Urgensi Penataan Keamanan Siber yang Demokratis di Indonesia

Yudha Kurniawan

Pendahuluan

Indonesia saat ini tengah mengalami proses transformasi digital yang pesat. Proses ini ditandai dengan beragam adaptasi masyarakat terhadap teknologi internet dan digital. Masyarakat Indonesia telah cukup familiar dengan penggunaan telepon pintar, menggunakan teknologi internet untuk keperluan sehari-hari, hingga menggunakan platform media sosial untuk berinteraksi sosial secara personal, membangun komunitas, atau sebagai platform dalam mengembangkan bisnis. Semakin banyaknya masyarakat Indonesia yang menggunakan internet dapat dilihat dari tingkat penetrasi internet yang ada di Indonesia. Dari hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada awal tahun 2024, penetrasi ifnternet di Indonesia telah mencapai 79,5% dari total penduduk, naik dari angka penetrasi tahun sebelumnya 78,19% (Santika, 2025). Peningkatan angka tersebut dapat diartikan semakin banyaknya masyarakat yang terlibat dalam pemakaian internet.

Khususnya dalam penggunaan media sosial di Indonesia, riset yang dilakukan pada tahun 2024 oleh *We Are Social*, sebuah situs layanan manajemen media sosial, menunjukkan bahwa 49,9% masyarakat Indonesia atau sekitar 83,5 juta orang telah memiliki dan menggunakan akun media sosial. Dari total pengguna media sosial di Indonesia tersebut, distribusi aplikasi media sosial yang dipakai yaitu: WhatsApp (90,9%), Instagram (85,3%), Facebook (81,6%), TikTok (73,5%), dan Telegram (61,3%) (Rainer, 2025). Jelas, berbagai kemajuan teknologi internet dan variasi penggunaan perangkat digital seperti

telepon pintar (*smartphone*) membuat masyarakat Indonesia semakin banyak menggunakan media sosial.

Selain untuk membangun komunikasi dan jaringan sosial, berkembangnya *platform* media sosial telah membuka kesempatan untuk melakukan transaksi komersial dan melakukan pengembangan bisnis. *Electronic Commerce Business Directory* (ECBD), sebuah situs yang menyediakan layanan data *e-commerce* global, pada risetnya tahun 2024 memperkirakan bahwa Indonesia menjadi negara dengan pertumbuhan *e-commerce* tertinggi di dunia, yaitu sekitar 30,5%, hampir tiga kali lipat dari rata-rata pertumbuhan global (Yonatan, 2025). Hal ini menunjukkan bawa *marketplace* di Indonesia memberikan potensi yang menjanjikan bagi model bisnis yang dilakukan secara daring.

Sebenarnya, semakin tingginya aktivitas masyarakat Indonesia yang dilakukan secara daring telah dimulai sejak Pandemi Covid-19, di mana masyarakat terpaksa menggunakan teknologi internet dan *platform* digital sebagai sarana pendidikan. Saat itu, perkuliahan dan kegiatan pembelajaran hampir seluruhnya dilaksanakan secara daring dengan menggunakan *platform video conference call*. Begitu juga kegiatan seminar dan keagamaan harus dilakukan secara daring. Selama pandemi, adaptasi masyarakat terhadap penggunaan internet dan berbagai *platform* digital merupakan suatu keharusan. Namun adaptasi masyarakat bukannya tidak menemui masalah.

Kesenjangan literasi digital antara masyarakat di wilayah satu dan lainnya menjadi kendala dalam menjalani adaptasi terhadap penggunaan internet. Tidak meratanya akses internet dan infrastruktur digital di seluruh wilayah Indonesia dan rendahnya pemahaman masyarakat tentang keamanan dan etika digital menjadi penyebab kesenjangan itu (Hervianty, 2025). Masyarakat Indonesia menjadi kurang awas terhadap pentingnya keamanan data pribadi dan pentingnya menjaga etika dalam melakukan berbagai aktivitas di ruang siber. Tulisan ini mau menunjukkan betapa urgennya Indonesia untuk

melakukan penataan keamanan siber yang demokratis agar keadilan di ruang siber bagi warga penggunanya bisa diwujudkan.

