuan mengenai ancaman siber, menjaring pengalaman dan pandangan para pemangku kepentingan, dan mengidentifikasi masalah dalam perancangan RUU KKS secara prosedural dan substansial. Penelitian ini diharapkan dapat memberikan rekomendasi yang dapat ditindaklanjuti untuk memastikan strategi keamanan dan ketahanan siber di tingkat nasional yang mempertimbangkan nilai-nilai dan prinsip HAM.

4. KERANGKA KONSEPTUAL

4.1. Keamanan Siber

Keamanan siber tidak memiliki definisi tunggal karena laskapnya yang terus berubah dan berkembang. Sektor swasta dan publik sendiri memiliki beragam pendekatan sesuai kebutuhan serta bagaimana teknologi digital itu sendiri digunakan. Misalnya, International Business Machines (IBM) mendefinisikan keamanan siber sebagai praktik untuk melindungi individu, sistem, dan data dari serangan siber.[8] Di Indonesia, Peraturan Presiden No. 47 Tahun 2023 mengenai Strategi Keamanan Siber Nasional dan Manajemen Krisis memaknai keamanan siber sebagai upaya adaptif dan inovatif untuk melindungi seluruh lapisan ruang siber, termasuk aset informasi yang di dalamnya terdapat ancaman dan serangan bersifat teknis maupun sosial. Sedangkan, aliansi multipihak di level internasional, yakni International Telecommunication Union (ITU), mendefinisikan keamanan siber sebagai sekumpulan alat, kebijakan, konsep keamanan, pedoman, pelindungan keamanan, pendekatan manajemen risiko, tindakan, praktik baik yang digunakan untuk melindungi ruang lingkup siber dan aset pengguna maupun organisasi.[9]

Li and Liu (2021) membagi tipe keamanan siber menjadi lima, yakni keamanan jaringan (*network security*), keamanan aplikasi (*application security*), keamanan informasi (*information security*), keamanan operasional (*operational security*), dan keamanan komputasi awan (*cloud security*).[10] Keamanan jaringan bertujuan untuk melindungi jaringan komputer terhadap aktivitas seperti *malware* dan peretasan. Keamanan aplikasi dilakukan dengan menggunakan perangkat keras dan lunak (seperti program antivirus dan enkripsi) untuk melindungi sistem dari ancaman eksternal yang dapat mengganggu pengembangan suatu aplikasi. Keamanan informasi berkaitan dengan perlindungan data fisik dan digital dari akses yang tidak diizinkan (*unauthorized access*) yang dapat mengubah, menyalahgunakan, atau menghapus data tersebut. Keamanan operasional mencakup proses atau keputusan yang dibuat untuk melindungi data, seperti ketika seorang pengguna memberikan izin untuk bagaimana informasinya disimpan dan dibagikan.

8 *Alexandra Jonker, Matthew Kosinski, and Gregg Lindemulder, What is cybersecurity, n/d,* online.

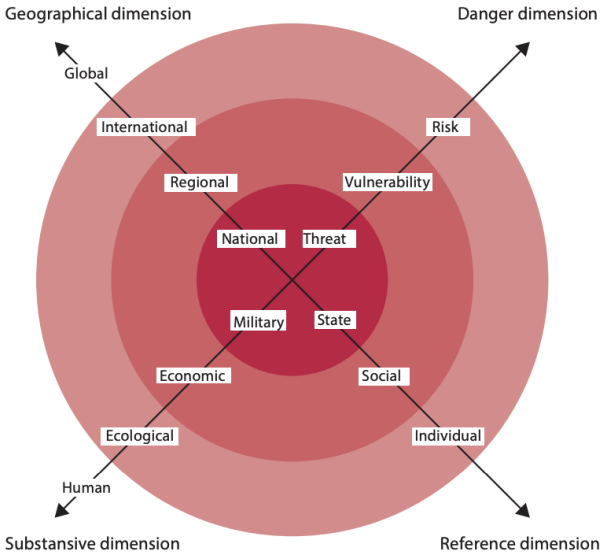
9 *Internet Telecommunication Union (ITU), Definition of cybersecurity, n/d,* online.

10 *Yuchong Li dan Qinghui Liu, "A Comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, 2021.*

4.2. Keamanan Tradisional

Menurut Asmoro et al. (2022), ancaman dapat diklasifikasikan menjadi ancaman faktual dan ancaman potensial. Ancaman faktual merupakan ancaman nyata yang terjadi saat ini, sedangkan ancaman potensial adalah ancaman yang belum terwujud, tetapi mungkin berkembang menjadi ancaman faktual jika tidak ada upaya antisipasi melalui langkah-langkah strategis.[11] Lebih lanjut lagi, ancaman dapat diklasifikasikan berdasarkan aktor, sumber, dan jenis ancaman. Hal ini mencakup, misalnya, ancaman dari luar maupun domestik dalam bentuk ancaman militer dan nonmiliter yang dilancarkan oleh aktor baik negara maupun non-negara.[12]

Gambar 1. The extension of concept of security



Sumber: Ballin, Dijstelbloem, and Goede (2022)

Ballin et al. (2020) menjelaskan konsep ancaman yang mencakup empat dimensi, yakni *geographical dimension, danger dimension, substantive dimension,* dan *reference dimension*.[13] Diagram tersebut menunjukkan bahwa definisi ancaman yang semula bersifat negara-sentris dan

11 *Novky Asmoro, Marsetio, Susanto Zuhdi, dan Resmanto Widodo Putro, "Management of National Security in Analysis and Threat Assessment of Indonesian Sovereignty," Jurnal Penelitian Pendidikan Indonesia (JPPI) Vol. 8 No. 4, 2022,* https://doi.org/10.29210/020221705

12 *Mykola Mykolaichuk, Nina Petrukha, Liudmyla Akimova, Nataliia Pozniakovska, Bohdan Hudenko, dan Oleksandr Akimov, "Conceptual principles of analysis and forecasting threats to national security in modern conditions," Sapienza: International Journal of Interdisciplinary Studies, Vol. 6 No. 2,* https://doi.org/10.51798/sijis.v6i2.985

13 *Ernst Hirsch Ballin, Huub Dijstelbloem, and Peter de Goede, "Chapter 2: The Extension of the Concept of Security," Shifts in the Security Environment, 2020,* https://doi.org/10.1007/978-3-030-37606-2_1

didominasi oleh perspektif militer kini telah bergeser kepada isu-isu yang berkaitan dengan HAM. Dalam dimensi geografis, keamanan nasional memiliki keterkaitan dengan konteks regional, internasional, maupun global. Hal ini juga didukung argumen Terry Terriff yang berpendapat bahwa ancaman keamanan saat ini tidak memiliki suatu wilayah geografis tertentu.[14]

Saat ini, karakteristik ancaman bergeser dari bentuk-bentuk tradisional ke ancaman nontradisional, salah satunya ancaman siber. Ancaman melalui operasi seperti pencurian data, serangan ransomware, penyerangan terhadap infrastruktur informasi kritis, serangan siber, serta influence operations. memiliki dampak signifikan bagi keamanan individu dan nasional secara keseluruhan. Kerentanan ini semakin kompleks seiring dengan kemajuan teknologi, ketergantungan antarnegara, serta keberagaman aktor ancaman yang memunculkan tantangan serius dalam pengatribusian sumber ancaman.[15] Kondisi tersebut mendorong negara-negara mengalokasikan sumber dayanya untuk meningkatkan keamanan dan menjaga kedaulatan di ruang siber.

4.3. Pendekatan Berbasis HAM *(Human-centric Approach)*

Diskusi keamanan siber dan HAM dalam perkembanganya datang bersamaan terkait masalah hak sipil dan politik serta ekonomi dan budaya. Bentuk konvergensi ini dapat dilihat di bidang-bidang seperti kebebasan internet dan gerakan *net neutrality* mengenai arus bebas informasi yang merupakan bagian dan paket pendekatan multipemangku kepentingan untuk tata kelola internet.[16] Pada titik itu pula pertemuan antara HAM dan keamanan siber secara operasional terjadi dalam pelaksanaan Panduan Perserikatan Bangsa-Bangsa (PBB) untuk Bisnis dan HAM (Panduan BHAM). Banyak perusahaan menerapkan prinsip-prinsip dalam HAM untuk menanamkan praktik terbaik HAM dalam pengambilan keputusan mereka, bersama dengan kerangka keamanan siber, untuk membantu memandu investasi keamanan siber perusahaannya.[17]

Pada 2014 Freedom Online Coalition (FOC) merespon perkembangan diskusi keamanan siber ini dengan menyepakati Deklarasi Tallinn tentang pendekatan HAM dalam pembentukan kebijakan keamanan siber (*human*

14 *Terry Terriff, Stuart Croft, Lucy James, dan Patrick M. Morgan, Security Studies Today, 1999.*

15 *Ballin, et al. (2020)*

16 *Scott J. Shackelford, Human Rights and Cybersecurity Due Diligence: A Comparative Study, University of Michigan Journal of Law Reform, Vol. 50, 2017, hlm. 882.*

17 *Ilse Griek, Forum PBB tentang Hak Asasi Manusia: Menilai Kerangka Ruggie,* http://www.sustainalytics.com/assessing-ruggie-framework

rights based approach on cybersecurity policy making).[18] Keamanan siber dalam hal ini telah melengkapi kerangka kerja HAM dan hukum humaniter internasional. FOC menarasikan bahwa "Hukum HAM internasional dan kemanusiaan internasional hukum berlaku daring dan juga luring. Keamanan siber harus melindungi inovasi teknologi dan pelaksanaan HAM."[19] Marry Robinson menilai bahwa pendekatan ini menambah nilai karena kerangka kerja normatif ini menegaskan tanggung jawab pemerintah terhadap HAM. Konsep pendekatan berbasis hak sebagian besar telah dipromosikan PBB dengan menetapkan seperangkat prinsip dasar HAM untuk inisiasi pembangunan.

Kelompok Ahli Pemerintah untuk Perkembangan di Bidang Informasi dan Telekomunikasi dalam UN General Assembly (68/98) mengungkapkan hal serupa. Bahwa upaya untuk mengatasi keamanan teknologi informasi dan komunikasi harus berjalan seiring dengan penghormatan terhadap HAM dan kebebasan mendasar yang ditetapkan dalam Deklarasi Universal Hak Asasi Manusia dan instrumen internasional lainnya. Pada 21 Desember 2009 PBB menetapkan Resolusi Nomor 64/211 tentang Penciptaan Budaya Global keamanan siber dan inventarisasi upaya nasional untuk melindungi infrastruktur informasi kritis (*critical information infrastructures).* Resolusi ini memberikan tekanan pada negara-negara untuk:

1. Menggunakan instrumen penilaian yang tepat bagi kebutuhan nasional mereka untuk memastikan perlindungan infrastruktur informasi kritis untuk memperkuat keamanan siber negara tersebut dan secara umum akan berkontribusi pada peningkatan budaya global keamanan siber.
2. Mendorong negara-negara dan organisasi-organisasi regional internasional yang relevan untuk mengembangkan berbagai strategi guna memastikan keamanan siber dan perlindungan infrastruktur informasi kritis.

