JIMU: Jurnal Ilmiah Multi Disiplin
Vol. 04, No. 01, Tahun 2025, Hal.892-902, ISSN: 3031-9498 (Online)

Strategi Keamanan Siber Indonesia dalam Perspektif Neorealisme

Agnes Glory Bakara[1], Indra Fauzan[2]

[1,2]Program Studi Ilmu Politik, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Sumatera Utara

E-mail : agnesbkr20@gmail.com

Article Info

Article history:
Received Oktober 10, 2025
Revised Oktober 13, 2025
Accepted Oktober 15, 2025

Keywords:
Cybersecurity, National Strategy, Neorealism, State Capacity, BSSN

ABSTRACT

The rapid development of digital technology has positioned cybersecurity as a strategic aspect in maintaining national stability and state sovereignty. As the fourth-largest internet user in the world, Indonesia faces an increasing escalation of cyberattacks targeting public infrastructure, personal data, and strategic state systems. This study aims to analyze Indonesia's cybersecurity strategy through the lens of neorealism and Francis Fukuyama's theory of state capacity. Using a qualitative method and literature-based approach, the research analyzes secondary data from government documents, academic journals, cybersecurity reports, and national regulations. The findings reveal that Indonesia has adopted an internal balancing strategy through the establishment of the National Cyber and Crypto Agency (BSSN), the strengthening of CSIRTs (Computer Security Incident Response Team), NSOC (National Security Operation Center), and public awareness programs, as a response to the anarchic nature of the international system. However, from Fukuyama's perspective, policy implementation still encounters structural challenges such as weak coordination, limited human resources, and governance gaps across institutions. Therefore, Indonesia's cybersecurity strategy must be supported by institutional strengthening, regulatory reform, and enhanced operational capacity to ensure resilience and adaptability in the face of evolving cyber threats.

Article Info

Article history:
Received Oktober 10, 2025
Revised Oktober 13, 2025
Accepted Oktober 15, 2025

Kata Kunci:
Keamanan Siber, Strategi Nasional, Neorealisme, Kapasitas Negara, BSSN

ABSTRAK

Perkembangan teknologi digital yang pesat telah menjadikan keamanan siber sebagai aspek strategis dalam menjaga stabilitas nasional dan kedaulatan negara. Indonesia sebagai negara dengan pengguna internet terbesar keempat di dunia menghadapi eskalasi serangan siber yang menargetkan infrastruktur publik, data pribadi, dan sistem strategis negara. Penelitian ini bertujuan untuk menganalisis strategi keamanan siber Indonesia melalui pendekatan teori neorealisme dan teori negara oleh Francis Fukuyama. Penelitian menggunakan metode kualitatif dengan pendekatan studi pustaka, menganalisis data sekunder dari dokumen pemerintah, jurnal, laporan keamanan, dan regulasi nasional. Hasil penelitian menunjukkan bahwa Indonesia telah mengadopsi strategi internal balancing melalui pembentukan Badan Siber dan Sandi Negara (BSSN), penguatan CSIRT (Computer Security Incident Response Team), NSOC (National Security Operation Center), serta peningkatan kesadaran publik sebagai respons terhadap sistem internasional yang anarkis. Namun, dari perspektif teori kapasitas negara Fukuyama,

implementasi kebijakan masih menghadapi kendala struktural, seperti lemahnya koordinasi, keterbatasan SDM, dan kesenjangan tata kelola antar lembaga. Oleh karena itu, strategi keamanan siber Indonesia perlu ditopang dengan penguatan kelembagaan, pembaruan regulasi yang komprehensif, serta peningkatan kapasitas operasional negara agar mampu bertahan dan adaptif terhadap ancaman siber yang terus berkembang.

Corresponding Author:
Bhaskara Wisnu Ardli Mahardika
PT. Adaro Indonesia
E-mail: bhaskarawisnu@gmail.com

PENDAHULUAN

Perkembangan era digital yang semakin pesat menjadikan aspek keamanan siber sebagai elemen fundamental dalam menjaga stabilitas negara, melindungi data pribadi, serta memastikan kelangsungan operasional layanan publik dan sektor bisnis. Digitalisasi yang merambah hampir seluruh sektor telah meningkatkan efisiensi dan efektivitas berbagai sistem, namun di saat yang bersamaan juga menciptakan celah yang dapat dimanfaatkan oleh ancaman siber yang semakin kompleks. Ancaman siber itu sendiri adalah setiap kondisi atau kejadian yang dapat membahayakan keamanan informasi, khususnya dalam aspek kerahasiaan, integritas, serta ketersediaan data dan sistem (Arianto & Anggraini, 2019).