Ruang Siber dan Keamanan Siber

Proses digitalisasi di Indonesia menunjukkan persoalan utama yang perlu diperhatikan, terutama terkait dengan ruang siber (*cyberspace*) sebagai arena berbagai interaksi digital. Ruang siber bisa didefinisikan sebagai lingkungan kompleks yang dihasilkan dari interaksi manusia, piranti lunak, jasa teknologi dan perangkat internet yang tidak eksis di dunia fisik (Newton, 2015). Sedangkan Gedung Putih Amerika Serikat (AS) mendefinisikan ruang siber sebagai sistem infrastruktur yang terdiri dari ratusan ribu komputer, *server, router, switch,* dan fiber optik yang saling terhubung sehingga membuat infrastruktur penting negara dapat bekerja (Reveron, 2012). Ruang siber menjadi arena penting bagi terciptanya interaksi digital yang kondusif. Oleh karena itu, ruang siber harus dijaga keamanannya agar interaksi antar warga penggunanya tidak terganggu. Singkatnya, keamanan siber harus diwujudkan.

Keamanan siber secara umum dipahami sebagai suatu situasi yang dihasilkan dari berbagai upaya untuk menanggulangi beragam ancaman yang dapat mengganggu interaksi digital di ruang siber. *Computer Science and Telecommunications Board* (CSTB) mendefinisikan keamanan siber sebagai perlindungan terhadap pengungkapan yang tidak diinginkan di ruang siber, perlindungan terhadap modifikasi atau kerusakan sistem, dan juga perlindungan untuk pengamanan sistem itu sendiri (Nissenbaum, 2009). Di tataran praktis, keamanan siber diwujudkan sebagai rangkaian aktivitas dan pengukuran yang dimaksudkan untuk melindungi ruang siber dari serangan, disrupsi, dan ancaman lainnya melalui pengelolaan elemen-elemen ruang siber, perangkat keras, perangkat lunak, jaringan komputer, informasi dan data, dan lain-lain (Fisher, 2005).

Saat ini, berbagai jenis ancaman keamanan siber menjadi masalah serius yang bisa meruntuhkan kedaulatan institusi. Ancaman-ancaman itu ditemukan dalam beragam insiden, mulai dari akses ilegal ke dalam jaringan komputer lain, perusakan terhadap *website* institusi, hingga pencurian data pribadi. Jenis-jenis ancaman siber yang umum dikenal dalam *IT Governance* (IT Governance, 2025) dapat diperiksa pada Tabel 1 sebagai berikut.

Tabel 1. Jenis-jenis Ancaman Keamanan Siber

No	Jenis Ancaman	Pengertian Ancaman
1	*Backdoors*	Mengakses komputer lain tanpa sepengetahuan pemilik yang sah.
2	*Formjacking*	Memasukkan kode *malicious* JavaScript ke pembayaran *online* untuk memperoleh data pengguna kartu kredit.
3	*Distributed Denial of Service (DDos) Attacks*	Mengganggu lalu lintas *web*, *server,* atau jaringan yang menyebabkan *crash* pada sistem komputer.
4	*Domain Name System (DSN) Poisoning Attacks*	Mengalihkan akses pengguna ke situs yang telah ditetapkan oleh seseorang, sehingga pengguna tidak dapat mengakses situs tujuan.
5	*Malware*	*Software* semacam *Botnet, Ransomware, Spyware, Trojan, Virus, dan Worms* ditujukan untuk mengganggu atau merusak komputer lain.
6	*Drive-by Downloads*	Menginstal *malware* ke korban yang mengunjungi suatu *website malicious*. Biasanya memanfaatkan lampiran email atau tautan sebuah *website*.
7	*Man in the Middle (MITM) Attacks*	*Hacker* masuk dalam jaringan perangkat dan *server* untuk mengintersepsi komunikasi, biasanya terjadi pada *wi-fi* publik yang tidak aman.