Pada 5 Desember 2018 PBB menegaskan kepada negara-negara untuk menghormati Resolusi Dewan HAM 20/8 tanggal 5 Juli 2016 dan resolusi 26/13 tanggal 26 Juni 2014 tentang promosi, perlindungan, dan penikmatan HAM di internet, termasuk pula sejumlah Resolusi Majelis Umum tentang hak privasi di era digital. Tata kelola ruang siber yang baik harus membentuk pendekatan berbasis HAM untuk (1) akuntabilitas yang lebih tinggi, (2) transparansi yang lebih besar, dan (3) partisipasi yang lebih luas dari para pemangku kepentingan melalui penggunaan

18 *Lihat Modul 3 bagian D*

19 *Deborah Brown, et al. Briefing Document : Cybersecurity Policy and Human Rights. Association for Porgressive Communications.* https://www.apc.org/sites/default/files/brief8.pdf

perangkat siber, seperti internet dan perangkat seluler.[20] Oleh karena itu, perlindungan terhadap individu dapat beriringan dengan pengembangan keamanan siber berbasis HAM dan demokrasi. Norma dan standar HAM universal dapat menjadi pedoman dan tolok ukur untuk menetapkan rezim pengaturan di ruang siber. Keamanan siber bukan hanya tentang keamanan aset dan informasi, tetapi juga membahayakan keselamatan individu, baik karena perbuatan jahat yang telah mengganggu keamanan individu secara daring maupun oleh kebijakan peraturan perundang-undangan keamanan siber yang telah menekan HAM dan kebebasan mendasar.

20 *Anja Mihr, Good Cyber Governance The Human Rights and Multi Stakeholder Approach, Goergetown Journal of Interational Affairs, hlm. 24*

5. PEMBAHASAN

5.1. Urgensi Pembentukan RUU KKS

Tingginya penetrasi internet yang diiringi dengan digitalisasi di berbagai sektor menjadi pendorong utama bagi pertumbuhan ekonomi digital di Indonesia. Misalnya di tahun 2021, ekonomi digital Indonesia menyumbang 42% dari keseluruhan ekonomi digital di level Asia Tenggara.[21] Pemanfaatan teknologi dan internet juga mendorong proses komunikasi secara langsung serta meningkatkan produktivitas pada sektor layanan publik. Beragam aktivitas, mulai dari ekonomi, sosial, dan administrasi pemerintahan yang semakin bergantung pada sektor digital menekankan pentingnya perlindungan terhadap bukan hanya infrastruktur vital, tetapi juga informasi sensitif individu yang terbentuk dan saling berinteraksi di dalamnya.[22]

Jika dilihat dari konteks geopolitik, Indonesia memiliki posisi strategis menjadi perlintasan rute perdagangan maritim yang menghubungkan ekonomi Asia Timur, Asia Selatan, dan Pasifik. Hal ini membuat kawasan Indo-Pasifik menjadi arena kompetisi bagi negara kekuatan besar, seperti Amerika Serikat, Tiongkok, dan Rusia untuk menyebarkan pengaruhnya di kawasan. Persaingan tersebut dilakukan melalui operasi di area abu-abu, melalui taktik hibrida, yang mengaburkan batasan antara konflik dan perdamaian.[23] Jika digabungkan, potensi ekonomi digital, meningkatnya penetrasi internet dan aktivitas di ruang digital, serta ketidakpastian kondisi geopolitik saat ini tidak hanya menciptakan peluang, tetapi juga meningkatkan keterpaparan ruang siber terhadap ancaman siber.

Beberapa bentuk ancaman siber ialah *phising*, pencurian identitas, peretasan sistem dan website, serta kejahatan finansial. Sedangkan, metode yang umumnya digunakan adalah *distributed denial of service* (DDoS), *man-in-the-middle*, *malware*, dan *phishing*.[24] Selain itu, kemunculan teknologi seperti kecerdasan artifisial atau *artificial intelligence* (AI) menjadi babak baru dalam lanskap risiko keamanan siber yang membuat taktik, teknik, dan prosedur serangan siber terus berkembang menjadi lebih canggih. Jika dilihat dari sumbernya, terdapat pengaburan aktor-aktor yang dapat

21 *Militcyano Samuel Sapulette dan Pyan A. Muchtar, "Redefining Indonesia's Digital Economy," ERIA Policy Brief No. 2022-06, 2023,* online.

22 *Yuchong Li dan Qinghui Liu, 2021.*

23 *Fitriani, Pieter Pandie, dan Sekar Arum Jannah, "Tackling Disinformation, Foreign Information Manipulation and Interference in Southeast Asia and Broader Indo-Pacific" Research Report Safer Internet Lab, 2025,* online.

24 *Yuchong Li dan Qinghui Liu, 2021.*

dikategorikan menjadi aktor negara, aktor non-negara, atau individu sebagai *proxy* yang disponsori negara.[25] Aktor-aktor kejahatan siber ini didorong oleh motivasi beragam, misalnya ideologi, finansial, atau untuk mengancam kedaulatan negara.[26] Hilangnya batasan antara aktor negara dan aktor non-negara dalam operasi siber memperluas bentuk dan jangkauan serangan siber, sekaligus memunculkan tantangan baru dalam hal akuntabilitas aktor yang melakukan operasi serangan siber.

Menurut Microsoft Digital Defense tahun 2024, setidaknya terdapat 1,500 *threat groups* yang terdiri lebih dari 600 kelompok aktor negara, 300 kelompok kejahatan siber, dan 200 kelompok *influence operations*.[27] Operasi siber ini didominasi Rusia, Tiongkok, Korea Utara, dan Iran, sedangkan beberapa negara di Asia Tenggara yang menjadi target ialah Malaysia, Filipina, Thailand, Indonesia, Vietnam, dan Kamboja. Meski Indonesia bukan merupakan target utama dari operasi siber negara-negara kekuatan besar, hal ini tidak lantas membuat kerentanan ruang siber Indonesia menjadi aman sepenuhnya.

Sepanjang Januari hingga Juli 2025, Badan Siber dan Sandi Negara (BSSN) mencatat 3,64 juta serangan siber atau anomali trafik yang terjadi di Indonesia.[28] Angka ini setara dengan jumlah keseluruhan insiden siber di Indonesia selama lima tahun terakhir. Di tahun 2024, serangan *ransomware* terhadap PDNS yang membuat lumpuhnya *server* beberapa lembaga atau kementerian sehingga pelayanan publik menjadi terganggu akibat serangan *ransomware*.[29] Instansi pertahanan dan militer juga turut menjadi target serangan siber. Beriringan dengan serangan terhadap PDNS, data milik Badan Intelijen Strategis Tentara Nasional Indonesia (BAIS TNI) dan Pusat Indonesia *Automatic Fingerprint Identification System* Kepolisian Negara Republik Indonesia (INAFIS Polri) diduga mengalami kebocoran yang memuat data pribadi mengenai anggota instansi, termasuk nama, foto wajah, nomor registrasi pokok (NRP), satuan tugas, dan sidik jari anggota instansi yang dijual di forum situs gelap oleh peretas.

Tidak hanya pada sektor publik, terintegrasinya internet dalam kehidupan sehari-hari juga meningkatkan kerentanan individu sebagai

25 *Michael N. Schmitt and Liis Vihul, " Proxy Wars in Cyberspace," Fletcher Security Review, 2014,* online.

26 *R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, P. Laplante, Dimensions of cyber-attacks: cultural, social, economic, and political. IEEE Technol. Soc. Mag., 30 (2011), pp. 28-38*

27 *Microsoft Digital Defense Report, 2024,* online.

28 *Yosea Iskandar, "The architecture of trust in Indonesia's digital dawn," The Jakarta Post, 24 September 2025,* online.

29 *Antara, "Kronologi Serangan Siber yang Lumpuhkan PDN hingga Tuntutan 8 Juta Dolar," Tempo, 25 Juni 2024,* online.

pengguna terhadap serangan siber. Pada saat terjadinya pandemi, Indonesia mengalami serangkaian insiden peretasan menargetkan sektor *e-commerce,* lembaga negara, dan perbankan. Di tahun 2020, Tokopedia dilaporkan mengalami kebocoran data 91 juta akun yang mencakup informasi mengenai nama akun, e-mail, nama lengkap, tanggal lahir, jenis kelamin, nomor ponsel, dan kata sandi.[30] Aplikasi Electronic Health Alert Card (eHAC) milik Kementerian Kesehatan juga turut mengalami peretasan data tes COVID-19 dan informasi kesehatan milik 1,3 juta pengguna, termasuk alamat, kartu identitas pengguna, tipe dan waktu tes COVID-19, hasil tes dan tanggal dikeluarkan, serta nomor antrean.[31] PT Bank Syariah Indonesia (Persero) Tbk atau BSI juga menjadi sasaran serangan *ransomware* oleh LockBit yang berimbas pada 15 juta nasabah yang dapat berpotensi dimanfaatkan untuk kejahatan seperti *scam* dan *phising.*[32] Di tahun 2024, PT Kereta Api Indonesia (PT KAI) menjadi target pembobolan data oleh Stormous yang memuat informasi sensitif mengenai detail karyawan dan pelanggannya.[33]

Meningkatnya serangan siber ke Indonesia memantik sejumlah evaluasi terhadap standar teknis hingga tata kelola keamanan siber secara menyeluruh. Kasus kebocoran data yang dialami sektor publik maupun swasta dalam lima tahun terakhir bukan hanya akibat dari tata kelola perlindungan data pribadi yang buruk, tetapi juga karena tiadanya tata kelola keamanan siber yang memadai. Hal ini berdampak pada turunnya kepercayaan masyarakat terhadap pemerintah sebagai pengelola pusat data, kerugian ekonomi, mengganggu atau merusak kinerja aset siber nasional, dan bahkan memungkinkan jika termanifestasi menjadi perang atau konfrontasi secara fisik di dunia nyata.[34] Hal ini mendesak kebutuhan melakukan pembenahan tata kelola keamanan siber untuk mengurai permasalahan yang bersifat kelembagaan maupun teknis di Indonesia. Pemerintah Indonesia menyadari urgensi ancaman siber serta keamanan dan ketahanan siber. Hal ini mendorong diinisiasinya RUU KKS yang menjadi landasan untuk penyelenggaraan keamanan siber yang meliputi pencegahan, penanggulangan, dan pemulihan dari insiden dan serangan siber.[35] Jika disahkan, Indonesia akan menjadi salah satu negara di Asia Tenggara yang memiliki undang-undang keamanan siber selain Filipina

30 *CNN Indonesia, "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dljual," 3 Mei 2020,* online.

31 *BBC Indonesia, "Data eHAC milik 1,3 juta penggunanya dilaporkan bocor, 'keamanan data tidak prioritas'", 31 Agustus 2021,* online.

32 *CNN Indonesia, "Daftar Dugaan Kebocoran Data 2023, Termasuk Data Pemilih dan Bank," CNN Indonesia, 31 Desember 2023,* online.

33 *M. Khorty Alfarizi, "Pengamat Siber Temukan Data Kredensial PT KAI yang Dibobol Hacker Stormous," Tempo, 18 Januari 2024,* online.

34 *Yuchong Li dan Qinghui Liu, 2021.*

35 https://berkas.dpr.go.id/akd/dokumen/RJ1-20190617-025848-5506.pdf

(Cybercrime Prevention Act 2012), Singapura (Cybersecurity Act 2018), Thailand (Cybersecurity Act 2019), Vietnam (Law on Cybersecurity 2018), dan Malaysia (Cyber Security Act 2024).

