Memperkuat Ketahanan Keamanan Siber Nasional: Antisipasi Serangan Siber Global Yang Terus Meningkat

Oleh: Yappi Manafe
Mantan Kepala Biro Prencanaan, Mantan Kepala Biro Hukum,
Kementerian KOMINFO

Pengantar

Isu ***"keamanan siber" ("cybersecurity")*** bukanlah fenomena yang baru muncul pada dekade 1990-an. Ancaman berupa virus dan *worm* telah menjadi bagian dari dinamika ruang siber ("*cyberspace*") sejak tahap awal perkembangannya. Sebagai contoh, film *WarGames* (1983) menggambarkan seorang remaja yang berhasil meretas sistem komputer yang mengendalikan komando dan kendali persenjataan nuklir Amerika Serikat. Selain itu, insiden *The Cuckoo's Egg* pada pertengahan 1980-an meningkatkan kesadaran internasional bahwa mata-mata asing telah memanfaatkan jaringan komputer sebagai sarana untuk memperoleh informasi rahasia dengan tingkat klasifikasi tinggi. Berbagai peristiwa tersebut menunjukkan bahwa ancaman terhadap sistem informasi telah muncul jauh sebelum Internet berkembang secara masif seperti saat ini.

Perubahan yang paling signifikan justru terletak pada perkembangan lingkungan teknologi informasi. Sejak awal dekade 1990-an, teknologi informasi mengalami transformasi dari penggunaan sistem komputer yang relatif sederhana dan berdiri sendiri ("*stand-alone systems*") dalam jaringan tertutup menjadi ekosistem digital yang terhubung melalui Internet dan berbagai jaringan komunikasi lainnya. Perkembangan tersebut memungkinkan terjalinnya konektivitas yang semakin luas antara pemerintah, dunia usaha, masyarakat, serta berbagai organisasi di seluruh dunia. Di samping itu, perangkat akses informasi juga berkembang pesat, tidak lagi terbatas pada komputer pribadi, tetapi mencakup berbagai perangkat portabel dan teknologi nirkabel. Peningkatan skala penggunaan teknologi tersebut turut diikuti oleh meningkatnya ancaman siber.

Selain peningkatan jumlah insiden, ancaman siber juga mengalami perubahan secara kualitatif. Perubahan tersebut berkaitan dengan semakin seriusnya dampak yang ditimbulkan terhadap keamanan nasional dan stabilitas masyarakat. Sejak pertengahan dekade 1990-an, isu keamanan siber memperoleh perhatian besar dalam agenda keamanan internasional karena mulai dikaitkan dengan ancaman terorisme dan perlindungan terhadap infrastruktur kritis **("*critical infrastructure protection*").** Pada periode tersebut dipahami bahwa berbagai sektor strategis dalam masyarakat modern—termasuk sektor yang berperan penting bagi keamanan nasional dan keberlangsungan perekonomian—bergantung pada sistem pengendalian berbasis perangkat lunak yang saling terhubung, baik pada tingkat nasional maupun internasional.

Infrastruktur informasi kritis **("*Critical Information Infrastructure/CII*")** menjadi fondasi utama bagi berbagai infrastruktur kritis, karena teknologi informasi dan komunikasi **("*Information and Communication Technology/ICT*")** telah terintegrasi ke dalam hampir seluruh sektor kehidupan. Akibatnya, berbagai sistem infrastruktur menjadi semakin saling bergantung ("*interdependen"t*), sehingga gangguan terhadap satu sistem berpotensi menimbulkan dampak berantai terhadap sektor-sektor strategis lainnya. Dengan demikian, keamanan siber tidak lagi dipandang semata-mata sebagai persoalan teknis, melainkan telah berkembang menjadi isu strategis yang berkaitan erat dengan ketahanan nasional, stabilitas ekonomi, serta keamanan masyarakat secara keseluruhan.

Meningkatnya kekhawatiran terhadap kerentanan masyarakat yang bergantung pada jaringan digital, disertai dengan semakin banyaknya gangguan di ranah siber, telah mendorong berbagai negara untuk memahami secara lebih mendalam kerentanan dan ancaman terhadap infrastruktur (informasi) mereka, sekaligus merumuskan berbagai langkah perlindungan terhadap aset-aset tersebut. Dalam kaitan ini, Pemerintah di perlu mempelajari praktik terbaik ("*best practices*") penangan keamanan siber di berbagai negara, serta berbagai permasalahan dan tantangan yang dihadapi dalam upaya membangun, memperkuat dan mewujudkan budaya keamanan siber nasional yang andal.

Pengertian: ***Cyber, Cybernetics, Cyberspace, Cyber Security, dan Cyber Resilience***

"Cyber/Siber" merupakan kata sifat (adjective) atau awalan (prefix) yang merujuk pada segala sesuatu yang berkaitan dengan komputer, jaringan elektronik, dan internet. Istilah ini berasal dari kata ***"Cybernetics"***, yaitu ilmu yang mempelajari komunikasi serta sistem pengendalian otomatis, yang dipelopori oleh ahli matematika Nobert Wiener 1948 melalui bukunya, "*Cybernetics Or Control and Communication in the Animal and the Machine*". Dalam perkembangannya, istilah "*Cyber"* kini lebih banyak digunakan untuk menggambarkan teknologi digital, sistem informasi berbasis komputer, dan lingkungan virtual. Menurut Merriam-Webster**,** istilah "*Cyber"* digunakan sebagai awalan yang menunjukkan hubungan dengan komputer, teknologi informasi, jaringan digital, atau internet. Istilah "*Cyber"* kemudian mengkait dengan istilah ***"Cyberspace"*** yang dipolerkan pertama kali oleh William Gibson dalam novel "*Neuromancer"* melalui deskripsi berikut:

"*Cyberspace adalah sebuah halusinasi konsensual yang dialami setiap hari oleh miliaran pengguna sah di seluruh dunia, termasuk anak-anak yang sedang mempelajari konsep-konsep matematika. Cyberspace merupakan representasi grafis dari data yang diabstraksikan dari bank-bank data pada setiap komputer dalam sistem manusia. Kompleksitasnya tidak terbayangkan, berupa garis-garis cahaya yang membentang dalam ruang nonfisik pikiran, membentuk gugusan dan konstelasi data layaknya cahaya kota yang terlihat menjauh.*"

Definisi tersebut menggambarkan **"***Cyberspace"* sebagai suatu ruang virtual yang terbentuk dari keterhubungan berbagai sistem komputer dan jaringan digital. Meskipun awalnya merupakan konsep fiksi ilmiah, istilah ini kemudian berkembang menjadi konsep yang digunakan dalam kajian teknologi informasi, keamanan siber, dan hukum siber untuk menjelaskan lingkungan digital tempat berlangsungnya komunikasi, pertukaran informasi, serta berbagai aktivitas elektronik.