No	Jenis Ancaman	Pengertian Ancaman
8	*Phishing Attacks*	Metode rekayasa sosial untuk membocorkan informasi rahasia, sering kali dilakukan melalui email.
9	*Social Engineering*	Metode manipulasi korban dengan tujuan mendapatkan informasi atau melakukan akses ke komputer korban.
10	*Structured Query Language (SQL) Injection*	Memasukkan kode *malicious* ke dalam *server* SQL, hingga didapatkan akses untuk melakukan modifikasi data.

Jenis-jenis ancaman tersebut di atas dapat dilakukan oleh beragam aktor, dari aktor negara sampai *hacker* (Imperva, 2025). Dalam kajian keamanan siber, aktor-aktor yang berpotensi menjadi sumber ancaman keamanan siber dapat diperiksa pada Tabel 2 berikut ini.

Tabel 2. Sumber Ancaman Keamanan Siber

No	Sumber Ancaman	Penjelasan
1	Negara	Negara musuh yang mampu melancarkan serangan siber terhadap perusahaan atau institusi lokal, tujuannya untuk mengintervensi komunikasi, menyebabkan kekacauan, dan menimbulkan kerusakan.
2	Organisasi Teroris	Aksi terorisme dengan metode serangan siber, tujuannya untuk menghancurkan infrastruktur, mengancam keamanan nasional, disrupsi ekonomi, dan membahayakan masyarakat.
3	Kelompok Kriminal	Kelompok *hacker* terorganisir yang bertujuan menerobos sistem komputer lain untuk keuntungan ekonomi. Kelompok ini melakukan *spam*, *phishing*, menginstal *spyware* dan *malware*, mencuri informasi pribadi, dan melakukan *online scam*.

No	Sumber Ancaman	Penjelasan
4	*Hacker*	Peretas individual yang menargetkan suatu organisasi melalui serangan yang variatif. Motivasinya adalah keuntungan personal, balas dendam, keuntungan finansial, atau aktivitas politik. Mereka biasanya selalu mengembangkan jenis ancaman baru untuk meningkatkan kredibilitasnya di antara komunitas peretas.
5	*Malicious Insider*	Merupakan 'orang dalam' yang memiliki akses jaringan perusahaan dan melakukan penyalah-gunaan kewenangan untuk mencuri informasi atau merusak sistem komputer. Biasanya pegawai, kontraktor, *supplier* perusahaan, dan pendukung organisasi kriminal.

Permasalahan Keamanan Siber di Indonesia

Ancaman serius keamanan siber di Indonesia terjadi dalam berbagai insiden di beberapa tahun belakangan ini, yaitu: peretasan data pelanggan Citilink dan tiket.com (2016), peretasan dan pembobolan data pengguna Tokopedia (2020), peretasan akun *youtube* DPR RI (2023), serangan *ramsomware* Pusat Data Nasional (PDN) (2024), peretasan dan pembobolan data NPWP oleh Bjorka (2024), dan kebocoran data di Satu Data ASN (2024). Kasus-kasus tersebut tentu saja menimbulkan kerugian tidak sedikit. Pada kasus serangan *ransomware* terhadap Pusat Data Nasional (Aldiansyah, 2025), misalnya, selain sebagian data dapat di kuasai peretas, muncul ancaman peretas untuk menyebarkan data yang telah dikuasainya itu. Saat itu, peretas meminta tebusan sebesar 8 juta dolar AS jika pemerintah ingin mendapatkan kunci deskripsi atas data yang dikuasainya.

Sebelum kasus Pusat Data Nasional (PDN), peretas yang menamakan dirinya Bjorka meretas data NPWP dari Direktorat Jenderal

Pajak Indonesia dan menjualnya di pasar gelap. Penyelidikan kasus itu dilakukan Kepolisian Republik Indonesia (Polri) bersama dengan Badan Siber dan Sandi Negara Republik Indonesia (BSSN RI) (Fadilah, 2025). Kasus lainnya yang perlu diperhatikan adalah kasus kebocoran Satu Data ASN yang dikelola oleh Badan Kepegawaian Negara (BKN). Melalui siaran pers, BKN memang menyatakan bahwa dugaan kebocoran data ASN dipastikan tidak mengganggu layanan manajemen ASN, tetapi kerugian non-finansial yang ditanggungnya tak bisa dianggap ringan. Akhirnya, BKN harus bekerja sama dengan BSSN dan Kementerian Komunikasi dan Informatika (saat ini disebut Komdigi) untuk melakukan investigasi di kasus tersebut (BKN, 2024).