Fokus utama RUU KKS adalah untuk melindungi infrastruktur informasi kritis mencakup beberapa sektor, seperti bank, kesehatan, transportasi, energi, dan pelayanan publik. Sehingga RUU ini diharapkan menjadi fondasi bagi upaya strategis untuk memperkuat sistem ketahanan siber nasional sehingga dapat mendorong potensi ekonomi digital dan inovasi teknologi. Dalam pelaksanaannya, BSSN akan ditunjuk sebagai badan pelaksana undang-undang yang berkoordinasi dengan kementerian atau lembaga terkait seperti Kementerian Komunikasi dan Digital (Komdigi), kepolisian, kejaksaan, dan TNI.

5.2. Komparasi Pendekatan Keamanan dan Ketahanan Siber di Tingkat Regional dan Internasional

Beberapa negara selain Indonesia telah memiliki perangkat regulasi mengenai keamanan dan ketahanan siber dengan pendekatan beragam. Uni Eropa memiliki NIS2 Directive, Cybersecurity Act, dan Cyber Resilience Act dengan pendekatan berbasis risiko (*risk-based approach*) yang berfokus pada perlindungan terhadap keamanan dan privasi pengguna. Di Amerika Serikat, pengaturan ruang siber sifatnya terfragmentasi berdasarkan sektor. Salah satu kebijakannya adalah Cybersecurity Information Sharing Act (CISA) yang mengatur mengenai pertukaran informasi berkaitan dengan ancaman siber antara sektor swasta dan pemerintah. Di Tiongkok, Cybersecurity Law (CSL) menjadi fondasi dari kerangka keamanan siber. Cybersecurity Law juga ditopang oleh dua regulasi berkaitan dengan keamanan data yakni Data Security Law (DSL) dan Personal Information Protection Law (PIPL).[36]

36 *PwC, A Comparison of cybersecurity regulations: China,* https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/china.html

Tabel 1. Regulasi Siber Kawasan atau Negara Lain

Kawasan atau Negara	Pendekatan	Regulasi	Tujuan dan Cakupan	Regulator
Uni Eropa	Pendekatan berbasis resiko dan hak atas privasi	NIS2 Directive (2022)	Fokus pada perlindungan *very critical sectors* (energi, transportasi, kesehatan, infrastruktur digital, dan lain-lain) dan diperluas ke *critical sectors* (penyedia jaringan dan layanan komunikasi elektronik, layanan pusat data, layanan pos dan kurir, dan lain-lain).	Otoritas di level nasional yang dibentuk oleh negara anggota.
		Cybersecurity Act (2019)	Memperkenalkan kerangka sertifikasi bagi produsen, pengembang, dan penyedia produk layanan berkaitan dengan produk, layanan, dan proses TIK.	European Union Agency for Network and Information Security (ENISA)
		Cyber Resilience Act (2024)	Memberikan standar keamanan siber yang harus dipenuhi oleh produk dengan elemen digital.	
Amerika Serikat (AS)	Terfragmentasi dan pendekatan berdasarkan sektor	Cybersecurity Information Sharing Act atau CISA (2015)	Mendorong *information sharing* mengenai ancaman siber antara sektor privat dan pemerintah.	Cybersecurity and Infrastructure Security Agency (CISA)

Kawasan atau Negara	Pendekatan	Regulasi	Tujuan dan Cakupan	Regulator
Tiongkok	Kedaulatan atau kontrol negara	Cybersecurity Law atau CSL (2017), Data Security Law (DSL), dan Personal Information Protection Law (PIPL)	CSL merupakan dasar dari keseluruhan kerangka keamanan siber. DSL mengatur mengenai keamanan data yang diproses, sementara PIPL untuk pemrosesan data personal. DSL dan PIPL memiliki *extra-territorial reach* untuk data-data dari luar Tiongkok yang dianggap dapat mengancam kedaulatan siber.	Cyberspace Administration of China (CAC)

Sumber: diolah kembali oleh penulis

Di lingkup Asia Tenggara, beberapa negara yang memiliki regulasi siber adalah Singapura, Filipina, Thailand, Vietnam, dan Malaysia. Di Singapura, Cybersecurity Act (CSA) memiliki pendekatan *whole-of-nation* yang memfasilitasi kerja sama antara otoritas pemerintah dan sektor privat untuk mencegah, menangani, dan merespons ancaman terhadap infrastruktur informasi kritis.[37] Cybercrime Prevention Act menjadi dasar hukum bagi negara Filipina untuk penanganan *computer-related offences* dan *content-related offences*.[38] Thailand Cybersecurity Act dan Malaysia Cybersecurity Act memiliki pendekatan manajemen risiko (*risk-management approach*) yang berfokus untuk melindungi infrastruktur informasi kritis. Sedangkan Vietnam Law on Cybersecurity menerapkan pendekatan *whole-of-government*. Meski tidak memiliki regulator utama, implementasi kebijakan keamanan siber di Vietnam melibatkan koordinasi lintas kementerian dan pemangku kepentingan terkait, seperti Kementerian Pertahanan, Kementerian Keamanan Publik, Kementerian Informasi dan Komunikasi, dan Kementerian Luar Negeri yang memiliki peran, keahlian, dan tanggung jawabnya masing-masing.[39]

37 *Ella Gorian, "Singapore's Cybersecurity Act 2018: A New Generation for Critical Information Infrastructure Protection," 2020, 10.1007/978-3-030-15577-3_1*

38 *Rules and Regulations Implementing Republic Act No. 10175m Otherwise Known as the Cybercrime Prevention Act of 2012,* https://ecommerce.dti.gov.ph/wp-content/uploads/2020/11/IRR-of-RA-10175-Cybercrime-Prevention-Act-of-2012.pdf

39 *Bich Tran, "Vietnam Strengthens Cyber Capabilities for Political Stability, National Defense, and Socio-economic Development," 2024,* https://www.iseas.edu.sg/wp-content/uploads/2024/09/ISEAS_Perspective_2024_78.pdf

Tabel 2. Regulasi Siber di Negara Asia Tenggara

Kawasan atau Negara	Pendekatan	Regulasi	Tujuan dan Cakupan	Regulator
Singapura	Pendekatan *whole-of-nation*	Cybersecurity Act (2018)	Fokus pada perlindungan infrastruktur kritis.	Cyber Security Agency (CSA)
Filipina	Pendekatan penegakan hukum	Cybercrime Prevention Act 2012 atau Republic Act No. 10175	Fokus pada perlindungan sistem komputer dan data dari penyalahgunaan dan akses ilegal. Juga sebagai kerangka hukum untuk menangani tindak kejahatan digital seperti peretasan, pencurian identitas, dan pornografi anak, sekaligus memfasilitasi *mutual assistance* dan ekstradisi dengan negara lain untuk hal-hal berkaitan dengan kejahatan siber.	Department of Justice (DOJ)
Thailand	Pendekatan manajemen resiko (*risk-management approach*)	Cybersecurity Act 2019	Fokus pada pencegahan, penanganan, dan mitigasi resiko dari ancaman siber terutama terhadap infrastruktur informasi kritis.	National Cyber Security Committee (NCSC)
Vietnam	Pendekatan *whole-of-government*	Law on Cybersecurity 2018	Fokus pada stabilitas politik, keamanan nasional, dan pembangunan ekonomi-sosial.	Koordinasi antar kementerian dan pemangku kepentingan
Malaysia	Pendekatan manajemen resiko (*risk-management approach*) dan kebijakan *top-down*	Cybersecurity Act 2024	Bertujuan untuk melindungi infrastruktur informasi kritis melalui: (1) asesmen resiko; (2) persyaratan perizinan oleh penyedia layanan keamanan siber; (3) penerapan ekstrateritorial.	National Cyber Security Committee (NACSA)

Sumber: diolah kembali oleh penulis

Karakteristik internet yang tidak mengenal batas yurisdiksi memungkinkan pelaku kejahatan siber melakukan kejahatan lintas batas, yang memunculkan tantangan terhadap proses penegakan hukum. Oleh sebab itu, perlu ada kerja sama di tingkat internasional untuk dapat menangani kejahatan di ruang siber secara efektif. Saat ini, sudah terdapat dua kerangka multilateral untuk penanganan kejahatan siber, yakni Budapest Convention dan UN Convention Against Cybercrime (UNCC).

Tabel 3. Kerangka Internasional dalam Keamanan Siber

	Budapest Convention	**UN Convention Against Cybercrime (UNCC)**
Cakupan	*Computer-related forgery:* mengubah atau menghapus data komputer dengan maksud untuk membuat data tidak autentik (*inauthentic data*) dianggap seolah-olah data tersebut autentik. *Computer-related fraud:* kejahatan yang dengan sengaja mengubah dan menghilangkan data komputer untuk keuntungan ekonomi. *Content-related offence* mengenai pornografi anak.	Menetapkan definisi kejahatan siber yang lebih luas, termasuk *cyber-dependent crimes* seperti akses ilegal terhadap informasi dan peretasan jaringan komputer serta *cyber-enabled crimes* seperti pornografi anak.
Lingkup Kerjasama	*Mutual legal assistance* dalam pengumpulan bukti elektronik suatu kejahatan sebagaimana didefinisikan dalam konvensi ini untuk dilakukannya investigasi dan penegakan hukum.	Kerja sama mencakup: (1) Penggeledahan, penyitaan, dan pembekuan barang bukti elektronik; (2) Pengumpulan data lalu lintas (*traffic data*); dan (3) Perpindahan bukti elektronik dari suatu negara ke negara lain untuk menangani kejahatan serius.

Sumber: diolah kembali oleh penulis

Convention on Cybercrime of the Council of Europe atau juga dikenal sebagai Budapest Convention diadopsi pada tahun 2001 dan mulai berlaku pada tahun 2004. Konvensi ini bertujuan untuk melindungi masyarakat sipil dari kejahatan di ruang siber. Kejahatan yang dimaksud berfokus pada *computer-related forgery, computer-related fraud,* serta kejahatan terkait konten yakni pornografi anak.[40] Konvensi ini dibentuk

40 *Article 19, The Council of Europe Convention on CYbercrime and the First and Second*

untuk memfasilitasi kerja sama dalam investigasi kriminal, termasuk pengumpulan bukti elektronik suatu kejahatan antara negara-negara penandatangan perjanjian.[41]

Pada tahun 2024, Majelis Umum PBB juga mengadopsi UN Convention Against Cybercrime (UNCC) dan telah ditandatangani oleh 60 negara, termasuk Rusia, Kanada, dan Uni Eropa.[42] Konvensi yang menjadi instrumen pelengkap dalam menangani kejahatan siber ini menetapkan setidaknya dua jenis kejahatan siber, yakni *cyber-dependent crime* dan *cyber-enabled crime.*[43] *Cyber-dependent crime* yang dimaksud dalam konvensi ini adalah akses ilegal atau peretasan terhadap jaringan komputer. Sedangkan *cyber-enabled crime* merupakan kejahatan yang dilakukan melalui komputer untuk mendapatkan keuntungan pribadi, misalnya pornografi anak. Konvensi ini juga memuat prosedural dalam investigasi kejahatan siber yang memungkinkan pencarian dan penyitaan bukti elektronik, termasuk data lalu lintas (*traffic data*) yang berkaitan dengan suatu pelanggaran. Dalam hal penegakan hukum, konvensi ini memfasilitasi ekstradisi dan *mutual legal assistance* bagi negara-negara penandatangan apabila suatu pelanggaran terjadi di wilayah yurisdiksinya.