Istilah **"***Cyber"* telah digunakan untuk menggambarkan hampir segala hal yang berkaitan dengan jaringan komputer dan sistem komputasi, khususnya dalam bidang keamanan. Seiring dengan perkembangannya, muncul pula bidang kajian baru yang berfokus pada konflik di ruang siber ("*cyberspace"*), seperti perang siber ("*cyber warfare"*) antarnegara, terorisme siber ("*cyber terrorism"*), milisi siber ("*cyber militias"*), dan berbagai bentuk konflik digital lainnya. Namun demikian, hingga saat ini belum terdapat konsensus mengenai definisi **"***Cyberspace"***,** apalagi mengenai implikasi yang ditimbulkan oleh konflik yang terjadi di dalamnya. Untuk memberikan kejelasan terhadap permasalahan tersebut, para penulis mengajukan definisi bahwa **"***Cyberspace"* merupakan sekumpulan sistem informasi yang saling terhubung dan bersifat dinamis berdasarkan waktu ("*time-dependent"*), beserta para pengguna yang berinteraksi dengan sistem tersebut

"*Cyber Security*" *("Keamanan Siber")*: Terdapat berbagai definisi mengenai keamanan siber **(***cyber security***)** yang telah diterima dan digunakan secara luas oleh organisasi internasional maupun lembaga yang bergerak di bidang keamanan informasi. Menurut International Organization for Standardization (ISO), keamanan siber atau keamanan ruang siber **("***cyberspace security"*) adalah upaya untuk menjaga kerahasiaan ("*confidentiality"*), integritas ("***integrity"***), dan ketersediaan ("***availability"***) informasi di dalam ruang siber ("***cyberspace"*****).** Selanjutnya, **"*ruang siber*" ("*cyberspace*")** didefinisikan sebagai lingkungan yang kompleks yang terbentuk dari interaksi antara manusia, perangkat lunak, dan berbagai layanan di internet melalui perangkat teknologi dan jaringan yang saling terhubung, serta "***tidak memiliki wujud fisik"***. Definisi ini menegaskan bahwa ruang siber merupakan suatu lingkungan virtual yang memungkinkan berlangsungnya komunikasi, pertukaran data, dan berbagai aktivitas digital. Committee on National Security Systems (CNSS-4009) mendefinisikan keamanan siber sebagai kemampuan untuk melindungi atau mempertahankan penggunaan ruang siber oleh suatu organisasi dari serangan yang dilakukan melalui **"*ruang siber*"**, dengan tujuan mencegah tindakan yang dapat mengganggu (*disrupting*), melumpuhkan (*disabling*), menghancurkan ("*destroying"*), atau mengendalikan secara tidak sah infrastruktur dan lingkungan komputasi. Keamanan siber merupakan proses melindungi informasi melalui upaya pencegahan, pendeteksian, dan pemberian respons terhadap serangan siber. Keamanan siber bukan hanya berkaitan dengan penggunaan teknologi untuk mencegah ancaman, tetapi juga mencakup kemampuan mendeteksi insiden keamanan serta melakukan respons yang efektif untuk meminimalkan dampak yang ditimbulkan.

Secara konseptual, "**keamanan siber" ("*cybersecurity*")** merupakan segala upaya yang bertujuan menciptakan ruang siber ("*cyberspace*") yang aman dari berbagai ancaman siber ("*cyber threats*"). Ancaman siber sendiri merujuk pada penggunaan teknologi informasi dan komunikasi ("*Information and Communication Technology/ICT*") secara sengaja untuk melakukan tindakan yang merugikan, baik dengan menjadikan sistem informasi sebagai sasaran serangan maupun sebagai sarana untuk melancarkan serangan tersebut. Ancaman tersebut dapat berasal dari berbagai aktor, seperti individu, kelompok kriminal, organisasi teroris, hingga negara. Dalam pengertian yang umum digunakan, *cybersecurity* mencakup tiga dimensi utama. Pertama, seperangkat aktivitas dan tindakan, baik yang bersifat teknis maupun nonteknis, yang bertujuan melindungi komputer, jaringan komputer, perangkat keras, perangkat lunak, data, serta seluruh elemen ruang siber dari berbagai ancaman, termasuk ancaman terhadap keamanan nasional. Kedua, tingkat perlindungan yang dihasilkan dari penerapan berbagai aktivitas dan tindakan tersebut. Ketiga, bidang keahlian profesional yang meliputi penelitian, pengembangan, analisis, serta implementasi berbagai strategi untuk meningkatkan efektivitas perlindungan keamanan siber.

Seiring dengan pesatnya perkembangan teknologi informasi yang menciptakan berbagai peluang baru, selalu terdapat pihak-pihak yang berupaya memanfaatkan kemajuan tersebut untuk kepentingan yang melanggar hukum, seperti pencurian informasi, pencurian dana, penyalahgunaan sistem komputer, maupun serangan terhadap organisasi lain. Oleh karena itu, tujuan utama keamanan siber adalah memberikan perlindungan terhadap organisasi, sistem informasi, dan aset digital dari berbagai ancaman yang dapat merugikan bisnis, mencuri data atau aset keuangan, maupun mengeksploitasi sistem komputer untuk melakukan serangan terhadap pihak lain. Menurut ITU (International Telecommunication Union)**:** keamanan siber ("*cybersecurity*") didefinisikan sebagai sekumpulan alat, kebijakan, konsep keamanan, mekanisme pengamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik ("*best practices*"), mekanisme penjaminan ("*assurance*"), serta teknologi yang digunakan untuk melindungi lingkungan siber ("*cyber environment*") beserta aset organisasi dan pengguna. Ruang lingkup keamanan siber tidak hanya mencakup perlindungan terhadap perangkat teknologi informasi, tetapi juga seluruh komponen yang mendukung operasional sistem informasi dan komunikasi digital. Keamanan siber bertujuan untuk menjamin tercapainya serta terpeliharanya karakteristik keamanan ("*security properties*") dari aset organisasi dan pengguna terhadap berbagai risiko keamanan yang muncul di lingkungan siber.

Untuk mencapai tujuan tersebut, keamanan siber berlandaskan pada tiga prinsip utama, yaitu:

- **Ketersediaan ("*Availability*")**, yaitu memastikan bahwa sistem, layanan, dan informasi dapat diakses serta digunakan oleh pihak yang berwenang pada saat diperlukan.

- **Integritas (“*Integrity*”)**, yaitu menjamin bahwa data dan sistem tetap utuh, akurat, serta tidak mengalami perubahan tanpa izin. Prinsip ini juga dapat mencakup **keaslian (“*Authenticity*”)**, yaitu jaminan bahwa identitas pengguna atau sumber informasi dapat diverifikasi, serta **anti-penyangkalan (“*Non-repudiation*”)**, yaitu jaminan bahwa pihak yang telah melakukan suatu tindakan atau transaksi tidak dapat menyangkal keterlibatannya.
- **Kerahasiaan (“*Confidentiality*”)**, yaitu memastikan bahwa informasi hanya dapat diakses oleh pihak yang memiliki hak atau kewenangan sehingga terlindungi dari akses, penggunaan, maupun pengungkapan yang tidak sah.