Atas kasus-kasus tersebut di atas, Lembaga Studi dan Advokasi Masyarakat (ELSAM) menyajikan analisisnya terkait kerentanan data pemerintah terhadap ancaman keamanan siber (ELSAM, 2014), yaitu: (1) kebocoran data yang terus terjadi diakibatkan karena tingkat kepatuhan pelindungan data yang rendah pada lembaga-lembaga negara; (2) pemerintah tidak belajar dari berbagai insiden yang pernah terjadi sebelumnya dengan tidak pernah adanya penyelesaian tuntas terhadap setiap insiden yang pernah terjadi; (3) belum adanya perbaikan sistemik dan sistematis terkait permasalahan yang konsisten ditemukan dalam pelaksanaan audit keamanan, keandalan sistem pemrosesan, dan penyimpanan data.

Data lain dari Unit Patroli Siber Kepolisian Republik Indonesia (Polri) juga menunjukkan situasi yang cukup memprihatinkan. Unit Patroli Siber Polri menyediakan suatu kanal bagi masyarakat untuk menyampaikan laporan terkait kejahatan siber yang dialaminya. Dari data yang disajikan pada *website* unit tersebut, diketahui berbagai jenis kasus kejahatan siber yang dilaporkan (Unit Patroli Siber, 2025), yaitu berupa: 14.495 kasus penipuan *online*, 8.614 ancaman kekerasan, 6.556 pencemaran nama baik, 3.675 ancaman pencemaran (*doxxing*, pemerasan), 952 pornografi, 778 berita bohong, 597 manipulasi data (pemalsuan identitas, pemalsuan data, perusakan situs web, dan lain-lain), 220 judi *online* (judol), dan 237 prostitusi.

Dari berbagai permasalahan di atas, kerentanan keamanan siber di Indonesia ternyata sangat mengkhawatirkan, baik di institusi-institusi pemerintahan (sektor publik) maupun sektor swasta. Kenyataan ini menuntut pentingnya pengadaan tata kelola keamanan siber yang didasarkan pada suatu kerangka kerja kebijakan siber yang komprehensif, efektif, namun tetap mempertimbangkan aspek demokratis. Pertimbangan aspek demokratis diletakkan pada partisipasi pemangku kepentingan yang luas dan akuntabilitas dalam menjalankan pengawasan terhadap implementasi strategi dan kebijakan keamanan siber. Tentunya, upaya untuk membangun literasi digital bagi masyarakat luas tidak diabaikan.

Membangun Tata Kelola Keamanan Siber yang Memadai dan Demokratis

Kebutuhan untuk menyusun tata kelola keamanan Siber yang memadai dan demokratis di Indonesia menjadi suatu kebutuhan yang bersifat imperatif. Pengelolaan keamanan siber nasional sebenarnya dapat dilihat dari berbagai peraturan yang telah diberlakukan pemerintah seperti Undang-Undang (UU) Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP), Peraturan Presiden (Pepres) Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN), Kitab Undang-Undang Hukum Pidana (KUHP), dan Peraturan Menteri Pertahanan (Permenhan) Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber.

Meskipun sudah diberlakukan berbagai peraturan, keseluruhan peraturan tersebut masih tersebar di berbagai sektor. Kebutuhan saat ini adalah membangun pengelolaan keamanan siber yang terintegrasi. Pada konteks ini, partisipasi berbagai pemangku kepentingan keamanan siber, baik sektor publik maupun swasta, menjadi sangat penting karena ancaman keamanan siber tidak bersifat *state-centric*. Ancaman keamanan siber di Indonesia memiliki spektrum yang luas

dan ancamannya tidak selalu dapat dihadapi oleh negara. Berbagai jenis ancaman keamanan siber membutuhkan kerja sama atau kolaborasi yang kuat di antara lembaga negara dengan aktor-aktor non negara dalam rangka menciptakan keamanan siber yang memadai.