Meskipun memberikan pedoman kerja sama dalam penanganan kejahatan siber, tetapi kedua konvensi tersebut tidak terlepas dari beberapa kekhawatiran menyangkut HAM, keamanan dan privasi, dan kebebasan berpendapat. Sebab, negara-negara yang meratifikasi konvensi ini dapat menjadikannya sebagai dasar untuk mengumpulkan informasi pribadi dan aktivitas daring masyarakat sipil sebagai pengguna internet. Pada konteks spesifik dalam UNCC, penegakan hukum yang dilakukan secara lintas batas memungkinkan dimotivasi oleh alasan politik. Sehingga memungkinkan bila konvensi ini mengakomodasi praktik-praktik intrusif bagi negara-negara yang memiliki rekaman kurang baik terhadap HAM di negaranya seperti Rusia, Tiongkok, dan Myanmar.

Additional Protocol, https://www.article19.org/wp-content/uploads/2022/06/Budapest-Convention-analysis-May-2022.pdf

41 *Convention on Cybercrime,* https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf

42 *Dig Watch, "UN cybercrime treaty signed in Hanoi amid rights concerns," 27 October 2025,* https://dig.watch/updates/un-cybercrime-treaty-signed-in-hanoi-amid-rights-concerns

43 *Nguyen Thanh Trung, "Addressing the Criticism against the United Nations Convention against Cybercrime," National University of Singapore," n/d,* https://cil.nus.edu.sg/blogs/addressing-the-criticisms-against-the-united-nations-convention-against-cybercrime/

5.3. Catatan Kritis atas Draf Rancangan UU KKS

Pada tanggal 12 Februari 2024, pemerintah mengadakan rapat panitia antarkementerian membahas RUU KKS. Rancangan yang mulanya menjadi inisiatif DPR pada 2019 lalu, saat ini menjadi inisiatif pemerintah dalam Prolegnas Tahun 2025-2029. Rancangan RUU KKS kali ini terdiri atas 104 pasal dengan 15 jenis kejahatan baru. Dalam rancangan ini juga, BSSN akan bertransformasi menjadi Badan Siber Republik Indonesia dan dilekati fungsi penyidikan. Badan ini merupakan lembaga negara setingkat menteri yang bertanggung jawab langsung kepada Presiden. Tak hanya itu, RUU ini memuat materi-materi lain yang penting dalam tata kelola keamanan siber di Indonesia. Sayangnya, proses perumusan RUU ini minim partisipasi dan dilakukan secara senyap.

Secara umum pembicaraan mengenai kebijakan keamanan siber mengarah pada panduan yang dirancang untuk mencapai beberapa tujuan, antara lain perlindungan terhadap Individu, perlindungan terhadap perangkat, dan perlindungan terhadap jaringan. Individu sebagai salah satu tujuan utama dalam keamanan siber akan meletakkan pendekatan berbasis hak sebagai suatu cara pandang sekaligus kerangka yang harus muncul sedari prosesnya. Hal ini hanya dapat dicapai manakala proses perumusan legislasi melibatkan para pemangku kepentingan, termasuk masyarakat. Sayangnya, beberapa hal ini tidak tercermin dalam beberapa draf Februari 2025 maupun versi 1 Oktober 2025.

Dalam versi terakhirnya di Oktober 2025, draf RUU KKS berubah secara signifikan dengan mengurangi beberapa ketentuan pidana, mengubah aspek kelembagaan, dan memperjelas tata kelola ketahanan siber. Akan tetapi, masih terdapat beberapa wilayah penting dalam draf termutakhir ini yang penting untuk dielaborasi lebih lanjut serta direorientasi agar mengarah pada pendekatan berbasis HAM.

5.3.1. Reorientasi Tujuan Keamanan Siber dan Pelindungan Individu

Keamanan siber dan HAM memiliki keterkaitan erat. Langkah-langkah tepat dalam meningkatkan keamanan siber berpotensi besar untuk memperkuat perlindungan terhadap hak-hak individu serta mengurangi risiko pelanggaran akibat serangan siber, khususnya terkait hak atas privasi dan kebebasan berekspresi. Namun, kebijakan yang dijalankan atas nama keamanan siber juga dapat menimbulkan ancaman terhadap HAM. Oleh karena itu, kerangka umum legislasi ini harus dimulai dengan mereorientasi tujuannya.

Menurut rancangan, tujuan dari undang-undang keamanan dan Ketahanan Siber mencakup beberapa aspek strategis, yaitu:[44]

1. Menjaga kepentingan nasional dari potensi ancaman dan serangan di ruang siber.
2. Melindungi infrastruktur informasi agar tetap tangguh dalam menghadapi gangguan siber.
3. Meningkatkan daya saing nasional dan mendorong inovasi teknologi digital secara bertanggung jawab, dengan tetap memenuhi standar keamanan dan ketahanan siber.
4. Mendukung pertumbuhan ekonomi digital melalui pemanfaatan ruang siber yang aman serta memperkuat kolaborasi antar pemangku kepentingan.
5. Mendorong penguatan keamanan dan ketahanan siber pada tingkat global melalui kerja sama internasional yang berkelanjutan.

Sebagian besar kebijakan keamanan siber diawali dengan bagian pendahuluan yang merumuskan kerangka strategi serta visi pemerintah mengenai keamanan siber dalam lingkup yurisdiksinya. Meskipun bagian ini bukan merupakan inti dari strategi, ia memiliki signifikansi tinggi dalam konteks HAM. Pendekatan terhadap keamanan siber dapat beragam, misalnya sebagai upaya menjaga keamanan nasional atau mendorong pertumbuhan ekonomi digital sebagaimana tercermin di Indonesia.

Namun, apabila HAM tidak menjadi bagian integral dari pemahaman dan visi negara terhadap keamanan siber, maka bagian substansial dari strategi tersebut cenderung tidak mendukung penghormatan, perlindungan, dan pemenuhan HAM. Oleh karena itu, bagian yang merumuskan kerangka atau visi keamanan siber dalam legislasi keamanan siber perlu secara eksplisit mengakui peran penting keamanan siber dalam melindungi hak-hak individu.

Keamanan individu adalah tujuan inti dari keamanan siber, dan internet yang aman merupakan pusat perlindungan HAM dalam konteks digital. Bahkan dalam definisi mengenai keamanan siber yang dikembangkan FOC, ditegaskan bahwa privasi dan kerahasiaan informasi adalah penting untuk keamanan individu, juga terhadap data, terutama dalam konteks digital di mana keamanan fisik dan informasi digital saling berhubungan. Pendekatan berbasis HAM sangat penting dalam mengingatkan para pembuat kebijakan, bahwa keamanan siber harus memperhitungkan keamanan individu dan HAM dan, sebagai konsekuensinya, kebijakan keamanan siber harus didesain dengan tujuan menghormati dan melindungi HAM.

44 Pasal 4 RUU KKS versi 1 Oktober 2025

5.3.2. Mendudukkan Kembali Ketahanan Siber dan Pertahanan Siber

Naskah akademik RUU KKS memaknai bahwa "ketahanan siber atau *cyber defense* merupakan suatu upaya untuk menanggulangi serangan siber yang menyebabkan terjadinya gangguan terhadap penyelenggaraan pertahanan negara".[45] Pengertian ini di samping menyamakan *resilience* sebagai *defence*, juga menyempitkan ketahanan siber hanya pada sektor pertahanan. Padahal secara konsep, resiliensi atau ketahanan tidak sama dengan pertahanan. Menurut Dorothy E. Denning, pertahanan siber dapat diklasifikasikan ke dalam dua kategori utama, yaitu *active cyber defense* dan *passive cyber defense*, yang merujuk pada prinsip-prinsip pertahanan aktif terhadap serangan udara dan misil.[46] *Active cyber defense* merujuk pada strategi pertahanan yang bersifat proaktif, yakni tindakan langsung yang bertujuan untuk menetralisasi, mengeliminasi, atau mengurangi efektivitas ancaman siber terhadap sistem, personel, dan aset yang dilindungi. Sementara itu, *passive cyber defense* mencakup seluruh bentuk perlindungan yang tidak termasuk dalam kategori aktif, yang difokuskan pada upaya mitigasi dampak dan pengurangan kerentanan terhadap serangan siber melalui mekanisme preventif dan protektif.

Sementara itu, pengertian ketahanan siber mencakup ruang lingkup lebih luas. Cyber Resilience Act (CRA) di Uni Eropa, misalnya, secara umum empat tujuan utama ketahanan siber yang tidak satu pun secara khusus membatasi pengertiannya, antara lain:[47]

1. Mendorong produsen untuk meningkatkan aspek keamanan produk yang memiliki komponen digital, dimulai sejak tahap perancangan dan pengembangan hingga seluruh siklus hidup produk.
2. Menetapkan kerangka kerja keamanan siber yang terpadu guna mempermudah kepatuhan bagi para pengembang perangkat keras dan perangkat lunak.
3. Meningkatkan keterbukaan informasi terkait karakteristik keamanan dari produk yang mengandung elemen digital.
4. Memastikan bahwa pelaku usaha dan konsumen dapat menggunakan produk digital secara aman.

Bahkan, CRA menegaskan bahwa ketentuan dalam regulasi ini tidak mencakup produk yang memiliki elemen digital yang dikembangkan atau diubah secara khusus untuk kepentingan keamanan nasional

45 *Naskah Akademik RUU Keamanan dan Ketahanan Siber 2025*

46 https://www.sciencedirect.com/science/article/abs/pii/S0167404813001661

47 *Cyber Resilience Act* https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

atau pertahanan, maupun produk yang secara khusus dirancang untuk menangani informasi yang bersifat rahasia.[48]

Ketahanan siber juga muncul misalnya dalam Direktif Kebijakan Presiden Nomor 21, yang dikeluarkan Pemerintah Amerika Serikat pada 12 Februari 2013, menetapkan kebijakan nasional terkait keamanan dan ketahanan infrastruktur kritis. Dalam konteks ini, ketahanan (*resilience*) diartikan sebagai kemampuan suatu sistem untuk melakukan persiapan, beradaptasi terhadap perubahan kondisi, serta bertahan dan pulih secara cepat dari gangguan. Ketahanan mencakup kapasitas untuk menghadapi dan mengatasi berbagai bentuk gangguan, baik yang bersifat disengaja seperti serangan, maupun yang tidak disengaja seperti kecelakaan atau ancaman alam.[49]

Pada penormaan dalam draf RUU, ketahanan siber dilaksanakan melalui peningkatan kapasitas sumber daya manusia, peningkatan kapasitas teknologi; dan peningkatan kapasitas proses bisnis.[50] Pengecualian terhadap standar dan tata kelola ketahanan siber, utamanya terkait produk dengan elemen digital diadopsi oleh RUU dalam dua hal. Pertama, pengecualian terhadap kewajiban menyampaikan informasi kerentanan Produk dengan Elemen Digital (PDED) dan perbaikannya kepada otoritas yang menjalankan tugas dan fungsi keamanan dan ketahanan siber. Kedua, pengecualian terhadap kewajiban dilaksanakannya audit oleh otoritas manakala terdapat indikasi ketidakpatuhan penerapan standar keamanan rantai pasokan.[51]

Oleh karena itu, RUU KKS masih secara sumir membedakan ketahanan dan pertahanan siber. Di satu sisi, ketahanan siber dibayangkan sebagai bagian dari upaya pertahanan untuk menjaga kedaulatan negara.[52] Namun, di sisi lain, beberapa kewajiban penting untuk menjaga resiliensi justru dikecualikan manakala berkaitan dengan pertahanan. Pengecualian terhadap sektor intelijen, sektor penegakan hukum, dan sektor pertahanan dikhawatirkan akan menjadi *leeway* pada sektor-sektor berpotensi lebih kritikal dari energi dan telekomunikasi.[53] Hal ini mungkin dilakukan dengan syarat bahwa standar pada sektor yang dikecualikan lebih tinggi menurut kerangka undang-undang di masing-masing institusi.