Ketahanan Siber (“*Cyber Resilience*”)

Ketahanan siber (*cyber resilience*) merupakan kemampuan suatu organisasi untuk mengantisipasi, mencegah, menghadapi, bertahan, merespons, serta memulihkan diri dari insiden keamanan siber (“*cybersecurity incidents*”) sehingga mampu mempertahankan keberlangsungan operasionalnya. Konsep ini tidak hanya menitik-beratkan pada perlindungan terhadap sistem informasi, tetapi juga pada kemampuan organisasi untuk tetap menjalankan fungsi-fungsi kritis dan mencapai tujuan operasional meskipun menghadapi gangguan atau serangan siber. Ketahanan siber mengintegrasikan tiga aspek utama, yaitu keberlangsungan bisnis (“*business continuity*”), keamanan sistem informasi (“*information systems security*”), dan ketahanan organisasi (“*organizational resilience*”). Integrasi ketiga aspek tersebut memungkinkan organisasi untuk tetap beroperasi secara efektif ketika menghadapi berbagai bentuk gangguan, seperti serangan siber (“*cyberattacks*”), bencana alam, maupun krisis ekonomi. Tingkat kematangan keamanan informasi serta ketahanan organisasi menjadi faktor yang sangat menentukan kemampuan organisasi dalam mempertahankan keberlangsungan layanan dengan gangguan seminimal mungkin, bahkan tanpa mengalami “*downtime*”. Perkembangan ancaman siber modern telah menghadirkan tantangan yang semakin kompleks sehingga pendekatan keamanan tradisional yang hanya berorientasi pada pencegahan tidak lagi memadai apabila diterapkan secara terpisah. Organisasi saat ini menghadapi pelaku ancaman (“*threat actors*”) yang semakin canggih dan memanfaatkan teknologi serta teknik serangan yang terus berkembang untuk mengganggu operasional. Selain mengeksploitasi kerentanan teknis pada sistem, pelaku serangan juga semakin sering memanfaatkan kelemahan manusia (“*human vulnerabilities*”) melalui berbagai teknik rekayasa sosial (“*social engineering*”), sehingga *“dimensi manusia menjadi salah satu titik kritis dalam keamanan siber modern”*. Ketahanan siber tidak hanya dimaknai sebagai kemampuan untuk mencegah terjadinya serangan siber, tetapi juga sebagai kapasitas organisasi untuk mengantisipasi risiko, mempertahankan keberlangsungan operasional, merespons insiden secara efektif, serta melakukan pemulihan dengan cepat setelah gangguan terjadi.

Ketahanan Siber menjadi salah satu elemen fundamental dalam tata kelola keamanan informasi modern karena didasarkan pada pemahaman bahwa tidak semua serangan dapat dicegah, tetapi dampaknya dapat diminimalkan melalui kesiapan organisasi, pengelolaan risiko yang baik, serta kemampuan adaptasi yang berkelanjutan.

Pentingnya Ketahanan Siber (*Cyber Resilience*)

Ketahanan siber ("*cyber resilience*") merupakan aspek yang sangat penting bagi setiap organisasi. Risiko siber saat ini termasuk dalam salah satu prioritas risiko tertinggi yang dihadapi organisasi, dan tingkat ancamannya terus mengalami peningkatan. Perkembangan ini menunjukkan bahwa ancaman siber bukan lagi sekadar isu teknis, melainkan telah menjadi risiko strategis yang dapat memengaruhi keberlangsungan organisasi. Tantangan keamanan siber juga bersifat dinamis. Transformasi lanskap digital dan infrastruktur teknologi, yang didorong oleh meningkatnya konektivitas serta munculnya berbagai teknologi baru, telah memperluas dan memperumit lanskap ancaman siber. Akibatnya, organisasi menghadapi risiko siber yang semakin kompleks dan sulit diprediksi. Di sisi lain, semakin disadari bahwa individu maupun organisasi tidak mungkin mampu mencegah seluruh bentuk serangan siber ataupun kegagalan sistem. Kesadaran tersebut, yang diiringi dengan pemanfaatan peluang dari transformasi digital, mendorong berkembangnya konsep ketahanan siber sebagai pendekatan yang lebih komprehensif dalam mengelola risiko siber.

Transformasi digital yang berlangsung secara berkelanjutan terus mengubah cara organisasi, baik di sektor bisnis maupun pemerintahan, menjalankan aktivitasnya. Sebagian besar tujuan strategis organisasi saat ini didukung oleh proses bisnis yang sangat bergantung pada teknologi digital dan, dalam banyak kasus, tidak lagi memiliki alternatif non-digital. Meskipun tujuan setiap organisasi berbeda, secara umum seluruh organisasi berkepentingan untuk menjaga keberlangsungan layanan yang bersifat kritis, mempertahankan kepercayaan para pemangku kepentingan, serta melindungi aset-aset utama yang menjadi sumber nilai dan keunggulan kompetitifnya. Oleh karena itu, pencapaian ketahanan siber yang sesungguhnya merupakan isu kepemimpinan strategis ("*leadership issue*") yang sangat menentukan kemampuan organisasi dalam mempertahankan nilai ekonomi dan keberlanjutan usahanya. Setiap organisasi perlu mempersiapkan diri menghadapi kemungkinan terjadinya insiden siber yang signifikan. Investasi yang berkelanjutan dalam pengembangan kapabilitas ketahanan siber memungkinkan organisasi untuk tetap mencapai tujuan strategisnya meskipun menghadapi serangan siber maupun insiden keamanan siber lainnya. Upaya tersebut mencakup kemampuan untuk memulihkan operasional secara cepat, meminimalkan dampak terhadap pemangku kepentingan internal maupun eksternal, memulihkan kinerja keuangan dan aktivitas bisnis, melindungi aset berwujud maupun tidak berwujud, serta menciptakan peluang pertumbuhan baru setelah terjadinya insiden.

Untuk mewujudkan ketahanan siber yang efektif, organisasi perlu mengembangkan strategi yang adaptif serta memanfaatkan pengalaman dan pembelajaran dari organisasi lain dalam menghadapi berbagai ancaman siber. Kolaborasi yang proaktif, pertukaran informasi, serta pembelajaran yang berkelanjutan menjadi faktor penting dalam meningkatkan kemampuan organisasi untuk mengantisipasi, merespons, dan beradaptasi terhadap dinamika ancaman siber yang terus berkembang.