Di Indonesia, terdapat sedikitnya enam aktor utama yang memiliki pengaruh besar dalam diskursus keamanan siber (Wamala, 2011). *Pertama*, aktor eksekutif. Dalam hal ini, pemerintah sebagai eksekutif memiliki kewajiban untuk menyusun agenda keamanan nasional, termasuk keamanan siber. Eksekutif berkewajiban menjalankan fungsinya sebagai regulator, pengelola sumber daya, dan pembangun mekanisme kerja sama inter-agensi. *Kedua,* aktor legislatif. Aktor legislatif memainkan peranan penting dalam menyediakan instrumen hukum bagi pelaksanaan regulasi keamanan siber. *Ketiga,* operator dan pemilik infrastruktur penting di ruang siber. Para operator siber/internet dan para pemilik infrastruktur penting di ruang siber, seperti pengelola jaringan listrik, transportasi, dan layanan kesehatan, memiliki kepentingan terhadap terciptanya ekosistem siber yang kondusif. *Keempat,* lembaga peradilan. Lembaga peradilan memainkan peran yang penting sebagai lembaga yang memastikan tegaknya keadilan dari berlakunya seluruh peraturan perundang-undangan negara yang mengatur ketentuan keamanan siber. *Kelima,* penegak hukum. Penegak hukum menjadi elemen penting dalam memastikan penegakan hukum sesuai dengan peraturan perundang-undangan yang mengatur keamanan siber. *Keenam,* komunitas intelijen. Komunitas intelijen memainkan peranan penting dalam melakukan *monitoring* jaringan telekomunikasi, perbantuan kriptografi atau kriptoanalisis.

Jadi, aktor-aktor yang berpengaruh dalam diskursus keamanan siber cukup beragam, semuanya harus dilibatkan dalam penyusunan kebijakan dan strategi keamanan siber agar tercipta ekosistem keamanan siber yang memadai. Kemitraan menjadi kunci penting dalam membangun ekosistem siber yang baik. Kemitraan antara pemerintah dan sektor swasta dipandang penting dan menentukan karena beberapa pertimbangan. *Pertama,* skala ancaman siber sangat

luas spektrumnya, mulai dari sektor pemerintahan hingga sektor swasta yang mengelola infrastruktur penting (transportasi, elektrifikasi, kesehatan, dan perbankan). *Kedua,* kebutuhan untuk pertukaran informasi intelijen sebagai upaya *early warning system* yang sangat menentukan dalam menanggulangi ancaman keamanan siber. *Ketiga,* kebutuhan koordinasi untuk melakukan respon cepat atas insiden dan pemulihan cepat atas ancaman keamanan siber. *Keempat,* kebutuhan kolaborasi untuk meningkatkan kapasitas, edukasi, dan literasi siber kepada masyarakat.

Contoh model kemitraan strategis antara pemerintah dan aktor-aktor swasta dalam menanggulangi ancaman keamanan siber dapat dilihat dari regulasi yang dikembangkan oleh Uni Eropa (UE), yaitu *European Union Cybersecurity Act* (*EU Regulation*) *2019/881* (EU, 2025). Pasal 3 dalam *EU Regulation 2019/881* disebutkan bahwa Badan Keamanan Siber Uni Eropa atau *European Union Agency for Cybersecurity* (ENISA) bertugas untuk memfasilitasi kerja sama pembentukan komunitas keamanan siber antara komunitas sektor publik dan swasta. Pada Pasal 4(3), ENISA diberikan mandat untuk mempromosikan keterlibatan semua pemangku kepentingan (*stakeholders*), termasuk sektor industri, dalam mendukung kebijakan sertifikasi. Sedangkan pada Pasal 8, ENISA diberikan mandat untuk mendorong kerja sama teknis antara *Computer Security Incident Response Teams (CSIRTs)* dan pelaku sektor swasta dalam penanganan insiden keamanan siber. Dalam hal standar penjaminan dan pengelolaan keamanan siber, Pasal 47 menjelaskan bahwa keterlibatan publik dan swasta dijamin dalam pengembangan skema sertifikasi keamanan produk, layanan, dan proses digital.