Indonesia sebagai negara dengan pertumbuhan pengguna internet terbesar keempat di dunia, meningkatnya aktivitas transaksi digital, serta penerapan sistem digital dalam layanan pemerintahan menjadikan negara ini sebagai salah satu sasaran utama serangan siber, baik yang bersifat kriminal, spionase, maupun sabotase. Dampak dari serangan siber sangat beragam, mencakup pencurian data pribadi, manipulasi sistem keuangan, gangguan terhadap layanan publik, hingga ancaman serius terhadap keamanan nasional.

Di Indonesia, aspek keamanan siber kian menempati posisi strategis dalam dinamika politik nasional, sebagaimana tercermin dalam debat calon presiden tahun 2024. Dalam forum tersebut, ketiga kandidat, yakni Anies Baswedan, Prabowo Subianto, dan Ganjar Pranowo, secara terbuka mengemukakan urgensi penguatan pertahanan siber Indonesia. Ketiganya sepakat bahwa ancaman di ruang siber merupakan permasalahan strategis yang membutuhkan respons serius melalui peningkatan kapabilitas pertahanan, pengembangan sumber daya manusia yang andal, serta pembaruan infrastruktur keamanan digital (Andhika R, 2024).

Dalam beberapa tahun terakhir, Indonesia mengalami sejumlah insiden kebocoran data dalam skala besar (Tabel 1.1), yang menunjukkan bahwa sistem pertahanan siber yang ada masih belum sepenuhnya mampu mengamankan infrastruktur digital nasional, bahkan serangan secara khusus menargetkan lembaga pemerintah dan institusi strategis, mengindikasikan adanya pola peretasan yang sistematis dan terencana.

Tabel 1 Data Serangan Siber di Indonesia

Tahun	Insiden	Keterangan
2013	Penyadapan oleh Australia	Dokumen yang dibocorkan oleh Edward Snowden mengungkap bahwa badan intelijen Australia menyadap komunikasi Presiden Susilo Bambang Yudhoyono, Ibu Negara Ani Yudhoyono, dan beberapa pejabat tinggi Indonesia pada tahun 2009.
2014	Serangan Terhadap Situs KPU	Situs Komisi Pemilihan Umum (KPU) mengalami serangan siber yang menyebabkan tampilan situs berubah dan informasi yang ditampilkan menjadi tidak akurat.
2015	Pembobolan Data Tokopedia	Platform e-commerce Tokopedia mengalami kebocoran data yang mengakibatkan informasi pribadi pengguna terekspos.
2016	Serangan Ransomware pada Rumah Sakit	Beberapa rumah sakit di Indonesia menjadi korban serangan ransomware, mengakibatkan gangguan operasional dan akses terhadap data pasien.
2017	Insiden Malware WannaCry	Indonesia termasuk salah satu negara yang terdampak oleh serangan malware WannaCry, yang menginfeksi berbagai institusi dan perusahaan, menyebabkan enkripsi data dan permintaan tebusan.
2019	Kebocoran Data e-Commerce	Beberapa platform e-commerce mengalami kebocoran data, mengakibatkan informasi pengguna tersebar di internet.
2020	Peretasan Situs DPR RI	Situs Dewan Perwakilan Rakyat Republik Indonesia diretas, menyebabkan perubahan tampilan dan gangguan akses sementara.
2021	Kebocoran data BPJS Kesehatan	Data pribadi sekitar 279 juta warga Indonesia yang terdaftar di BPJS Kesehatan dilaporkan bocor dan dijual di forum daring.
2022	Serangan oleh peretas "Bjorka"	Peretas dengan nama samaran "Bjorka" mengklaim membocorkan 1,3 juta data registrasi SIM card warga Indonesia, termasuk nomor induk kependudukan (NIK) dan nomor telepon.
2023	Serangan ransomware terhadap Bank Syariah Indonesia (BSI)	Pada pertengahan tahun 2023, Bank Syariah Indonesia mengalami serangan ransomware yang mengakibatkan gangguan operasional dan akses layanan perbankan bagi nasabah.
2024	Kebocoran data Direktorat	Data nomor pokok wajib pajak (NPWP) milik jutaan warga Indonesia, termasuk Presiden Joko Widodo dan beberapa

	Jenderal Pajak	menteri, dilaporkan bocor dan tersebar di internet.