Seiring dengan pesatnya perkembangan teknologi dan meningkatnya ketergantungan terhadap ruang siber, pemahaman mengenai praktik keamanan siber juga mengalami perubahan yang signifikan. Jika pada awalnya keamanan siber lebih berfokus pada penerapan pengendalian keamanan dasar (*basic security controls*), saat ini perhatian organisasi telah bergeser menuju perlindungan informasi (*information security*), penjaminan keamanan (*information assurance*), serta penguatan ketahanan siber (*cyber resilience*). Pergeseran ini mencerminkan kesadaran bahwa dalam lingkungan digital yang terus berubah, organisasi harus beroperasi dengan asumsi bahwa insiden siber yang signifikan sewaktu-waktu dapat terjadi. Insiden siber modern tidak lagi hanya berdampak pada satu perangkat komputer atau sistem tertentu, tetapi berpotensi mengganggu keseluruhan operasional organisasi bahkan memberikan dampak yang luas terhadap masyarakat. Oleh karena itu, menjaga keberlangsungan operasional organisasi di tengah berbagai bentuk gangguan harus menjadi bagian yang tidak terpisahkan dari pembangunan ketahanan siber. Memiliki ketahanan siber yang baik, organisasi akan mampu meminimalkan dampak insiden siber terhadap tujuan dan sasaran strategisnya. Ketahanan siber memungkinkan organisasi untuk mempertahankan penyelenggaraan layanan yang bersifat kritis, menjaga kepercayaan para pemangku kepentingan, melindungi aset strategis, serta mempertahankan nilai ekonomi dan daya saing organisasi dalam jangka panjang. Ketahanan siber tidak lagi dipandang sebagai sekadar kemampuan teknis untuk mencegah serangan, melainkan sebagai kemampuan strategis organisasi untuk tetap beroperasi, beradaptasi, dan pulih secara efektif ketika menghadapi berbagai gangguan siber. Organisasi yang memiliki tingkat ketahanan siber yang tinggi akan lebih mampu memanfaatkan peluang digital untuk meningkatkan inovasi, produktivitas, dan pertumbuhan ekonomi. Oleh karena itu, pembangunan ketahanan siber tidak dapat lagi dipandang hanya sebagai tanggung jawab unit teknologi informasi, melainkan harus menjadi bagian dari strategi utama organisasi dalam mewujudkan transformasi digital yang berkelanjutan. Keberhasilan membangun ketahanan siber sangat bergantung pada peran kepemimpinan organisasi. Ketahanan siber tidak cukup hanya didukung oleh Tim Keamanan Siber yang kompeten, tetapi memerlukan budaya organisasi yang menempatkan keamanan siber sebagai pertimbangan utama dalam setiap pengambilan keputusan strategis. Para pemimpin organisasi harus secara aktif terlibat dalam penyusunan dan implementasi strategi keamanan siber dengan memahami bahwa keamanan siber merupakan fungsi bisnis yang sama pentingnya dengan aspek hukum, keuangan, maupun manajemen risiko, sehingga pengelolaan risiko operasional organisasi pada dasarnya selalu mencakup pengelolaan risiko siber.

Faktor-Faktor Pendorong Kesenjangan Ketahanan Siber (“*Drivers of Cyber Inequity*”) Di Tahun 2026

Kapasitas keamanan siber di tingkat global masih menunjukkan tingkat yang tidak merata di berbagai sektor industri maupun kawasan. Perbedaan tersebut dipengaruhi oleh variasi dalam ketersediaan sumber daya manusia yang memiliki kompetensi keamanan siber, kapasitas pendanaan, infrastruktur digital, serta kerangka tata kelola yang dimiliki oleh masing-masing organisasi maupun negara. Meskipun sebagian organisasi terus meningkatkan investasi di bidang keamanan siber, masih banyak organisasi lain yang menghadapi kesulitan untuk mempertahankan bahkan pada tingkat dasar (“*baseline*”) keamanan siber. Kondisi ketimpangan tersebut dikenal sebagai “**kesenjangan siber” (“*cyber inequity*”)**, yaitu keadaan ketika kemampuan suatu organisasi atau negara dalam membangun keamanan dan ketahanan siber berbeda secara signifikan dibandingkan dengan organisasi atau negara lainnya. Kesenjangan ini tidak hanya meningkatkan risiko terhadap organisasi yang memiliki kapasitas rendah, tetapi juga menciptakan kerentanan bagi seluruh ekosistem digital yang saling terhubung, terutama dalam rantai pasok (“*interconnected supply chains*”). Dengan demikian, kelemahan pada satu organisasi dapat menjadi pintu masuk yang berdampak terhadap organisasi lain yang memiliki hubungan operasional dengannya. Kesenjangan siber dapat dipahami melalui tiga dimensi utama. Pertama, perbedaan kapasitas keamanan siber antara organisasi berskala kecil dan organisasi berskala besar. Kedua, kesenjangan antara negara maju dan negara berkembang dalam membangun kemampuan keamanan siber. Ketiga, perbedaan tingkat kesiapan keamanan siber antar sektor, baik sektor publik, sektor swasta, maupun organisasi nirlaba. Data survei menunjukkan bahwa organisasi kecil, yang diukur berdasarkan tingkat pendapatan (“*revenue*”), memiliki kemungkinan dua kali lebih besar mengalami tingkat ketahanan siber yang tidak memadai dibandingkan organisasi berskala besar. Kondisi ini mengindikasikan bahwa keterbatasan sumber daya finansial, teknologi, dan tenaga ahli menjadi hambatan utama bagi organisasi kecil dalam membangun sistem keamanan siber yang memadai.

Secara keseluruhan, fenomena “*cyber inequity*” menunjukkan bahwa ketahanan siber global belum berkembang secara merata. Perbedaan kapasitas sumber daya, tingkat investasi, kualitas tata kelola, serta kematangan infrastruktur digital menyebabkan sebagian organisasi dan negara lebih rentan terhadap ancaman siber dibandingkan yang lain. Oleh karena itu, upaya memperkuat ketahanan siber tidak hanya memerlukan peningkatan kemampuan pada tingkat organisasi, tetapi juga memerlukan kolaborasi nasional dan internasional, pembangunan kapasitas sumber daya manusia, pemerataan akses terhadap teknologi keamanan siber, serta penguatan tata kelola keamanan informasi agar kesenjangan ketahanan siber dapat diminimalkan.

Regulasi Keamanan Siber Di Indonesia

Keamanan siber di Indonesia diatur dalam kerangka hukum utama: UU ITE (Informasi dan Transaksi Elektronik); UU PDP (Perlindungan Data Pribadi); serta regulasi teknis di bawah koordinasi Badan Siber dan Sandi Negara (BSSN), mencakup strategi nasional, pelindungan data, dan penindakan kejahatan siber.