Model kemitraan lain yang melibatkan multi pemangku kepentingan dapat juga dilihat pada model yang dikembangkan Jepang melalui *The Basic Act on Cybersecurity* 2014 (*Act no. 104 of November 12, 2014*) (Justice, 2025). Pasal 17 (2) dari undang-undang tersebut menjelaskan tentang mandat pembentukan Dewan Keamanan Siber di Jepang. Di situ Kepala Kantor Pusat Keamanan Siber Strategis (*Cybersecurity Strategic Headquarters*) ditugaskan untuk membentuk

Dewan Keamanan Siber Jepang yang beranggotakan: Kepala Kantor Pusat Keamanan Siber Strategis, pemerintahan lokal, penyedia jasa infrastruktur sosial yang penting, entitas bisnis terkait ruang siber, universitas, organisasi pendidikan dan riset, dan orang-orang lainnya yang dipandang perlu oleh Kepala Kantor Pusat Keamanan Siber Strategis. Selain itu, Pasal 17 (3) menjelaskan bahwa Dewan Keamanan Siber dapat meminta berbagai materi, opini, penjelasan, atau melakukan kerja sama dalam rangka meningkatkan kebijakan keamanan siber.

Di Indonesia, upaya untuk menciptakan kerangka regulasi tentang keamanan siber telah dimulai sejak 2019, namun pembahasannya kemudian terhenti. Kerangka regulasi itu dinamakan Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) (DPR-RI, 2019). Dalam naskah RUU tersebut, partisipasi luas pemangku kepentingan keamanan siber tidak dijelaskan secara eksplisit. Pasal 9(2) dan pasal 4(3) dalam RUU KKS memang memberikan penugasan kepada Badan Siber dan Sandi Negara (BSSN) untuk mengonsolidasikan koordinasi dan kolaborasi dalam penyelenggaraan keamanan dan ketahanan siber. Namun di situ tidak disebutkan pemangku kepentingan mana saja yang perlu dilibatkan dalam kolaborasi dan koordinasi penyelenggaraan keamanan siber. Muncul kesan bahwa RUU KKS menitikberatkan pada kepentingan yang sifatnya negara-sentris. Tidak ada pengaturan yang jelas tentang kolaborasi sektor publik dan swasta, terutama identifikasi aktor-aktor yang perlu dilibatkan dalam penyelenggaraan keamanan siber.

Hal lain yang tidak dapat dipisahkan dari penataan keamanan siber yang demokratis adalah pengawasan tata kelola. Pengawasan tata kelola keamanan siber penting dilakukan karena beberapa alasan. *Pertama,* pengawasan dibutuhkan untuk memastikan bahwa pengelolaan keamanan siber oleh para pemangku kepentingan telah dilaksanakan sesuai dengan prinsip demokratis, yaitu transparansi dan akuntabilitas kepada publik. *Kedua,* pengawasan publik secara demokratis penting karena dapat meningkatkan kualitas kebijakan dan sekaligus menjadi sarana untuk mendapatkan legitimasi yang kuat dari

publik (Stapenhurst, 2006). *Ketiga,* pengawasan berfungsi untuk memastikan prinsip *check and balances* dapat terlaksana, sehingga penyalahgunaan wewenang dapat dicegah (EU, 2011). Jika pengelolaan keamanan siber diselenggarakan dengan baik berdasarkan prinsip *check and balances*, cabang-cabang kekuasaan politik tidak hanya menjadi domain kekuasaan politik tertentu. *Keempat,* pengawasan penting untuk efektifnya penegakan hukum. Prinsip penegakan hukum dalam pengelolaan keamanan siber menjamin terlaksananya tatanan hukum untuk melindungi masyarakat dari ancaman keamanan siber.