Sumber: Diolah dari CSIRT (2024), EXABYTES (2022), dan Kompaspedia (2024).

Insiden-insiden diatas menegaskan bahwa keamanan siber di Indonesia masih menghadapi tantangan yang signifikan dan belum sepenuhnya teratasi. Walaupun perkembangan global telah sepenuhnya mengarah pada era digital, sistem keamanan siber di Indonesia masih menghadapi berbagai kelemahan yang bersifat mendasar. Salah satu faktor utama yang memengaruhi kondisi ini adalah keterbatasan sumber daya manusia yang memiliki kompetensi di bidang keamanan siber, baik dari sisi jumlah maupun kualitas. Di samping itu, tingkat literasi digital serta kesadaran akan pentingnya perlindungan data di kalangan masyarakat, pelaku usaha, dan instansi pemerintah masih tergolong rendah.

Ancaman siber telah menjadi isu yang krusial di berbagai sektor di Indonesia, mencakup pemerintahan, layanan publik, hingga industri swasta. Kemajuan dalam teknologi informasi serta percepatan digitalisasi memang menawarkan efisiensi dan kemudahan dalam berbagai aspek kehidupan. Namun, di sisi lain, perkembangan ini turut meningkatkan potensi risiko serangan siber yang berpotensi merugikan individu, lembaga, bahkan stabilitas negara secara keseluruhan (Ginanjar, 2022). Serangan siber tidak hanya berimplikasi pada kebocoran data pribadi, tetapi juga dapat mengancam operasional layanan publik dalam skala luas, salah satunya adalah serangan ransomware WannaCry yang terjadi pada Mei 2017. Serangan ini merupakan salah satu insiden siber terbesar dalam sejarah, dengan lebih dari 200.000 komputer di 150 negara mengalami gangguan keamanan termasuk Indonesia. Di Indonesia sendiri, sektor yang paling terdampak adalah layanan kesehatan, terutama rumah sakit.

Beberapa institusi medis mengalami gangguan signifikan, seperti Rumah Sakit Harapan Kita dan Dharmais di Jakarta, dimana sistem komputer mereka terkena enkripsi oleh ransomware ini, sehingga menyebabkan disrupsi operasional yang meliputi proses pendaftaran pasien, akses terhadap data rekam medis, serta kegiatan administrasi lainnya. Penyebaran ransomware ini berlangsung dengan sangat cepat karena mengeksploitasi kelemahan dalam jaringan internal yang tidak memiliki perlindungan memadai (Hapsari & Pambayun, 2023). Serangan ini juga semakin merugikan korban karena pelaku meminta tebusan dalam bentuk Bitcoin agar kunci dekripsi dapat diperoleh. Pemilihan Bitcoin sebagai metode pembayaran dalam serangan ini tidak terlepas dari karakteristiknya yang anonim dan sulit dilacak, memungkinkan pelaku untuk menerima pembayaran tanpa mudah teridentifikasi oleh otoritas keamanan siber atau lembaga penegak hukum internasional.

Pelaku serangan *ransomware* kerap beroperasi dari lokasi yang sulit dijangkau dan berada di luar cakupan yurisdiksi hukum negara-negara yang terdampak, sehingga upaya mitigasi dan penegakan hukum menjadi sangat terbatas. Ketiadaan otoritas global yang memiliki kewenangan untuk mengoordinasikan respons atau menetapkan regulasi yang mengikat menyebabkan setiap negara harus menghadapi ancaman ini secara mandiri, sehingga efektivitas penanganan sangat bergantung pada kapasitas keamanan siber masing-masing negara (Jayakarta, 2024). Selain itu, terdapat indikasi bahwa beberapa serangan ransomware memiliki keterkaitan dengan kepentingan aktor negara tertentu, yang semakin memperumit

situasi serta berpotensi meningkatkan ketegangan dalam dinamika hubungan internasional. Ketimpangan dalam penguasaan teknologi dan kesiapan pertahanan siber antarnegara juga menyebabkan beberapa wilayah lebih rentan menjadi sasaran serangan, bahkan dapat berfungsi sebagai titik awal penyebaran ransomware secara luas. Seiring dengan meningkatnya ketergantungan terhadap sistem digital, penguatan keamanan siber menjadi suatu keharusan guna meminimalisasi dampak dari serangan serupa di masa yang akan datang.