---

48 *Pasal 2 Nomor 7 Cyber Resilience Act* https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

49 *The White House Office of the P.S. Presidential Policy Directive, Critical Infrastructure Security and Resilience.*https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructuresecurity-and-resil

50 *Pasal 23 RUU KKS versi 1 Oktober 2025*

51 *Pasal 32 ayat 3 dan Pasal 38 ayat 3 RUU KKS. versi 1 Oktober 2025*

52 *Pasal 3 terkait asas dan Pasal 4 terkait tujuan RUU KKS versi 1 Oktober 2025*

53 *Dikutip dari hasil FGD "Diskusi Kelompok Terpumpun (FGD) Telaah Urgensi dan Catatan atas RUU KKS" Kamis, 23 Oktober 2025*

5.3.3. Mengeluarkan Kewenangan TNI dalam Penegakkan Hukum pada Tindak Pidana Nonmiliter

Rancangan Undang-Undang ini menimbulkan kekhawatiran serius terhadap prinsip demokrasi dan negara hukum, terutama karena adanya ketentuan yang mengizinkan TNI bertindak sebagai penyidik dalam kasus pidana yang berkaitan dengan keamanan dan ketahanan siber. Pasal 56 (1) dari draf RUU KKS versi Oktober 2025 mengatur bahwa penyidikan terhadap tindak pidana bidang keamanan dan ketahanan siber dilakukan oleh, salah satunya, penyidik TNI yang diberi kewenangan sebagai penyidik tindak pidana bidang keamanan dan ketahanan siber.

Pelibatan TNI sebagai aparat penegak hukum dalam tindak pidana nonmiliter ini bertentangan dengan Pasal 30 ayat (3) UUD 1945, yang menyatakan bahwa tugas TNI adalah menjaga keutuhan dan kedaulatan negara, bukan menjalankan fungsi penegakan hukum. Formulasi pasal ini memperlihatkan meningkatnya campur tangan militer dalam ranah sipil, yang merusak prinsip supremasi sipil dalam sistem hukum demokratis, di mana penegakan hukum pidana seharusnya menjadi kewenangan institusi sipil. Keterlibatan TNI dalam proses penyidikan pidana, termasuk dalam isu siber, tidak hanya melanggar konstitusi dan UU TNI, tetapi juga berpotensi mengancam kebebasan sipil dan nilai-nilai demokrasi.[54]

Jika pasal ini disahkan, semakin terlihat militerisasi ruang siber di Indonesia pascapengesahan UU TNI pada Maret 2025, yang telah memberi kewenangan luas terhadap militer untuk melakukan operasi militer selain perang (OMSP) di ruang siber. Penambahan tugas ini menjadi bermasalah karena tidak adanya kejelasan mengenai tingkat ancaman yang dimaksud. Ketidakpastian dalam definisi ancaman siber memberikan celah bagi keterlibatan militer dalam berbagai aspek penanganannya, bahkan pada situasi yang tidak berkaitan langsung dengan perang siber. Padahal, peran TNI dalam pertahanan siber semestinya terbatas pada strategi defensif, baik secara aktif, dengan cara menetralisir atau mengurangi dampak serangan siber terhadap personel dan aset militer, maupun secara pasif, melalui tindakan perlindungan yang bertujuan mengurangi risiko terhadap kekuatan militer.[55]

Pemberian kewenangan baru terhadap TNI ini bertentangan dengan prinsip-prinsip dalam negara demokrasi yang memisahkan kewenangan militer dari penegakan hukum pada tindak pidana nonmiliter. Keberadaan pasal ini masih menunjukkan orientasi yang dominan terhadap kepentingan negara *(state-oriented),* alih-alih berfokus pada perlindungan hak dan

54 *Lihat : Penyidik TNI dalam RUU KKS, Ancam Demokrasi dan Negara Hukum* https://pbhi.or.id/penyidik-tni-dalam-ruu-kks-ancam-demokrasi-dan-negara-hukum/

55 *Ibid.*

kebebasan individu (*people-oriented*) sekaligus mempertegas aspek pertahanan alih-alih resiliensi itu sendiri. Tindak pidana yang diatur dilihat sebagai ancaman terhadap eksistensi negara, bukan keamanan bagi individu.

5.3.4. Harmonisasi Legislasi Keamanan dan Ketahanan Siber dengan Kejahatan Siber

Perumusan legislasi keamanan siber di Indonesia kerap kali mencampuradukan sesuatu yang berkaitan dengan siber ke dalam satu peraturan perundangan. Arah pengaturan ini muncul dalam draf versi Februari maupun versi Oktober. Dalam versi pertamanya, terdapat 15 jenis kejahatan baru yang menjadi salah satu materi muatan dalam regulasi keamanan siber. Bahkan, di antara 15 pasal tersebut terdapat tiga delik baru yang berkaitan dengan *content related crime.* Draf RUU ini melihat *deepfake* sebagai bagian dari serangan siber sehingga diatur secara khusus dalam rancangan. Draf RUU ini mengatur bahwa setiap orang yang dengan sengaja membuat, menyebarluaskan, atau memfasilitasi penyebaran konten *deepfake* yang mengakibatkan kekacauan publik, merugikan kepentingan nasional dipidana penjara paling lama 10 tahun dan/atau denda paling banyak Rp2.000.000.000 (dua miliar rupiah). Sementara *deepfake* yang menyerang kehormatan orang lain, dipidana dengan pidana penjara paling lama 2 tahun dan/atau denda paling banyak Rp750.000.000 (tujuh ratus lima puluh juta rupiah).

Sementara itu, perubahan signifikan terdapat dalam draf versi Oktober 2025. Draf RUU ini mengenalkan sejumlah ketentuan pidana baru dalam konteks ruang siber (Pasal 58, 59, dan 60), disertai dengan ancaman pidana yang tergolong berat (Pasal 61 hingga 64).[56]

a. *Pasal 61 Setiap Orang yang melakukan tindakan yang mengganggu, merusak, menghancurkan, melumpuhkan, atau membuat IIK (Infrastruktur Informasi Kritis, pen.) tidak dapat digunakan atau mengakibatkan terganggunya atau tidak berfungsinya IIK sebagaimana dimaksud dalam Pasal 58 dipidana dengan pidana penjara paling lama 15 (lima belas) tahun atau pidana denda paling banyak kategori VIII.*
b. *Pasal 62 Setiap Orang secara tanpa hak mengakses IIK sebagaimana dimaksud dalam Pasal 59 dipidana dengan pidana penjara paling lama 15 (lima belas) tahun atau pidana denda paling banyak kategori VIII.*
c. *Pasal 63 Setiap Orang yang memperoleh, memproduksi, menjual,*

56 *RUU KKS versi 1 Oktober 2025*

mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, memiliki, atau menguasai: a. perangkat keras atau perangkat lunak sistem elektronik yang dirancang, diadaptasi, atau dikembangkan untuk melakukan tindak pidana di bidang Keamanan dan Ketahanan Siber yang ditujukan terhadap IIK; atau b. kata sandi, kode akses, tanda tangan elektronik atau data serupa dengan itu yang digunakan untuk melakukan tindak pidana di bidang Keamanan dan Ketahanan Siber yang ditujukan terhadap IIK sebagaimana dimaksud dalam Pasal 60,

d. *Pasal 64 Perbuatan sebagaimana dimaksud dalam Pasal 61, Pasal 62 ayat (1) dan ayat (2) huruf a, dan Pasal 63 tidak dipidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian IIK, atau untuk pelindungan yang diotorisasi dari IIK itu sendiri secara sah dan tidak melawan hukum.*

Meskipun tindak-tindak pidana tersebut bukan *content-related crime*, tetapi pembuat kebijakan perlu mempertegas perbedaan antara keamanan siber dan kejahatan siber. Aturan kejahatan siber dimaksudkan untuk mengatur kejahatan yang dilakukan dengan perangkat digital dan komputer, seperti *phising, doxing,* menyebarkan virus, atau merusak sistem, termasuk juga pencurian atau penipuan yang dilakukan dalam jaringan *(online)*. Sedangkan keamanan siber harusnya hanya berfokus pada upaya untuk melindungi keamanan individu, perangkat digital *(devices)*, dan jaringan *(network).* Pasal-pasal serupa terdapat di dalam legislasi lain yang mengatur mengenai kejahatan siber seperti UU ITE dan KUHP baru. Oleh karena itu, RUU ini perlu mengharmonisasikan jenis-jenis kejahatan baru di dalam RUU ini dengan jenis kejahatan serupa yang tersebar di beberapa UU yang telah berlaku untuk menghindari over-kriminalisasi. RUU KKS seharusnya lebih fokus mengatur mitigasi dan tata kelola, alih-alih pemidanaan.

Dengan demikian penting untuk memisahkan secara tegas antara urusan pertahanan siber dan penanganan kejahatan siber. Menggabungkan keduanya dalam satu regulasi berisiko menimbulkan penyalahgunaan kewenangan yang lebih besar. Oleh karena itu, juga penting untuk menetapkan batas yang jelas, serta mendefinisikan secara rinci pembagian peran, kewenangan, dan tanggung jawab di antara para pemangku kepentingan dalam ekosistem tersebut. BSSN memiliki peran dalam mendeteksi serangan siber melalui pemantauan terhadap anomali lalu lintas data. Apabila dari hasil pemantauan tersebut ditemukan indikasi tindak pidana, maka BSSN seharusnya menyerahkan kasus tersebut kepada kepolisian untuk dilakukan penyidikan, yang selanjutnya dilimpahkan ke kejaksaan hingga proses peradilan. Namun, dalam RUU yang beredar saat ini, mekanisme penanganan semacam itu belum tergambar secara jelas dan sistematis.[57]

57 *Dikutip dari hasil FGD "Diskusi Kelompok Terpumpun (FGD) Telaah Urgensi dan Catatan atas RUU KKS" Kamis, 23 Oktober 2025*

5.3.5. Mengakomodasi Model Multipemangku Kepentingan

Perlindungan HAM secara mendasar membutuhkan adanya pemisahan kekuasaan politik yang dijalankan melalui mekanisme formal pengawasan timbal balik (*checks and balances*), baik di tingkat nasional maupun internasional. Mekanisme ini memberikan makna lebih mendalam dan konkret terhadap konsep "*multistakeholderism*," yang sebelumnya cenderung bersifat permukaan atau simbolik.[58]