Dalam pengaturan tata kelola siber di Uni Eropa, model pengawasan dalam tata kelola keamanan siber dapat dilihat dari norma-norma yang terdapat dalam *EU Cybersecuirty Act 2019* (EU, 2025). Model pengawasan yang diterapkan tercermin pada pasal-pasal yang mengatur peran Dewan Manajemen dalam memastikan fungsi direktifnya pada ENISA. Pasal 14(1) menyatakan bahwa Dewan Manajemen dibentuk berdasarkan komposisi satu anggota untuk masing-masing negara anggota Uni Eropa dan dua anggota ditunjuk komisi Eropa. Untuk menjalankan fungsinya, Pasal 15(1a) menyebutkan bahwa Dewan Manajemen memiliki kewenangan untuk menyusun petunjuk umum bagi penyelenggaraan operasional ENISA dan memastikan ENISA menyelenggarakan keamanan siber sesuai dengan aturan dan prinsip-prinsip yang terkandung dalam *EU Cybersecurity Act 2019*. Selanjutnya pada pasal 15(1d), Dewan Manajemen juga memiliki kewenangan untuk melakukan supervisi terhadap program tahunan atau multi tahun.

Pada model yang diterapkan di Jepang, pengawasan dilakukan Dewan Keamanan Siber Jepang untuk memastikan penyelenggaraan keamanan siber oleh Kantor Pusat Keamanan Siber Strategis Jepang. Pasal 3(1) di *The Basic Act on Cybersecurity* 2014 menyatakan bahwa penyelenggaraan keamanan siber di Jepang dilakukan melalui koordinasi berbagai aktor, yaitu aktor nasional, aktor lokal, hingga penyedia infrastruktur sosial (Justice, 2025). Berdasarkan pasal itu, aktor-aktor penyelenggara keamanan siber dapat melakukan *check and balances*, terutama aktor non-pemerintah yang disebutkan

sebagai penyedia infrastruktur sosial dan entitas bisnis. Bahkan pasal 7 menyatakan bahwa entitas bisnis diharapkan dapat memastikan keamanan siber secara independen dan proaktif, meskipun harus tetap mengacu pada kebijakan keamanan siber nasional Jepang.

Di Indonesia, perihal pengawasan dalam RUU Keamanan dan Ketahanan Siber belum mengakomodir model pengawasan yang demokratis. Pasal 19 RUU tersebut memang seolah-olah telah memberikan peluang untuk sistem *check and balances* dengan pemberlakuan koordinasi dan kolaborasi (DPR-RI, 2019). Namun model koordinasi dan kolaborasi yang dimaksud belum memadai untuk *check and balances*, karena tidak ada kejelasan tentang aktor-aktor yang akan dilibatkan dan model pengawasan yang akan dilakukan. Norma yang ada di RUU ini menempatkan BSSN sebagai lembaga yang bertugas untuk mengonsolidasikan koordinasi dan kolaborasi, namun tidak menyebutkan jenis sektor atau aktor-aktor pemangku kepentingan mana saja yang akan melakukan koordinasi dan kolaborasi. Ketidakjelasan ini berpotensi memberikan kewenangan penuh dan terpusat kepada BSSN sebagai satu-satunya aktor yang sifatnya eksklusif, sehingga pada akhirnya berpotensi menghambat efektivitas koordinasi dan kolaborasi. Dengan demikian, memastikan pengawasan yang demokratis melalui mekanisme *check and balances* tidak boleh luput dalam penyusunan kerangka regulasi keamanan siber di Indonesia.

Penutup

Indonesia yang tengah berada dalam transformasi digital yang pesat membutuhkan penataan tata kelola keamanan siber. Hal ini perlu dipastikan untuk membangun ekosistem keamanan siber yang kondusif. Dalam diskursus keamanan siber, ekosistem yang kondusif dapat dibangun dengan cara mengedepankan prinsip-prinsip demokratis yang terkandung dalam pemenuhan dua syarat penting. *Pertama,* memastikan adanya keterlibatan luas para pemangku kepentingan keamanan siber, tidak hanya terbatas pada aktor negara (Pemerintah Pusat), namun juga entitas bisnis hingga penyedia

infrastruktur sosial penting yang diharapkan dapat terlibat secara aktif. *Kedua,* memastikan bahwa penyelenggaraan keamanan siber dapat diawasi dengan baik sesuai dengan prinsip pengawasan demokratis. Artinya, mekanisme *check and balances* berlangsung dengan baik sehingga akuntabilitas, transparansi, dan penghindaran terhadap penyalahgunaan wewenang sungguh-sungguh terwujud.