Keamanan siber merupakan integrasi antara unsur manusia, kebijakan, prosedur, dan teknologi yang secara bersama-sama berfungsi untuk melindungi sistem komputer, jaringan, serta data dari akses ilegal atau serangan siber, sekaligus menjamin terpeliharanya prinsip kerahasiaan, integritas, dan ketersediaan informasi dalam lingkungan digital (Stallings, 2018). Keamanan siber tidak hanya berkutat pada aspek teknis semata, melainkan juga mencakup dimensi institusional dan regulatif yang saling melengkapi dalam membentuk sistem perlindungan menyeluruh terhadap ancaman digital yang bersifat domestik maupun transnasional. Ancaman tersebut dapat muncul dalam berbagai bentuk, seperti malware, phishing, hacking, dan ransomware, yang keseluruhannya memiliki potensi menimbulkan konsekuensi serius, mulai dari kerugian ekonomi, kebocoran data pribadi, hingga gangguan terhadap infrastruktur kritis negara, termasuk sistem keuangan, jaringan komunikasi, dan layanan publik.

Pemerintah Indonesia tengah berupaya membangun pertahanan digital yang lebih tangguh guna menghadapi ancaman siber yang kian berkembang. Sementara Angkatan Siber Indonesia diproyeksikan akan menjadi benteng pertahanan utama dalam menghadapi serangan siber berskala besar. Peraturan BSSN No. 10 Tahun 2021 bertujuan untuk memperkuat tata kelola dan kebijakan keamanan siber nasional. Dengan langkah-langkah ini, Indonesia berusaha untuk meningkatkan kesiapan dan ketahanan siber dalam menghadapi tantangan di era digital yang semakin kompleks. Strategi berbasis organisasi juga memiliki peran signifikan dalam mengatasi ketidakamanan digital .

Dalam pembahasan mengenai keamanan siber, dimensi politik dan kekuasaan berperan penting dalam membentuk lanskap keamanan digital di tingkat global. Sejarah telah membuktikan bahwa persaingan geopolitik dan perlombaan teknologi memiliki keterkaitan yang erat, di mana kemajuan di bidang siber tidak hanya bergantung pada inovasi teknologis semata, tetapi juga dipengaruhi oleh keputusan strategis yang diambil dalam konteks politik dan kepentingan nasional. Ruang siber bukan sekadar hasil perkembangan teknologi, melainkan juga cerminan dari kepentingan negara-negara besar yang merancang strategi politik untuk mempertahankan dominasinya di ranah internasional.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kepustakaan (*library research*) (Sugiyono, 2019). Pendekatan tersebut dipilih karena penelitian ini berfokus pada analisis strategi keamanan siber Indonesia melalui kacamata teori neorealisme dalam studi hubungan internasional. Metode kualitatif memungkinkan peneliti menggali secara mendalam fenomena yang diteliti berdasarkan berbagai sumber data yang relevan, seperti dokumen resmi,

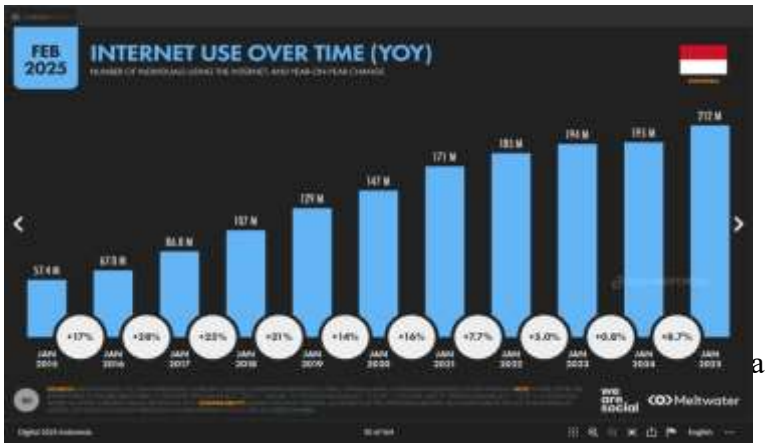
kebijakan pemerintah, jurnal ilmiah, serta literatur yang berkaitan dengan keamanan siber dan teori neorealisme.