Regulasi utama yang menjadi landasan keamanan siber di Indonesia antara lain:

- Undang-Undang tentang Informasi dan Transaksi Elektronik (UU ITE): UU No 11 Tahun 2008 yang telah direvisi menjadi UU No. 19 Tahun 2016**,** menjadi dasar hukum utama untuk mengkriminalisasi berbagai kejahatan siber seperti akses tanpa izin, intersepsi ilegal, peretasan, hingga penyebaran "*malware*".
- Undang-Undang tentang Pelindungan Data Pribadi (UU PDP): UU No. 27 Tahun 2022 mengatur kewajiban bagi seluruh Penyelenggara Sistem Elektronik (PSE) untuk melindungi data pribadi dan menerapkan sistem keamanan yang kuat, dengan sanksi administratif dan denda bagi pelanggar yang mengalami kebocoran data.
- Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE): Aturan ini mewajibkan setiap PSE untuk memastikan keandalan dan keamanan sistem elektronik mereka, serta melakukan pelaporan jika terjadi insiden atau gangguan siber.
- Peraturan Presiden No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber: Perpres ini menjadi payung kebijakan bagi pemerintah untuk mengoordinasikan langkah pertahanan negara terhadap ancaman siber dan menangani krisis keamanan siber nasional.
- Peraturan BSSN: Badan Siber dan Sandi Negara (BSSN) mengeluarkan berbagai regulasi teknis untuk mengelola ketahanan siber, seperti Peraturan BSSN No. 5 Tahun 2024 yang mengatur Manajemen Krisis Siber, serta pedoman keamanan informasi.

Perkembangan Kasus Kejahatan Siber Di Indonesia

Jumlah kasus *cyber crime* di Tanah Air terus meningkat sepanjang 2025. BSSN mencatat ada 5,5 miliar serangan siber, naik 714% dibandingkan dengan rata-rata tahunan 2020–2024. Tren berlanjut pada periode Januari–April 2026, telah terjadi 1,52 miliar serangan, menunjukkan eskalasi konsisten. Sasaran utamanya infrastruktur pemerintahan, sektor ekonomi, dan keamanan nasional. Metode serangan kian canggih, sehingga tidak hanya mengancam keamanan data, tetapi juga berpotensi mengguncang stabilitas ekonomi nasional. Indonesia saat ini tengah dalam keadaan mendesak keamanan dunia maya (cyber-security), karena melihat kenyataan bahwa tingkat kejahatan di dunia maya (cybercrime) di Indonesia telah mencapai tahap memprihatinkan.

Berbeda dengan penanganan kejahatan lainnya, cyber-security membutuhkan pemikiran yang komprehensif untuk menanganinya. Ancaman siber mencakup semua jenis serangan digital yang bertujuan mencuri data, mengganggu operasi, atau merusak sistem teknologi. Di Indonesia, ancaman ini berkembang seiring dengan pesatnya digitalisasi di berbagai sektor. Menurut BSSN, serangan siber di Indonesia meningkat 200% dalam 3 tahun terakhir. Jenisnya beragam, mulai dari phishing, malware, hingga ransomware yang semakin canggih. Tiga faktor utama yang membuat ancaman siber menjadi sorotan global:

- Pertumbuhan Ekonomi Digital yang Pesat:
  Nilai ekonomi digital Indonesia diprediksi mencapai $130 miliar pada 2025 (Google dan Temasek) membuat negara ini menjadi target empuk bagi pelaku kejahatan siber.
- Rendahnya Kesadaran Keamanan Siber:
  Data ID-SIRTII menunjukkan hanya 28% perusahaan di Indonesia yang memiliki protokol keamanan siber memadai. Banyak organisasi masih menganggap keamanan siber sebagai biaya tambahan daripada investasi penting, membuat sistem mereka rentan terhadap berbagai bentuk serangan digital.
- Posisi Rentan dalam Peringkat Keamanan Siber:
  Laporan INTERPOL menempatkan Indonesia sebagai negara kedua paling rentan terhadap serangan siber di Asia. Kombinasi antara tingginya penetrasi internet, minimnya regulasi ketat, dan kurangnya SDM ahli di bidang keamanan siber menjadikan Indonesia sebagai sasaran empuk bagi cyber crime internasional.

Ketiga faktor tersebut saling berkaitan membuat ancaman siber di Indonesia semakin mengkhawatirkan dan membutuhkan penanganan serius dari semua pemangku kepentingan. Indonesia saat ini menghadapi beragam ancaman siber yang terus berkembang. Lima jenis serangan paling umum yang kerap menimpa perusahaan dan individu:

1. Phishing: Perangkap digital yang sulit dikenali; Serangan phishing di Indonesia semakin canggih dengan teknik social engineering yang memanfaatkan psikologi korban.
2. Ransomware: Penyanderaan data yang merugikan**;** Serangan ransomware seperti LockBit telah melumpuhkan operasional berbagai perusahaan di Indonesia.
3. Malware: Silent killer di perangkat digital**;** Spyware dan malware jenis baru mampu menyusup tanpa terdeteksi melalui aplikasi tidak resmi atau lampiran email. Malware ini bekerja diam-diam mencuri data login, informasi kartu kredit, hingga memantau aktivitas pengguna.
4. DDoS: Serangan yang melumpuhkan layanan digital; Banyak e-commerce dan layanan publik di Indonesia menjadi korban serangan Distributed Denial of Service (DDoS).

5. Kebocoran Data: Ancaman terhadap privasi**;** Kasus seperti kebocoran data BPJS Kesehatan 2021 menunjukkan betapa rentannya sistem penyimpanan data di Indonesia. Data pribadi yang bocor sering dijual di dark web dan digunakan untuk kejahatan lebih lanjut.

Sektor-Sektor Kritis yang Menjadi Target Utama Serangan Siber di Indonesia:

- Perbankan dan Fintech: Gudangnya Uang Digital; Sektor keuangan menjadi target utama serangan siber karena menyimpan aset bernilai tinggi. Modus yang sering digunakan antara lain skimming ATM, pembobolan sistem mobile banking, dan penipuan melalui aplikasi fintech palsu.
- E-Commerce: Ladangnya Transaksi Digital; Platform belanja online sering mengalami serangan DDoS yang mengganggu operasional, terutama saat event besar. Selain itu, marak penipuan melalui pembajakan akun pembeli dan manipulasi transaksi.
- Kesehatan: Harta Karun Data Medis; Data pasien bernilai tinggi di pasar gelap, bisa dijual $250 per rekam medis. Rumah sakit dan platform kesehatan digital sering menjadi sasaran ransomware karena sistem keamanan yang masih lemah.
- Pemerintah: Ancaman terhadap Infrastruktur Vital; Instansi pemerintah dan BUMN seperti PLN dan Pertamina pernah mengalami serangan yang mengancam stabilitas nasional.