Dalam draf RUU KKS versi Februari 2025, penyelenggaraan keamanan dan ketahanan siber dilakukan melalui peran pemerintah, strategi nasional keamanan dan ketahanan siber, kerangka kerja keamanan siber; tata kelola PDED, kewajiban Penyelenggara IIK, pemantauan, dan evaluasi; lalu pelaporan Insiden Siber, dan koordinasi antarlembaga. Dalam skema tersebut, tidak ada keterlibatan masyarakat maupun swasta dalam tata kelola keamanan siber pada RUU. Sementara itu, dalam draf Oktober 2025, masyarakat dapat berpartisipasi baik secara langsung maupun tidak langsung dalam mendukung terselenggaranya keamanan dan ketahanan Siber. Bentuk partisipasi masyarakat justru diamanatkan untuk diatur dalam Peraturan Pemerintah.[59]

Kendati telah dirumuskan demikian, RUU ini belum mampu untuk mengakomodasi pendekatan multipemangku kepentingan. Berdasarkan cara-cara di atas, secara eksplisit RUU ini menginginkan bahwa penyelenggaraan keamanan siber di Indonesia dilakukan sepenuhnya oleh pemerintah, tanpa melibatkan pemangku kepentingan lain dalam pengambilan keputusan yang pada dasarnya berdampak pada masyarakat itu sendiri. Dari sudut pandang yang berorientasi pada manusia, memastikan keterwakilan yang beragam dalam pengaturan tata kelola bukanlah sekadar penghormatan simbolis terhadap pluralisme; melainkan merupakan unsur esensial dan konstitutif dalam pembatasan kekuasaan politik.[60]

Oleh karena itu, RUU KKS seharusnya secara esensial meletakkan masyarakat sebagai pemangku kepentingan yang memiliki kuasa untuk terlibat dalam menentukan tata kelola keamanan siber. Keterlibatan masyarakat sipil perlu diakomodasi di level undang-undang dan tidak diserahkan lebih lanjut melalui peraturan pemerintah tanpa ruang lingkup yang jelas. RUU KKS perlu melakukan pemetaan aktor sehingga terbentuk ekosistem serta model-model penjangkauan yang bisa dilakukan baik oleh pemerintah dan swasta dengan perannya masing-masing. Misalnya,

58 *Deibert, Ronald J. "Toward a Human-Centric Approach to Cybersecurity." Ethics & International Affairs 32, no. 4 (2018): hlm. 411*

59 *Pasal 53 RUU KKS versi Oktober 2025*

60 *Pasal 53 RUU KKS versi Oktober 2025*

komunitas teknis ini dapat tergabung dalam *computer emergency response team.*[61]

5.3.6. Harmonisasi Tata Kelola Kecerdasan Artifisial dengan RUU Keamanan dan Ketahanan Siber

Legislasi keamanan siber menjadi salah satu aspek utama dalam pengembangan tata kelola AI yang bertanggung jawab dan dapat dipercaya, sebagaimana juga telah diakui oleh Stranas AI. Dalam versi Februari 2025, terdapat 19 kata kecerdasan artifisial yang tersebar di pasal 13 dan pasal 43 rancangan. RUU KKS mewajibkan produsen PDED untuk melakukan pemberitahuan pada BSSN/BSRI dalam setiap pengembangan, penerapan, dan/atau produksi kecerdasan artifisial. BSSN/BSRI juga diberikan kewenangan untuk melakukan koordinasi, pengawasan, penindakan, dan evaluasi terhadap penggunaan kecerdasan artifisial pada IIK untuk Penyelenggaraan Peningkatan Kapasitas Keamanan Siber. Perumusan skema kewenangan ini berangkat dari ragam ancaman siber yang diperkuat melalui teknologi AI.

Beberapa jenis serangan tersebut adalah:[62]

1. *AI Generated Cyber Attack. Penyerang menggunakan AI untuk membuat malware yang adaptif dengan ingkungannya (polymorphic dan metamorphic malware) sehingga deteksi sistem keamanan menjadi sangat sulit.*
2. *Deepfake dan Social Engineering. AI dapat digunakan untuk membuat video palsu yang sangat meyakinkan dari orang penting yang dapat menjadi ancaman secara finansial dan berdampak pada stabilitas politik serta kepercayaan publik.*
3. *Automated Disinformation Campaigns. AI dapat digunakan untuk meluncurkan kampanye disinformasi dan hoaks secara massal yang dapat memecah belah sosial dan mengganggu proses demokrasi.*
4. *AI-Powered Vulnerability Discovery. Peretas menggunakan AI untuk memindai kerentanan dalam sistem elektronik pemerintah dengan kecepatan lebih tinggi dibanding keamanan sistem elektronik pemerintah.*

Rencana penambahan kewenangan BSSN/BSRI terkait tata kelola AI di atas kemudian dihapus di dalam draf Oktober 2025. Dalam draf terbaru,

---

61 *Dikutip dari hasil FGD "Diskusi Kelompok Terpumpun (FGD) Telaah Urgensi dan Catatan atas RUU KKS" Kamis, 23 Oktober 2025*

62 *Diambil dari paparan Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia BSSN, 22 Oktober 2025*

prinsip-prinsip etika AI yang semula muncul di dalam Surat Edaran Kominfo, kali ini diadopsi ke dalam rancangan. Konsekuensinya, prinsip tersebut akan bertransformasi dari semula sebagai instrumen sukarela, menjadi *legally binding.*

Penegakkan terhadap etika tersebut akan bertumpu pada kewenangan pemerintah yang didesain dalam RUU ini. Pemerintah (merujuk pada pemerintah pusat) diberikan kewenangan untuk melakukan pengaturan, koordinasi, pembinaan, pengawasan, penindakan, dan evaluasi terhadap pengembangan dan pemanfaatan kecerdasan artifisial (Pasal 36 RUU KKS). Skema kewenangan ini berpotensi tidak selaras dengan peta jalan yang mengedepankan pendekatan multipemangku kepentingan dan *co-regulation*, alih-alih *direct regulation*. Di samping itu, penting untuk melihat arah pengembangan model tata kelola yang sedang dikembangkan oleh K/L lain untuk menghindari tumpang tindih kewenangan yang berakibat pada sektoralisme. Harmonisasi tersebut perlu mempertimbangkan pula beberapa rencana regulasi yang sedang dikembangkan terutama terkait Rancangan Perpres Peta Jalan AI dan Rancangan Perpres Etika AI.[63]

Walau demikian, penting juga untuk mempertimbangkan desain penormaan yang tidak berangkat dari fenomena serangan berbasiskan teknologi baru tertentu. Kecepatan perkembangan *new and emerging technology* lain akan dengan mudah menciptakan kebutuhan akan jaring pengaman tambahan di level legislasi maupun pengaturan di bawahnya.

Sebagaimana diakui oleh BSSN, serangan siber hari ini tidak hanya berbasis pada AI, tetapi juga spesifik menggunakan teknologi *quantum computing*. Teknologi ini bisa menerobos kriptografi modern yang membuat algoritma seperti RSA dan ECC yang melindungi komunikasi, data sensitif pemerintah, transaksi keuangan dapat dipecahkan.[64] Dengan maraknya kebocoran data pribadi, penyerang juga sudah dapat dengan mudah mengumpulkan data rahasia yang terenkripsi, sehingga di kemudian hari didekrip ketika *quantum computing* sudah tersedia secara praktis. Pusat Keamanan Siber Nasional (NCSC) Inggris juga telah menerbitkan panduan baru yang merekomendasikan agar entitas besar, termasuk penyedia layanan energi dan transportasi, mengadopsi "kriptografi pasca-kuantum" guna mencegah teknologi kuantum digunakan untuk meretas sistem mereka.[65]

63 *Judul rancangan regulasi ini sewaktu-waktu bisa berubah.*

64 *Diambil dari paparan Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia BSSN, 22 Oktober 2025*

65 *UK cybersecurity agency warns over risk of quantum hackers* https://www.theguardian.com/technology/2025/mar/20/uk-cybersecurity-agency-quantum-hackers

Dengan demikian keterhubungan teknologi baru dan ancaman siber tidak akan berhenti pada isu-isu seputar kecerdasan artifisial belaka. Perkembangan teknologi yang akan makin masif ke depan membutuhkan respons visioner yang tidak terbatas pada jenis-jenis serangan berdasarkan basis teknologi tertentu. Respons terhadap perkembangan serangan-serangan jenis baru ini akan lebih efektif dan adaptif jika diletakkan sebagai panduan (*guideline)* sebagaimana juga dilakukan negara-negara dalam menghadapi jenis *malware* baru hingga teknologi baru seperti quantum maupun kecerdasan artifisial.

5.4. Pentingnya Pendekatan Berbasis HAM dalam Legislasi Keamanan Siber

Pertemuan antara HAM, keamanan siber, dan tata kelola internet mencapai momentumnya setelah diskusi ini diperkuat oleh resolusi Dewan HAM PBB pada 2012 yang meletakkan bahwa HAM berlaku baik secara daring maupun luring.[66] Dalam studinya, APC memberikan gambaran lebih praktis bagaimana hubungan antara HAM dan keamanan siber ini terjadi. Dalam studi ini salah seorang responden menggarisbawahi benang merah penting antara HAM dan keamanan siber tersebut, bahwa "Kehidupan pribadi kita memiliki bagian digital. Fail rekaman kami, gambar, pesan, sejarah, interaksi sosial makin terjadi dalam bentuk digital. Ingatan kita juga terkait dengan pengalaman digital."[67]

Diskusi keamanan siber dan HAM dalam perkembangannya datang bersamaan terkait masalah hak sipil dan politik serta ekonomi dan budaya. Bentuk konvergensi ini dapat dilihat di bidang-bidang seperti kebebasan internet dan gerakan net neutrality mengenai arus bebas informasi yang merupakan bagian dan paket pendekatan multipemangku kepentingan untuk tata kelola internet.[68] Pada titik itu pula pertemuan antara HAM dan keamanan siber secara operasional terjadi dalam pelaksanaan Panduan BHAM. Banyak perusahaan menerapkan prinsip-prinsip dalam HAM untuk menanamkan praktik terbaik HAM dalam pengambilan keputusan mereka, bersama dengan kerangka keamanan siber, untuk membantu memandu investasi keamanan siber perusahaannya.[69]

---

66 *Resolusi Dewan HAM PBB No. A/HRC/20/L.13 diakses dari* https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F20%2FL.13&Language=E&DeviceType=Desktop&LangRequested=False

67 https://www.apc.org/sites/default/files/Putting_cybersecurity_on_the_rights_track.pdf hlm. 14

68 *Scott J. Shackelford, Human Rights and Cybersecurity Due Diligence: A Comparative Study, University of Michigan Journal of Law Reform, Vol. 50, 2017, hlm. 882.*

69 *Ilse Griek, Forum PBB tentang Hak Asasi Manusia: Menilai Kerangka Ruggie,* http://www.sustainalytics.com/assessing-ruggie-framework

Peran perusahaan di atas menjadi antitesis atas konsep keamanan siber yang sedianya hanya berkutat pada pertahanan negara dan penegakan hukum. Konsep tersebut hanya memandang keamanan siber sebagai kepentingan negara belaka atau *state-centric*. Sebaliknya, muncul pendekatan lain yang meletakkan keamanan siber sebagai kepentingan manusia yang sekaligus meletakkannya sebagai objek utama dari keamanan siber. Oleh Diabert hal ini dikenalkan sebagai pendekatan *human-centric*. Oleh karena itu pendefinisian keamanan siber tidak lagi menyangkut masalah teknis semata, tetapi juga perlu mencakup aktor, subjek, objek, tujuan, luaran, serta juga struktur.[70] Walau begitu memang tidak ada definisi yang disepakati secara internasional untuk topik ini termasuk mengenai konsep *human-centric* itu sendiri. Pendekatan *human-centric* pada dasarnya berusaha menjelaskan keamanan siber sebagai bagian integral dari HAM.