Proses pengumpulan data dilakukan dengan menelusuri berbagai sumber pustaka, termasuk dokumen pemerintah yang memuat kebijakan keamanan siber, jurnal akademik yang meninjau isu keamanan siber dalam konteks hubungan internasional, laporan organisasi internasional mengenai kebijakan dan strategi keamanan siber global, serta artikel dari media yang kredibel. Data yang diperoleh kemudian dianalisis menggunakan metode analisis isi (*content analysis*) untuk menafsirkan strategi keamanan siber Indonesia dalam kerangka teori neorealisme. Tahapan analisis meliputi reduksi data untuk memilah dan menyederhanakan informasi penting, penyajian data dalam bentuk uraian naratif yang disertai interpretasi teoritis, serta penarikan kesimpulan berdasarkan prinsip-prinsip neorealisme guna memahami bagaimana Indonesia merancang strategi menghadapi ancaman siber.

HASIL DAN PEMBAHASAN

Kondisi Keamanan Siber di Indonesia

Perkembangan teknologi informasi dan komunikasi (TIK) di Indonesia telah mengalami lonjakan signifikan dalam dua dekade terakhir. Hal ini ditandai dengan meningkatnya akses internet, penggunaan perangkat digital, serta adopsi sistem berbasis teknologi dalam berbagai sektor. Indonesia merupakan salah satu negara dengan jumlah pengguna internet terbesar di dunia. Berdasarkan laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pada tahun 2024 terdapat lebih dari 221 juta pengguna internet di Indonesia setara dengan 79,5 persen dari total populasi Indonesia. Jumlah pengguna internet di Indonesia terus menunjukkan tren peningkatan, hingga pada awal Januari 2025 tercatat telah mencapai 212 juta pengguna (APJII, 2024).



a

Jumlah pengguna internet di Indonesia terus mengalami peningkatan dari waktu ke waktu. Pada awal Januari 2025, telah tercatat sebanyak 212 juta pengguna, dan jumlah ini diperkirakan akan meningkat lagi sebesar 1% hingga 2%. Pertumbuhan ini dipicu oleh pergeseran fungsi internet yang kini telah menjadi salah satu kebutuhan dasar masyarakat Indonesia. Angka tersebut mencerminkan betapa cepatnya transformasi digital terjadi dan menuntut kesiapan negara dalam melindungi ruang digitalnya.

Regulasi dan Kebijakan Keamanan Siber di Indonesia

Era global yang ditandai oleh konektivitas digital dan disrupsi teknologi telah mendorong ruang siber menjadi salah satu dimensi strategis utama dalam hubungan internasional. Peran ruang siber tidak lagi terbatas sebagai sarana komunikasi dan pertukaran informasi, melainkan telah berkembang menjadi arena kontestasi yang memengaruhi aspek ekonomi digital, dinamika sosial, serta pertahanan dan keamanan nasional. Negara-negara berlomba untuk memperkuat postur keamanan digitalnya sebagai bentuk upaya mempertahankan kedaulatan dan menanggulangi ancaman non-tradisional yang bersifat asimetris.

Sebagai respons terhadap meningkatnya kompleksitas ancaman siber, diperlukan strategi nasional yang komprehensif dan berkelanjutan. Penguatan sistem keamanan digital harus mencakup dimensi teknis, normatif, dan kelembagaan, termasuk melalui pembentukan regulasi dan kebijakan yang berfungsi sebagai fondasi hukum dan politik dalam mengatur ruang digital secara sistematis. Selain itu, kerja sama internasional perlu diperluas untuk mengantisipasi risiko lintas batas yang melibatkan aktor dari berbagai yurisdiksi.

Lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian direvisi melalui Undang-Undang Nomor 19 Tahun 2016, menjadi tonggak awal dalam pembangunan kerangka hukum nasional untuk mengatur aktivitas digital dan menangani pelanggaran di ruang siber. UU ITE disahkan pada tanggal 21 April 2008 dan mulai berlaku setelah diundangkan dalam Lembaran Negara Republik Indonesia Nomor 58 Tahun 2008. Undang-undang ini dirancang dengan tujuan utama untuk memberikan kepastian hukum terhadap penggunaan teknologi informasi yang aman, bertanggung jawab, dan produktif di seluruh sektor, termasuk pemerintahan, dunia usaha, serta masyarakat secara umum. Kebutuhan akan regulasi tersebut muncul sebagai respons atas pesatnya perkembangan teknologi informasi dan komunikasi (TIK) di Indonesia, yang menghadirkan peluang sekaligus potensi ancaman terhadap tatanan sosial, ekonomi, dan hukum nasional.

Kementerian Komunikasi dan Digital (Komdigi) juga memegang peranan strategis dalam memperkuat keamanan siber nasional melalui serangkaian kebijakan, regulasi teknis, dan penguatan kelembagaan yang menyasar seluruh ekosistem penyelenggara sistem elektronik. Sebagai institusi pemerintah yang bertanggung jawab atas tata kelola ruang digital Indonesia, Komdigi berperan aktif dalam merumuskan regulasi terkait keamanan data, perlindungan infrastruktur informasi vital, serta peningkatan ketahanan sistem digital nasional dari berbagai ancaman siber yang bersifat lintas batas dan semakin kompleks.

Penyebab Terjadinya Serangan Siber di Indonesia

Maraknya serangan siber, baik dalam skala global maupun nasional, tidak dapat dilepaskan dari karakter anarkis sistem internasional, yang tidak memiliki otoritas pusat untuk secara efektif mengatur perilaku negara-negara di dalamnya. Dalam konteks ini, setiap negara bertindak berdasarkan prinsip *self help*, yaitu mengandalkan kapabilitas internal masing-masing guna menjamin keamanan dan kepentingan nasionalnya. Ancaman terhadap keamanan kini tidak hanya bersumber dari kekuatan militer konvensional, melainkan juga dari kemajuan

teknologi informasi yang berkembang pesat tanpa diiringi oleh mekanisme pengawasan global yang mengikat.

Negara-negara lebih cenderung mengedepankan kepentingan nasional dalam menanggapi ancaman siber, sehingga sulit tercapai konsensus global mengenai standar dan norma keamanan digital. Ketimpangan teknologi antara negara maju dan berkembang turut memperumit proses perumusan aturan bersama. Negara dengan kapabilitas teknologi tinggi cenderung mempertahankan keunggulan strategisnya daripada mendorong keterbukaan dan kerja sama internasional. Akibatnya, harmonisasi kebijakan keamanan siber di tingkat global berjalan lambat, sementara negara-negara berkembang seperti Indonesia menjadi kelompok yang paling rentan terhadap ancaman siber karena keterbatasan dalam aspek perlindungan dan kapasitas retaliasi yang memadai dalam ketiadaan kerangka hukum universal.

Ketiadaan kerangka hukum internasional yang bersifat *binding* menjadi salah satu penyebab utama lemahnya tata kelola siber antarnegara. Hingga saat ini, berbagai inisiatif internasional masih bersifat sukarela atau berupa *soft law*, seperti resolusi Majelis Umum PBB mengenai norma perilaku negara di ruang siber, panduan teknis dari *International Telecommunication Union* (ITU), dan deklarasi politik pada forum seperti ASEAN *Ministerial Conference on Cybersecurity*. Meskipun inisiatif tersebut mencerminkan kesadaran global akan pentingnya keamanan digital, kelemahannya terletak pada absennya mekanisme penegakan hukum yang bersifat memaksa dan dapat menjatuhkan sanksi atas pelanggaran yang terjadi.

Kondisi ini menciptakan kekosongan hukum (*legal vacuum*) yang dieksploitasi oleh aktor negara maupun non-negara untuk melakukan serangan siber yang merugikan. Negara korban sering kali tidak memiliki jalur hukum internasional yang efektif untuk menuntut pertanggungjawaban pelaku. Hal ini diperburuk oleh tidak adanya kesepakatan global terkait definisi kejahatan siber, mekanisme atribusi serangan, serta prinsip-prinsip normatif seperti kedaulatan digital dan *due diligence*. Perbedaan persepsi antarnegara mengenai batasan dan bentuk ancaman siber menghambat proses harmonisasi hukum internasional, sehingga penanganan insiden kerap kali tidak efektif dan cenderung berlarut-larut.