Daftar Pustaka

Aldiansyah, F. (2025, April 2). *Netmarks Indonesia*. diakses dari netmarks.co.id: https://www.netmarks.co.id/post/serangan-siber-terbesar-yang-pernah-terjadi-di-indonesia

BKN. (2024, Agustus 11). BKN Pastikan Dugaan Kebocoran Data ASN Tidak Mengganggu Layanan Manajemen ASN. *Siaran Pers*

DPR-RI. (2019). Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber. *Legislasi*

ELSAM. (2014, Agustus 13). Kebocoran Data Publik Terus Terjadi, Kepatuhan Institusi Pemerintah terhadap UU PDP Minim. *Siaran Pers*

EU. (2011). *Concepts and Principles of Democratic Governance and Accountability*. Kampala: Konrad-Adenauer-Stiftung

EU. (2025, April 8). *European Union*. diakses dari EU Website: https://eur-lex.europa.eu/eli/reg/2019/881/oj

Fadilah, K. (2025, April 3). *detikNews*. diakses dari detik Web site: https://news.detik.com/berita/d-7556022/bareskrim-koordinasi-dengan-bssn-usut-dugaan-kebocoran-data-npwp

Fisher, E. A. (2005). Creating National Framework for Cybersecurity: An Anlysis of Issues and Options. *CSR Report for Congress*, 6

Hervianty, M. (2025, March 29). *RRI*. diakses dari rri.co.id: https://rri.co.id/index.php/iptek/769749/tantangan-dibalik-peningkatan-indeks-literasi-digital-di-indonesia

Imperva. (2025, April 2). *Imperva Company*. diakses dari Imperva Web Site: https://www.imperva.com/learn/application-security/cyber-security-threats/#:~:text=Nation%20states%E2%80%94hostile%20countries%20can,private%20information%2C%20and%20online%20scams

IT Governance. (2025, April 2). *IT Governance*. diakses dari from itgovernance.co.uk: https://www.itgovernance.co.uk/cyber-threats

Ministry of Justice of Japan. (2025, April 14). *Japanese Law Translation*. diakses dari Japanese Law Translation Web Site: https://www.japaneselawtranslation.go.jp/en/laws/view/4755

Newton, M. H. (2015). Supplemental Information for The Interagency Report on Strategic U.S Government Engagement in Internatoinal Standardization to Achieve US Objectives for Cyber Security. *National Institute of Standards and Technology Report*, 41

Nissenbaum, L. H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quaterly*, 1155-1175

Rainer, P. (2025, March 3). *Goodstats*. diakses dari goodstats.id: https://goodstats.id/article/inilah-media-sosial-paling-sering-dipakai-di-indonesia-Pdyt0

Reveron, D. S. (2012). *Cyberspace and National Security: Threats, Opportunities, amd Power in a Virtual World*. Washington: Georgetown University Press

Santika, E. F. (2025, March 28). *databoks*. diakses dari katadata.co.id: https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/e6f9d69e252de32/tingkat-penetrasi-internet-indonesia-capai-795-per-2024

Stapenhurst, R. R. (2006). Democracy and Oversight. *Research Collection School of Social Sciences*, 1-25

Unit Patroli Siber. (2025, April 2). *Polri*. diakses dari patrolisiber.id: https://patrolisiber.id/statistic/

Wamala, F. (2011). *ITU National Cybersecurity Strategy Guide*. Geneva: ITU

Yonatan, A. Z. (2025, March 3). *Goodstats*. diakses dari goodstats web site: https://data.goodstats.id/statistic/makin-maju-pertumbuhan-e-commerce-indonesia-yang-diprediksi-tertinggi-di-dunia-QiN5h