Meski ancaman siber terus meningkat, Indonesia masih menghadapi beberapa kendala utama dalam membangun pertahanan siber yang kuat. Tantangan kritis yang perlu segera diatasi:

- Kelangkaan SDM Ahli Siber: Indonesia saat ini hanya memiliki sekitar 500 ahli siber bersertifikat, jauh di bawah kebutuhan ideal sekitar 20.000 profesional. Kesenjangan ini diperparah dengan minimnya perguruan tinggi yang menawarkan program studi khusus keamanan siber, serta rendahnya minat generasi muda terhadap bidang ini.
- Alokasi Anggaran yang minim: Banyak perusahaan, terutama UMKM, masih menganggap investasi *"cybersecurity"* sebagai beban biaya daripada kebutuhan strategis. Survei menunjukkan hanya 15% perusahaan di Indonesia yang mengalokasikan lebih dari 5% budget IT untuk keamanan siber, padahal standar global mencapai 10-15%.
- Fragmentasi Koordinasi: Masih terjadi ego sektoral antara instansi pemerintah, swasta, dan komunitas keamanan siber. BSSN sebagai koordinator nasional seringkali kesulitan menyelaraskan kebijakan karena tumpang tindih kewenangan dan kurangnya mekanisme berbagi informasi ancaman secara real-time.

Menghadapi ancaman siber yang semakin kompleks, organisasi perlu menerapkan pendekatan keamanan berlapis. Lima strategi efektif yang dapat segera diimplementasikan:

1. Multi-Factor Authentication (MFA) sebagai Pertahanan Awal; Implementasi MFA dapat mengurangi 99% upaya pembobolan akun dengan menambahkan verifikasi tambahan selain password. Solusi sederhana ini sangat efektif mencegah akses tidak sah meskipun password berhasil dicuri.

2. Update Sistem Secara Berkala; Pembaruan rutin sistem dan aplikasi menutupi celah keamanan yang sering dimanfaatkan peretas. Perusahaan perlu menerapkan patch management terstruktur untuk memastikan semua perangkat mendapatkan pembaruan keamanan tepat waktu.

3. Edukasi dan Pelatihan Karyawan; Mengingat 95% serangan bermula dari human error, program pelatihan kesadaran keamanan siber wajib dilakukan secara berkala. Fokuskan pada identifikasi email phishing, praktik password yang aman, dan protokol melaporkan insiden.

4. Backup Data Terenkripsi secara Rutin; Prosedur backup yang teratur dengan sistem 3-2-1 (tiga salinan, dua media berbeda, satu lokasi terpisah) menjadi senjata ampuh melawan ransomware. Pastikan backup dilakukan secara terenkripsi dan diuji secara berkala.

5. Audit Keamanan Menyeluruh; Assessment berkala seperti Cyber Security Maturity Assessment membantu mengidentifikasi kerentanan sebelum dieksploitasi peretas. Audit harus mencakup penetration testing dan review kebijakan keamanan minimal setahun sekali.

Problematika Kementerian Komunikasi dan Digital (KOMDIGI) dan Badan Siber dan Sandi Negara (BSSN) Dalam Upaya Memperkuat Ketahanan Siber Nasional

Upaya meningkatkan ketahanan siber nasional (Indonesia) bersifat multidimensional, mencakup aspek regulasi, kelembagaan, teknologi, sumber daya manusia, hingga koordinasi antarinstansi. Beberapa permasalahan utama yang dapat dijadikan dasar analisis akademik sbb:

1. Tumpang tindih kewenangan dan koordinasi kelembagaan

   Meskipun BSSN berperan sebagai lembaga utama di bidang keamanan siber nasional, sejumlah fungsi keamanan siber juga dijalankan oleh Kementerian KOMDIGI, POLRI, TNI, Badan Intelijen Negara (BIN), Otoritas Jasa Keuangan (OJK), Bank Indonesia (BI), serta kementerian dan lembaga lainnya.

Kondisi ini sering menimbulkan duplikasi fungsi dan program; koordinasi yang belum optimal dalam penanganan insiden siber; serta perbedaan standar keamanan antar sektor. Akibatnya, respons terhadap ancaman siber nasional menjadi kurang terintegrasi.

2. Regulasi yang belum komprehensif

Indonesia belum memiliki **Undang-Undang Keamanan Siber** yang mengatur secara menyeluruh mengenai tata kelola keamanan siber nasional; pembagian kewenangan lembaga; kewajiban pelaporan insiden siber; standar minimum keamanan siber nasional; perlindungan infrastruktur informasi kritis. Akibatnya, berbagai kebijakan masih tersebar dalam sejumlah peraturan yang belum sepenuhnya terintegrasi.

3. Meningkatnya kompleksitas ancaman siber

Ancaman siber berkembang lebih cepat dibandingkan kemampuan organisasi untuk mengantisipasinya. Indonesia menghadapi berbagai bentuk serangan, antara lain ransomware; phishing; malware; Distributed Denial of Service (DDoS); pencurian data pribadi; Advanced Persistent Threat (APT); serangan terhadap infrastruktur kritis *("critical infrastructure").* Kemajuan teknologi seperti kecerdasan buatan (AI) juga dimanfaatkan oleh pelaku kejahatan siber untuk meningkatkan skala dan efektivitas serangan.

4. Rendahnya tingkat keamanan pada sektor publik

Banyak instansi pemerintah masih menghadapi kendala seperti penggunaan sistem yang sudah usang (*legacy systems*); pembaruan keamanan yang tidak rutin; lemahnya pengelolaan identitas dan akses; keterbatasan anggaran untuk keamanan siber. Insiden kebocoran data dan gangguan terhadap layanan publik menunjukkan bahwa penguatan tata kelola keamanan masih menjadi tantangan.

5. Keterbatasan sumber daya manusia

Indonesia masih mengalami kekurangan tenaga profesional di bidang keamanan siber. Tantangan meliputi jumlah tenaga ahli yang belum mencukupi; kompetensi yang belum merata antarinstansi; tingginya perpindahan talenta ke sektor swasta karena perbedaan remunerasi; kebutuhan pelatihan yang berkelanjutan. Kondisi ini memengaruhi kemampuan pemerintah dalam mendeteksi, menganalisis, dan menangani insiden siber secara efektif.

6. Perlindungan infrastruktur informasi kritis

   Sektor-sektor seperti energi, telekomunikasi, keuangan, transportasi, kesehatan, dan pemerintahan semakin bergantung pada sistem digital. Tantangannya meliputi belum seragamnya standar keamanan; tingkat kematangan keamanan yang berbeda-beda; meningkatnya risiko serangan terhadap layanan esensial yang dapat berdampak pada stabilitas nasional.

7. Rendahnya kesadaran keamanan siber

   Faktor manusia masih menjadi salah satu penyebab utama keberhasilan serangan siber. Permasalahan yang sering ditemukan meliputi penggunaan kata sandi yang lemah; rendahnya kewaspadaan terhadap phishing; minimnya budaya keamanan informasi; kurangnya pelatihan keamanan siber bagi pegawai dan masyarakat.