Pada tahun 2014 FOC merespons perkembangan diskusi keamanan siber ini dengan menyepakati Deklarasi Tallinn tentang pendekatan HAM dalam pembentukan kebijakan keamanan siber *(human rights based approach on cybersecurity policy making)*.[71] Keamanan siber dalam hal ini telah melengkapi kerangka kerja HAM dan hukum humaniter internasional. FOC menarasikan bahwa "Hukum HAM internasional dan kemanusiaan internasional hukum berlaku daring dan luring. Keamanan siber harus melindungi inovasi teknologi dan pelaksanaan HAM."[72] Marry Robinson menilai bahwa pendekatan ini menambah nilai karena kerangka kerja normatif ini menegaskan tanggung jawab pemerintah terhadap HAM. Konsep pendekatan berbasis hak sebagian besar telah dipromosikan PBB dengan menetapkan seperangkat prinsip dasar HAM untuk inisiasi pembangunan.

Kelompok Ahli Pemerintah untuk Perkembangan di Bidang Informasi dan Telekomunikasi dalam UN General Assembly (68/98) mengungkapkan hal serupa bahwa upaya untuk mengatasi keamanan teknologi informasi dan komunikasi harus berjalan seiring dengan penghormatan terhadap HAM dan kebebasan mendasar yang ditetapkan dalam Deklarasi Universal HAM dan instrumen internasional lainnya. Perserikatan Bangsa-Bangsa pada 21 Desember 2009 menetapkan Resolusi Nomor 64/211 tentang Penciptaan Budaya Global Keamanan Siber dan Inventarisasi Upaya

---

70 Uni Eropa misalnya mendefinisikan keamanan siber sebagai "perlindungan dan tindakan yang dapat digunakan untuk melindungi domain siber, baik di bidang sipil maupun militer, dari ancaman yang terkait dengan atau yang dapat membahayakan jaringan dan infrastruktur informasi yang saling bergantung.

71 Lihat Modul 3 bagian D

72 Deborah Brown, et al. Briefing Document : Cybersecurity Policy and Human Rights. Association for Porgressive Communications. https://www.apc.org/sites/default/files/brief8.pdf

Nasional untuk Melindungi Infrastruktur Informasi Kritis. Resolusi ini memberikan tekanan pada negara-negara untuk:

1. Menggunakan instrumen penilaian yang tepat bagi kebutuhan nasional mereka untuk memastikan perlindungan infrastruktur informasi kritis untuk memperkuat keamanan siber negara tersebut dan secara umum akan berkontribusi pada peningkatan budaya global keamanan siber.
2. Mendorong negara-negara dan organisasi-organisasi regional internasional yang relevan untuk mengembangkan berbagai strategi guna memastikan keamanan siber dan perlindungan infrastruktur informasi kritis.

Pada 5 Desember 2018 PBB menegaskan kepada negara-negara untuk menghormati Resolusi Dewan HAM 20/8 tanggal 5 Juli 2016 dan resolusi 26/13 tanggal 26 Juni 2014 tentang promosi, perlindungan, dan penikmatan HAM di internet, termasuk pula sejumlah Resolusi Majelis Umum tentang hak privasi di era digital. Tata kelola ruang siber yang baik harus membentuk pendekatan berbasis HAM untuk (1) akuntabilitas yang lebih tinggi, (2) transparansi yang lebih besar, dan (3) partisipasi yang lebih luas dari para pemangku kepentingan melalui penggunaan perangkat siber, seperti internet dan perangkat seluler.[73]

Oleh karena itu perlindungan terhadap individu dapat beriringan dengan pengembangan keamanan siber yang berbasis HAM dan demokrasi. Norma dan standar HAM universal dapat menjadi pedoman dan tolok ukur untuk menetapkan rezim pengaturan di ruang siber. Keamanan siber bukan hanya tentang keamanan aset dan informasi, namun juga membahayakan keselamatan individu, baik karena perbuatan jahat yang telah mengganggu keamanan individu secara online maupun oleh kebijakan peraturan perundang-undangan keamanan siber yang telah menekan HAM dan kebebasan mendasar. Secara umum, RUU KKS justru lebih banyak mengatur mengenai kewenangan dan fungsi badan ketimbang tata kelola keamanan siber itu sendiri.

Berkaca dari rancangan tersebut, keberadaan legislasi keamanan siber yang andal dan komprehensif mendesak untuk dibentuk. Kebijakan keamanan siber bertumpu pada strategi regulatif dan tata kelola yang memadai, mulai dari hulu hingga hilir, untuk memastikan dan menjamin kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) sistem. Dalam hal ini, legislasi keamanan siber nasional harus diarahkan bukan semata-mata untuk melindungi infrastruktur fisik belaka, tapi juga individu.

---

73 Anja Mihr, Good Cyber Governance The Human Rights and Multi Stakeholder Approach, Goergetown Journal of Interational Affairs, hlm. 24

Berangkat dari poin-poin di atas, pemerintah perlu mengimplementasikan pendekatan berbasis hak agar memungkinkan penerapan pendekatan yang berpusat pada manusia *(human-centric)*. Pendekatan berbasis hak adalah "ujung tombak" nilai-nilai dan kerangka kerja HAM, yang memberikan dasar substantif untuk mengatasi masalah-masalah yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Oleh karena itu keamanan siber dan HAM harus saling melengkapi, saling menguatkan dan saling bergantung satu sama lain, seperti halnya prinsip-prinsip dalam HAM *(interdependent)*, keduanya harus diupayakan bersama untuk secara efektif mempromosikan kebebasan dan keamanan. Pendekatan berbasis hak tidaklah mungkin dapat dicapai tanpa adanya partisipasi bermakna terutama dari para pemangku kepentingan termasuk juga masyarakat. Salah satu elemen pendekatan berbasis HAM dalam kebijakan keamanan siber adalah proses yang terbuka, inklusif, dan transparan yang melibatkan semua pemangku kepentingan.

Secara umum, pendekatan HAM belum menjadi rujukan utama dalam mengerangkakan tata kelola keamanan dan ketahanan siber dalam rancangan. Hal ini menghasilkan tantangan HAM yang meliputi beberapa topik penting terkait pendekatan yang digunakan, tujuan keamanan siber, hingga keterlibatan aktor militer dalam tata kelola keamanan siber. Beberapa masalah pokok sebagaimana telah disinggung sebelumnya di atas mengindikasikan pentingnya menyusun ulang RUU dengan pendekatan berbasis hak.

FOC mengesahkan rekomendasi Kelompok Kerja FOC tentang Pendekatan HAM dalam Keamanan Siber[74] dan Agenda Tallinn, yang secara menggarisbawahi bahwa penghormatan terhadap HAM dan keamanan di ruang siber harus dianggap sebagai konsep yang saling melengkapi. FOC merekomendasikan hal-hal berikut:[75]

1. Negara-negara perlu mematuhi kewajiban mereka berdasarkan hukum HAM internasional saat mempertimbangkan, mengembangkan, dan menerapkan kebijakan dan peraturan nasional tentang keamanan siber.
2. Negara-negara perlu mengembangkan dan menerapkan undang-undang, kebijakan, dan praktik terkait keamanan siber secara konsisten dengan hukum HAM internasional, serta berusaha meminimalkan dampak negatif potensial terhadap kelompok

74 https://freeandsecure.online/recommendations/)

75 *FOC Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies* https://freedomonlinecoalition.com/wp-content/uploads/2021/06/FOC-Joint-Statement-on-the-Human-Rights-Impact-of-Cybersecurity-Laws-Practices-and-Policies.pdf

rentan dan masyarakat sipil, termasuk pembela HAM dan jurnalis. Hal ini termasuk membangun, jika sesuai, proses dan kerangka kerja pendukung untuk transparansi, akuntabilitas, pengawasan independen dan efektif melalui peradilan atau bentuk lain, serta mekanisme ganti rugi untuk membangun kepercayaan. Hal ini juga dapat mencakup pengintegrasian prinsip-prinsip legitimasi, legalitas, keharusan, atau proporsionalitas ke dalam kebijakan dan praktik.

3. Undang-undang, kebijakan, dan praktik terkait keamanan siber harus dikembangkan melalui pendekatan yang berkelanjutan, terbuka, inklusif, dan transparan yang melibatkan semua pemangku kepentingan.
4. Negara-negara harus mempromosikan kerja sama internasional dalam isu-isu siber yang berfokus pada perlindungan dan pemenuhan HAM guna membangun kepercayaan mutual antara semua pemangku kepentingan.
5. Negara-negara seharusnya berusaha untuk menerapkan aturan, norma, dan prinsip perilaku negara yang bertanggung jawab yang tercantum dalam laporan konsensus UNGGE (2010, 2013, 2015).
6. Negara-negara seharusnya mencari cara untuk menarik perhatian terhadap tindakan yang bertentangan dengan aturan, norma, dan prinsip perilaku negara yang bertanggung jawab guna meningkatkan akuntabilitas, transparansi, dan membantu membangun pola perilaku yang bertanggung jawab.
7. Karena manusia secara langsung terdampak oleh ancaman di ruang siber, termasuk serangan siber, perhatian yang cukup harus diberikan pada dimensi manusia dalam keamanan siber.Hal ini mencakup kerugian langsung dan tidak langsung terhadap kesejahteraan individu yang manifestasinya beragam, termasuk kehilangan nyawa, kehilangan akses terhadap layanan vital, kerugian finansial, pelemahan institusi dan proses demokratis, penindasan hak atas kebebasan berekspresi dan kebebasan berserikat, serta kegagalan menghormati hak untuk bebas dari campur tangan sewenang-wenang atau ilegal terhadap privasi, dan sebagainya.
8. Sesuai dengan undang-undang dan standar peraturan pelindungan data, negara-negara seharusnya mempertimbangkan, sesuai dengan kebutuhan, untuk mengumpulkan dan berbagi data, serta mendanai penelitian, mengenai sifat dan skala kerugian-kerugian yang disebutkan di atas, guna mendukung dan mendorong agenda pembangunan kapasitas siber internasional yang berorientasi pada manusia.

9. Negara-negara seharusnya mendorong pendidikan, literasi digital, pemikiran kritis, pertukaran informasi, serta pelatihan teknis dan hukum sebagai sarana untuk meningkatkan keamanan siber dan membangun kapasitas kolektif di tingkat lokal, regional, dan global.
10. Negara-negara seharusnya mendorong aktor sektor swasta untuk mematuhi Prinsip Panduan PBB tentang Bisnis dan HAM, guna meningkatkan akuntabilitas mereka dan berbagi praktik terbaik dalam hal ini, serta membantu berbagi pelajaran yang dipetik.
11. Negara-negara seharusnya mendorong aktor sektor swasta untuk mempromosikan dan menerapkan kebersihan siber yang baik. Kami sebagai anggota Koalisi Kebebasan Online bermaksud untuk menjadi teladan dan oleh karena itu berkomitmen pada rekomendasi di atas. Kami mendorong semua negara untuk menerapkan rekomendasi ini saat membahas, mengembangkan, dan menerapkan kebijakan terkait keamanan siber.