Keterbatasan Kelembagaan dan Tata Kelola Siber

Salah satu faktor mendasar yang menyebabkan lemahnya respons Indonesia terhadap berbagai insiden siber dalam beberapa tahun terakhir adalah fragmentasi kelembagaan dalam tata kelola keamanan digital nasional. Sejumlah lembaga negara seperti Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Digital (Komdigi), Direktorat Tindak Pidana Siber Bareskrim Polri. Direktorat Tindak Pidana Siber (Dittipidsiber), serta Satuan Siber Tentara Nasional Indonesia (Satsiber TNI) memiliki mandat dan peran masing-masing dalam menangani isu- isu siber.

Ketidakterpaduan ini berdampak pada absennya struktur komando terpadu yang dapat mengoordinasikan respons ketika terjadi serangan besar atau pelanggaran data berskala nasional. Masing-masing lembaga cenderung beroperasi berdasarkan fungsi sectoral misalnya, unit patroli siber Polri lebih menitikberatkan pada penegakan hukum, Satsiber TNI fokus pada aspek pertahanan, sementara Komdigi lebih berperan dalam formulasi kebijakan dan

diseminasi publik. Tanpa sistem integrasi yang menyeluruh, penanganan insiden cenderung bersifat sektoral dan reaktif. Dalam kasus kebocoran data yang dialami oleh instansi pemerintah atau perusahaan strategis, langkah yang diambil seringkali terbatas pada klarifikasi administratif, tanpa dilengkapi investigasi forensik atau perbaikan sistemik.

Lemahnya Landasan Hukum yang Menyeluruh dan Mengikat

Ketiadaan kerangka regulatif yang utuh, komprehensif, dan mengikat yang secara jelas mengatur aspek teknis, strategis, dan kelembagaan dalam sistem keamanan digital. Meskipun Indonesia telah mengesahkan sejumlah peraturan perundang-undangan seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), regulasi tersebut belum secara menyeluruh menjawab kebutuhan strategis keamanan siber. UU ITE, misalnya, lebih menitikberatkan pada aspek penindakan terhadap kejahatan digital, tanpa memberikan kerangka kebijakan preventif dan teknis dalam menghadapi serangan siber yang bersifat terstruktur dan sistemik. Di sisi lain, UU PDP lebih berorientasi pada aspek perlindungan data pribadi individu, bukan pada penguatan sistemik terhadap infrastruktur keamanan digital nasional atau manajemen risiko siber lintas sektor.

Ketiadaan undang-undang khusus mengenai keamanan siber menyebabkan terjadinya kekosongan regulasi yang berdampak langsung pada ketidakterpaduan standar keamanan digital antar sektor. Setiap lembaga atau entitas cenderung mengembangkan sistem pengamanan sendiri berdasarkan kemampuan internal dan interpretasi masing-masing terhadap risiko siber. Dalam banyak kasus, pendekatan yang diambil bersifat reaktif dan minimalis, bukan preventif dan strategis.

Penguatan Infrastruktur dan Teknologi

Penguatan infrastruktur dan teknologi merupakan komponen vital dalam strategi internal balancing, di mana negara berupaya membangun kapasitas domestik guna menghadapi ancaman eksternal tanpa ketergantungan pada pihak luar. Dalam era digital yang semakin kompleks, ruang siber telah berkembang menjadi domain strategis yang menuntut fondasi teknologi yang kokoh agar negara mampu menjaga kedaulatan serta stabilitas nasional.

Salah satu langkah utama yang diambil adalah pembangunan Pusat Data Nasional (PDN), yang dirancang sebagai simpul utama pengelolaan data pemerintahan. Melalui PDN, pemerintah melakukan konsolidasi penyimpanan dan pengolahan data secara terpusat, sehingga tidak hanya meningkatkan efisiensi, tetapi juga memperkuat kontrol keamanan yang lebih terstandarisasi.

Peningkatan Kapasitas SDM dan Kesadaran Siber

Kapasitas sumber daya manusia (SDM) serta tingkat kesadaran masyarakat memegang peranan sentral dalam strategi internal balancing untuk memastikan keberlanjutan negara di tengah sistem internasional yang tidak memiliki otoritas sentral. Selain penguatan infrastruktur dan teknologi, negara juga dituntut untuk mengembangkan kemampuan aktor-aktor manusianya agar mampu mengelola, memelihara, dan mengembangkan sistem keamanan digital secara berkesinambungan.