8. Keterbatasan pendanaan dan infrastruktur

   Tidak semua instansi pemerintah memiliki kapasitas untuk mengembangkan Security Operations Center (SOC); sistem deteksi dan respons insiden; teknologi pemantauan ancaman ("*threat intelligence*"); sistem pencadangan (*backup*) dan pemulihan ("*disaster recovery*"). Perbedaan kapasitas ini menyebabkan tingkat kesiapan keamanan siber yang tidak merata.

9. Tantangan transformasi digital

   Percepatan digitalisasi layanan pemerintah meningkatkan efisiensi, tetapi juga memperluas "*attack surface*". Semakin banyak aplikasi, perangkat, dan layanan digital yang digunakan, semakin besar pula potensi kerentanan apabila keamanan tidak menjadi bagian dari proses perancangannya ("*security by design*")

Perkembangan Keamanan Siber Global - Tahun 2026

Tahun 2026, keamanan siber ("*cybersecurity*") diperkirakan akan terus mengalami perkembangan yang signifikan, tidak hanya dari aspek teknologi, tetapi juga dalam dimensi geopolitik, ekonomi, dan strategi. Perkembangan tersebut menunjukkan bahwa keamanan siber telah menjadi isu multidimensional yang memengaruhi stabilitas negara, keberlangsungan bisnis, serta kehidupan masyarakat yang semakin bergantung pada teknologi digital. Ruang siber ("*cyberspace*") semakin terintegrasi dengan dinamika geopolitik, perekonomian global, serta aktivitas sehari-hari individu maupun institusi. Berbagai insiden siber generasi baru telah memperlihatkan rapuhnya keterhubungan tersebut. Gangguan pada rantai pasok sektor ritel dan manufaktur, perlambatan operasional penerbangan, penyusupan ke sistem pemerintahan, hingga gangguan layanan komputasi awan ("*hyperscale cloud outages*") menunjukkan bahwa ekosistem digital global kini saling bergantung satu sama lain.

Dalam kondisi seperti ini, satu gangguan lokal atau serangan yang ditujukan kepada satu organisasi dapat dengan cepat menimbulkan dampak berantai ("*cascade effect*") yang meluas hingga tingkat global. Dalam konteks tersebut, keamanan siber tidak lagi dipandang sebagai fungsi teknis yang hanya menjadi tanggung jawab unit teknologi informasi. Sebaliknya, keamanan siber telah berkembang menjadi isu strategis yang memerlukan perhatian pemerintah, dunia usaha, dan masyarakat secara keseluruhan. Tantangan yang akan dihadapi pada tahun 2026 tidak hanya berkaitan dengan kesiapan teknologi, tetapi juga kemampuan berbagai pemangku kepentingan dalam menyelaraskan kebijakan, etika, tata kelola, serta kolaborasi untuk melindungi ekosistem digital yang semakin kompleks. Pendekatan yang bersifat proaktif melalui penguatan tata kelola, peningkatan kapasitas sumber daya manusia, pemanfaatan intelijen ancaman ("*threat intelligence*"), serta investasi pada teknologi keamanan yang adaptif menjadi faktor penting dalam membangun ketahanan siber yang berkelanjutan di era transformasi digital.

Penutup

Berbagai kebijakan dan inisiatif keamanan siber dipandang sebagai hasil dari proses politik yang dikenal sebagai **politik ancaman** ("*threat politics*"), yaitu proses politik yang menentukan bagaimana suatu ancaman dimasukkan, diprioritaskan, diubah, atau bahkan dihapus dari agenda kebijakan publik. Dengan kata lain, kebijakan keamanan siber tidak dapat dipisahkan dari persepsi terhadap ancaman siber yang berkembang pada suatu waktu. Oleh karena itu, setiap upaya untuk memahami strategi perlindungan siber harus mempertimbangkan bagaimana para pengambil keputusan memandang tingkat risiko dan ancaman yang dihadapi. Hasil dari proses politik tersebut dipengaruhi oleh berbagai faktor, antara lain aktor-aktor yang berperan dalam pengambilan kebijakan, persepsi mereka terhadap ancaman, serta lingkungan kelembagaan yang mencakup aturan hukum, norma, kebiasaan, dan sumber daya yang tersedia.

Keamanan siber tetap menjadi persoalan yang kompleks dan multidimensional, melibatkan beragam aktor dari berbagai sektor dengan kepentingan dan perspektif yang berbeda. Mekipun setiap negara mengembangkan pendekatan yang berbeda sesuai dengan kondisi nasionalnya, terdapat sejumlah tema utama yang muncul secara konsisten, yaitu pentingnya sistem peringatan dini ("*early warning*"), penguatan kerangka hukum, pengembangan kemitraan antara sektor publik dan swasta ("*public-private partnership*"), serta peningkatan kegiatan penelitian dan pengembangan.

Perspektif penegakan hukum dan penanggulangan kejahatan siber (*cybercrime*) menjadi pendekatan yang paling dominan. Kondisi ini dipengaruhi oleh karakteristik ancaman siber, ketersediaan sumber daya dalam institusi penegak hukum, serta norma hukum dan budaya yang membatasi pilihan strategi yang dapat diterapkan.

Oleh karena itu, salah satu tantangan utama yang dihadapi masyarakat internasional adalah harmonisasi regulasi hukum guna mempermudah proses penyelidikan, penuntutan, dan penegakan hukum terhadap pelaku kejahatan siber lintas negara. Dalam konteks tersebut," *Convention on Cybercrime*" atau Konvensi Budapest yang disusun oleh Dewan Eropa menjadi instrumen hukum internasional yang paling penting. Meskipun implementasi konvensi tersebut masih menghadapi berbagai tantangan praktis, keberadaannya mencerminkan adanya kesepahaman global mengenai perlunya standar hukum minimum dalam penanggulangan kejahatan siber.

Kebutuhan akan budaya keamanan siber global pada dasarnya muncul sebagai konsekuensi logis dari karakter Internet yang bersifat lintas batas dan tidak mengenal yurisdiksi negara. Ancaman siber yang dapat berasal dari mana saja menuntut adanya kerja sama internasional yang efektif, meskipun setiap pelaku kejahatan pada akhirnya tetap merupakan individu yang berada di lokasi fisik tertentu. Namun demikian, upaya membangun budaya keamanan siber global masih menghadapi tantangan besar, terutama akibat berkembangnya strategi militer yang memanfaatkan operasi jaringan komputer ("*computer network operations*") sebagai instrumen pertahanan maupun serangan terhadap negara lain. Kondisi tersebut berpotensi mengurangi peluang terciptanya budaya keamanan siber yang benar-benar bersifat universal, sehingga diperlukan adanya kesamaan pemahaman mengenai bentuk ancaman, kepentingan, serta kebutuhan seluruh pemangku kepentingan. Kesamaan pemahaman hanya dapat diwujudkan melalui dialog dan kerja sama yang memungkinkan semua pihak menggunakan kerangka berpikir dan bahasa yang sama dalam menghadapi isu keamanan siber. Dengan demikian, berbagai pemangku kepentingan tidak lagi bergerak secara parsial berdasarkan kepentingannya masing-masing, melainkan dapat bekerja secara terkoordinasi untuk mengurai kompleksitas persoalan dan mewujudkan budaya keamanan siber global yang lebih efektif, inklusif, dan berkelanjutan.