Meskipun Indonesia tidak tergabung dalam FOC, tetapi penting untuk mempertimbangkan dan mengadopsi rekomendasi-rekomendasi yang dikeluarkan oleh koalisi negara-negara demokratis tersebut yang relevan dan sejalan dengan kepentingan nasional Indonesia dalam menghadirkan regulasi keamanan siber dengan pendekatan HAM. Secara umum, penting bagi RUU KKS untuk memuat beberapa hal utama yang secara ringkas tercermin dalam beberapa hal berikut:

1. **Kerangka kerja, visi, tujuan, dan definisi:** Pendekatan keseluruhan pemerintah terhadap (atau visi tentang) keamanan siber, serta tujuan, prinsip, dan definisi atas istilah-istilah kunci yang menggambarkan pendekatan berbasis HAM
2. **Peran dan tanggung jawab:** peran dan tanggung jawab berbagai pihak dalam mengembangkan dan mengimplementasikan legislasi keamanan dan ketahanan siber.
3. **Ketahanan siber:** tindakan yang akan diambil pemerintah untuk melindungi infrastruktur, jaringan, sistem, informasi, dan pengguna dari serangan siber dan ancaman siber—misalnya, langkah-langkah untuk melindungi infrastruktur nasional kritis, tindakan proaktif oleh Tim Tanggap Insiden Komputer (CIRTs), latihan keamanan siber, penelitian dan pengembangan, serta pembangunan kapasitas.
4. **Tim Tanggap insiden siber:** tindakan yang akan diambil pemerintah saat terjadi serangan siber—misalnya rencana darurat, tindakan reaktif oleh CIRTs, dan penyediaan sumber daya untuk lembaga penegak hukum, serta dukungan bagi bisnis dan individu yang terdampak.

5. **Kerja sama internasional:** cara pemerintah akan bekerja sama dengan pemerintah lain, serta organisasi internasional dan regional, dalam isu-isu keamanan siber. Hal ini biasanya melibatkan kolaborasi untuk menangani ancaman bersama, tetapi juga dapat mencakup promosi nilai-nilai dan prioritas kebijakan luar negeri pemerintah di tingkat internasional dan regional.

Guna menjamin bahwa RUU KKS tidak terdisorientasi pada kepentingan negara belaka, maka secara prinsip rancangan harus memuat beberapa komponen utama dalam konteks pendekatan berbasis HAM sebagaimana tercantum di atas.

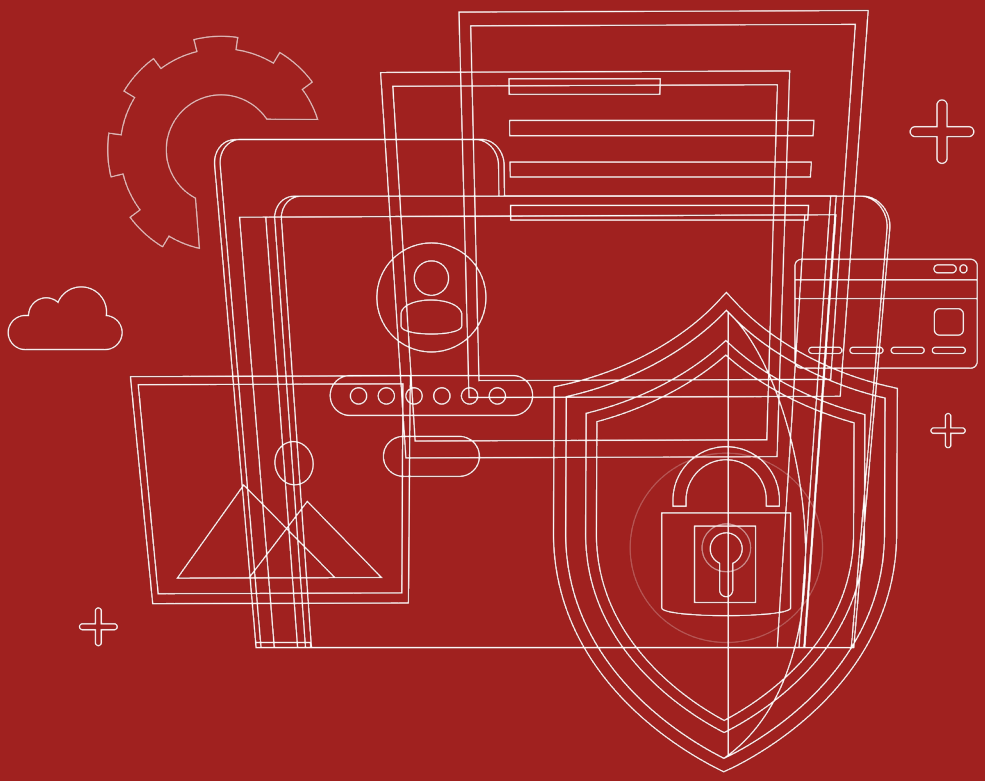
6. KESIMPULAN

Percepatan digitalisasi serta tingginya penetrasi internet di Indonesia menghadirkan peluang bagi transformasi ekonomi, politik, sosial, dan budaya, sekaligus tantangan dalam keamanan siber yang menjadikan ruang digital sebagai domain yang rentan terhadap ancaman siber yang terus berkembang. Dualitas dari ruang siber itu sendiri mencerminkan dua kepentingan utama yang beririsan, tetapi memiliki orientasi berbeda, yakni keamanan nasional dan perlindungan HAM. Hal ini relevan dengan konteks Indonesia yang saat ini sedang dalam proses perancangan UU KKS. Pendekatan berbasis HAM penting untuk dipertimbangkan dalam penyusunan peraturannya agar tidak memperluas kewenangan negara secara berlebihan yang dapat membuka ruang bagi praktik intrusif termasuk penyensoran, pengawasan digital, dan pembatasan kebebasan berekspresi dalam preteks keamanan nasional.

7. REKOMENDASI

Pemerintah perlu mengimplementasikan pendekatan berbasis hak agar memungkinkan penerapan pendekatan yang berpusat pada manusia *(human-centric)*, dengan cara:

1. Mengintegrasikan pendekatan yang berpusat pada manusia dalam kerangka kerja, visi, tujuan, dan definisi yang ada dalam RUU KKS. Hal ini dapat dilakukan dengan memasukkan penghormatan dan pelindungan terhadap HAM dan keamanan individu sebagai salah satu tujuan dari dibuatnya RUU KKS. Keamanan individu adalah tujuan inti dari keamanan siber, dan internet yang aman merupakan pusat perlindungan HAM dalam konteks digital.
2. Mempertegas penggunaan konsep ketahanan siber (*cyber resilience*), alih-alih pertahanan siber (*cyber defense*). Ketahanan siber memiliki cakupan yang luas dan tidak terbatas pada aspek-aspek pertahanan militer.
3. Memperjelas peran dan tanggung jawab setiap lembaga negara yang saat ini menjalani kerja-kerja keamanan dan ketahanan siber. Peran yang dimainkan oleh BSSN, Komdigi, Polri, dan institusi lainnya, harus didefinisikan secara jelas untuk menutup peluang tumpang tindih kewenangan dan egosektoral lembaga ke depannya.
4. Mengeluarkan militer dalam tata kelola keamanan siber, termasuk sebagai penyidik dalam tindak pidana nonmiliter di dalam rancangan. Militer harus dijauhkan dari peran-peran penegakkan hukum pada wilayah sipil demi menjaga supremasi sipil dalam negara demokratis.
5. Mengakomodasi model multi-pemangku kepentingan (multistakeholderisme) dengan memperjelas bentuk-bentuk partisipasi masyarakat dalam penyelenggaraan keamanan dan ketahanan siber. Partisipasi masyarakat dalam multistakeholderisme harus bermakna, tidak hanya sebagai representasi simbolik.
6. Mengharmonisasi jenis-jenis kejahatan dalam RUU KKS dengan legislasi lain. RUU ini perlu mengharmonisasikan jenis-jenis kejahatan baru di dalam RUU ini dengan jenis kejahatan serupa yang tersebar di beberapa undang-undang untuk menghindari over-kriminalisasi.



8. DAFTAR PUSTAKA

1. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), Survei Internet APJII 2025, online.
2. Kevin Socquet-Clerc, Samantha Khoo Su-Yen, Fitriani, Miguel Alberto Gomez and Nguyen Viet Lam. Cybersecurity Governance in Southeast Asia. Thematic SSG Brief. Geneva: DCAF - Geneva Centre for Security Sector Governance, 2023.
3. Nuurrianti Jalli dan Angel Martinez, "Artificial Intelligence is Intensifying South China Sea Disputes in the Philippines," Fulcrum, 25 Februari 2025, online.
4. Kementerian Pertahanan Republik Indonesia, "Kabainstrahan Kemhan Buka FGD tentang Rumusan Ancaman Peperangan Hibrida," 16 Agustus 2023, online.
5. Dani Aswara, "Kaleidoskop 2024: 6 Serangan Siber Besar di Indonesia," Tempo, 31 Desember 2024, online.
6. Willy Medi Christian Nababan, "Data Bais TNI-Inafis Polri Bobol, Dokumen Rahasia, Nama, Foto, NRP, dan Kesatuan Pun Terkuak," Kompas, 26 Juni 2024, online.
7. Sekretaris Kabinet, "President Jokowi Issues Presidential Regulation on Protection for Vital Information Infrastructure," 15 Juni 2022, online.
8. Robb Shawe, "Cybersecurity and Human RIghts: Navigating the Balance between Security and Freedom in the Digital Era," Journal of Information Technology and Integrity, 2025.
9. Alexandra Jonker, Matthew Kosinski, and Gregg Lindemulder, What is cybersecurity, n/d, online.
10. Internet Telecommunication Union (ITU), Definition of cybersecurity, n/d, online.
11. Yuchong Li dan Qinghui Liu, "A Comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, 2021.
12. Novky Asmoro, Marsetio, Susanto Zuhdi, dan Resmanto Widodo Putro, "Management of National Security in Analysis and Threat Assessment of Indonesian Sovereignty," Jurnal Penelitian Pendidikan Indonesia (JPPI) Vol. 8 No. 4, 2022, https://doi.org/10.29210/020221705
13. Mykola Mykolaichuk, Nina Petrukha, Liudmyla Akimova, Nataliia Pozniakovska, Bohdan Hudenko, dan Oleksandr Akimov, "Conceptual principles of analysis and forecasting threats to

national security in modern conditions," Sapienza: International Journal of Interdisciplinary Studies, Vol. 6 No. 2, https://doi.org/10.51798/sijis.v6i2.985

14. Ernst Hirsch Ballin, Huub Dijstelbloem, and Peter de Goede, "Chapter 2: The Extension of the Concept of Security," Shifts in the Security Environment, 2020, https://doi.org/10.1007/978-3-030-37606-2_1
15. Terry Terriff, Stuart Croft, Lucy James, dan Patrick M. Morgan, Security Studies Today, 1999.
16. Ballin, et al. (2020)
17. Resolusi Dewan HAM PBB No. A/HRC/20/L.13 diakses dari https://undocs.org/


DDRN
Digital Democracy
Resilience Network