Kesimpulan

Lanskap keamanan siber pada tahun 2026 ditandai oleh perubahan teknologi yang berlangsung sangat cepat, semakin kuatnya keterhubungan antar sistem dan antar organisasi, serta masih adanya kesenjangan kapasitas keamanan siber ("*cyber inequity*"). Di tengah meningkatnya ancaman siber yang didukung oleh kecerdasan buatan ("*Artificial Intelligence/AI*"), ketidak-stabilan geopolitik, dan kerentanan rantai pasok, kebutuhan untuk membangun ketahanan siber ("*cyber resilience*") menjadi semakin mendesak. Risiko siber tidak lagi dapat dipandang semata-mata sebagai persoalan teknis, melainkan telah berkembang menjadi isu strategis yang berdampak terhadap aspek ekonomi, pemerintahan, dan kehidupan sosial. Oleh karena itu, penanganannya memerlukan koordinasi dan kolaborasi yang erat lintas sektor maupun lintas negara.

Pelaku ancaman ("*threat actors*") semakin memanfaatkan otomatisasi serta teknik serangan yang lebih canggih untuk mengeksploitasi berbagai kelemahan sistemik. Kondisi tersebut menuntut organisasi untuk tidak hanya mengandalkan inovasi teknologi dalam menghadapi ancaman siber, tetapi juga memperkuat tata kelola ("*governance*"), meningkatkan kapasitas sumber daya manusia, serta membangun budaya organisasi yang didasarkan pada kepercayaan dan kolaborasi. Kesenjangan antara organisasi yang memiliki tingkat ketahanan siber tinggi dengan organisasi yang masih memiliki keterbatasan kapasitas tetap menjadi tantangan utama. Kekurangan tenaga ahli keamanan siber dan keterbatasan sumber daya semakin memperbesar risiko sistemik yang dihadapi berbagai organisasi.

Terdapat alasan yang memberikan optimisme terhadap masa depan keamanan siber. Organisasi yang menjadikan ketahanan siber sebagai bagian dari agenda strategis kepemimpinan, secara proaktif mengelola risiko yang berasal dari rantai pasok dan penerapan kecerdasan buatan, serta membangun kolaborasi dengan seluruh ekosistem pemangku kepentingannya, akan memiliki kemampuan yang lebih baik dalam menghadapi gangguan dan beradaptasi terhadap berbagai bentuk ketidak-pastian. Selain itu, berkembangnya pendekatan kolaboratif berbasis intelijen ("*intelligence-driven collaboration*"), pelaksanaan pengujian berbasis skenario ("*scenario-based testing*"), serta harmonisasi regulasi menunjukkan bahwa tata kelola keamanan siber global bergerak menuju pendekatan pertahanan kolektif ("*collective defence*") yang semakin matang.

Pada akhirnya, pembangunan masa depan digital yang aman tidak dapat diwujudkan hanya melalui penerapan solusi teknologi semata. Upaya tersebut memerlukan kepemimpinan yang visioner, pembagian tanggung jawab yang jelas di antara seluruh pemangku kepentingan, serta komitmen bersama untuk meningkatkan standar minimum ketahanan siber secara kolektif sehingga manfaatnya dapat dirasakan oleh seluruh organisasi, bukan hanya oleh organisasi yang memiliki sumber daya besar.

Dengan semakin kaburnya batas antara dunia digital dan dunia fisik, organisasi yang mampu bertahan dan berkembang adalah organisasi yang memandang ketahanan siber sebagai tanggung jawab strategis bersama. Ketahanan siber menjadi fondasi dalam membangun kepercayaan, mendorong inovasi, serta melindungi keberlangsungan ekosistem digital global yang saling terhubung. Ketahanan siber tidak hanya bergantung pada penerapan teknologi keamanan, tetapi juga pada kepemimpinan yang kuat, tata kelola yang efektif, budaya organisasi yang mendukung, serta kerja sama antar pemangku kepentingan dalam membangun ekosistem digital yang aman, tangguh, dan berkelanjutan.

Problematika yang dihadapi Kementerian KOMDIGI dan BSSN dalam upaya meningkatkan ketahanan siber nasional, tidak hanya berkaitan dengan aspek teknis, tetapi juga menyangkut tata kelola keamanan siber nasional. Tantangan utama meliputi belum optimalnya koordinasi antar instansi, belum komprehensifnya regulasi, keterbatasan sumber daya manusia dan anggaran, meningkatnya kompleksitas ancaman siber, serta perlunya peningkatan perlindungan terhadap infrastruktur informasi kritis. Oleh karena itu, peningkatan keandalan keamanan siber Indonesia memerlukan pendekatan yang terintegrasi melalui penguatan regulasi, pengembangan kapasitas kelembagaan, peningkatan kompetensi SDM, investasi teknologi, dan kolaborasi yang lebih erat antara pemerintah, sektor swasta, akademisi, dan masyarakat.

Jakarta, 21 Juli 2026

Referensi:

1. A Comparative Analysis of Cybersecurity Initiatives Worldwide, ITU, June 2005
2. Cyberspace: Definition and Implications, Ottis, R & Lorents P, 2010
3. Cyber-Security dan Tantangan Pengembangan Di Indonesia, Handrini Ardiyanti, Politica Vol 5, Juni 2014
4. Guide To Developing A National Cybersecurity Strategy: Strategic Engagement in Cybersecurity, ITU, 2017
5. Cyber Security, Rabab Syed, et.al, Sustainable Policy Institute, 2019
6. Unpacking Cyber Resilience, White Paper, World Economic Forum, November 2024
7. Mengapa Ancaman Cyber Menjadi Fokus Global Khusnya Di Indonesia, POXSIS, IT GRC, June 11, 2025
8. The Cyber Resilience Compass: Journeys Towards Resilience, White Paper, World Economic Forum, April 2025
9. EDAVOS, Kasus Cybercrime Terbaru Yang Mengguncang Indonesia, 2026
10. The Current and Future Trends of ICT (version 2.0), National Institute of Information and Communication Technology, March, 2026
11. What Is Cyber Resiliance, IBM, July 23, 2026
12. Global Cybersecurity Outlook 2026, Insight Report, World Economic Forum, April 2025