Indonesia memahami bahwa keberhasilan dalam menjaga keamanan siber tidak hanya bergantung pada aspek teknologi, melainkan juga pada kompetensi individu serta kesadaran kolektif masyarakat terhadap risiko di dunia digital. Oleh sebab itu, pengembangan kapasitas SDM dan peningkatan kesadaran siber menjadi salah satu fondasi utama dalam kebijakan keamanan siber nasional.

KESIMPULAN DAN SARAN

Penelitian ini menyimpulkan bahwa strategi keamanan siber Indonesia secara konseptual telah sejalan dengan prinsip-prinsip neorealisme yang menekankan pentingnya penguatan kapasitas domestik (internal balancing) untuk menjaga kedaulatan negara di tengah sistem internasional yang anarkis. Pembentukan Badan Siber dan Sandi Negara (BSSN) serta peningkatan kapasitas nasional melalui pengembangan CSIRT dan sistem deteksi insiden siber mencerminkan langkah adaptif Indonesia terhadap dinamika ancaman global. Namun, efektivitas strategi tersebut masih menghadapi sejumlah tantangan sebagaimana dikemukakan oleh teori negara Francis Fukuyama, yakni lemahnya kapasitas institusional dan tata kelola pemerintahan dalam menjalankan kebijakan secara efisien, akuntabel, dan berkelanjutan. Masih tingginya kasus kebocoran data, rendahnya literasi siber masyarakat, serta keterbatasan koordinasi lintas lembaga menunjukkan bahwa ketahanan digital Indonesia belum sepenuhnya kokoh.

Oleh karena itu, strategi keamanan siber Indonesia ke depan perlu diarahkan pada penguatan kapasitas kelembagaan dan sumber daya manusia, peningkatan koordinasi lintas instansi, serta percepatan pembentukan regulasi komprehensif seperti RUU Keamanan dan Ketahanan Siber. BSSN harus diberdayakan tidak hanya sebagai institusi teknis, tetapi juga sebagai pusat koordinasi nasional yang mampu memimpin kebijakan, pelatihan, serta literasi siber secara menyeluruh. Selain itu, Indonesia perlu memperkuat kerja sama internasional di bidang keamanan siber untuk memperluas kapasitas deteksi dini dan pertukaran keahlian, tanpa mengabaikan prinsip kemandirian nasional. Dengan langkah-langkah tersebut, diharapkan strategi keamanan siber Indonesia dapat lebih efektif, adaptif, dan berdaya saing dalam menghadapi tantangan dunia digital yang terus berkembang.

DAFTAR PUSTAKA

Arianto, A. R., & Anggraini, G. (2019). Membangun Pertahanan Dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team On Internet Infrastructure (ID-SIRTII). *Jurnal Pertahanan Dan Bela Negara, 9(1), 13.* https://doi.org/https://doi.org/10.33172/jpbh.v9i1.497

Andhika R. (2024, 8 Januari). *Debat Ketiga Calon Presiden 2024: Soroti Isu Peningkatan Keamanan Siber untuk Kedaulatan Nusantara*. Fourtrezz. https://fourtrezz.co.id/debat-ketiga- calon-presiden-2024-soroti-isu-peningkatan-keamanan-siber-untuk-kedaulatan-nusantara/

APJII. (2024). *Laporan Survei Internet Indonesia 2024*. Jakarta: Asosiasi Penyelenggara Jasa Internet Indonesia.

Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi

Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara. *Jurnal Dinamika Global*, *7*(02), 291–312. https://doi.org/10.36859/jdg.v7i02.1187

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman Cybercrime Di Indonesia: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, *5*(1), 1–17. https://doi.org/10.33701/jk.v5i1.3208

Jayakarta, D. (2024). Strategi Keamanan Siber Amerika Serikat Dalam Perang Dagang Dengan China. *Diplomacy and Global Security Journal : Jurnal Mahasiswa Magister Hubungan Internasional*, *1*(1), 90–98. https://doi.org/10.36859/dgsj.v1i1.2862

Kementerian Komunikasi dan Informatika Republik Indonesia. (n.d.). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Retrieved from https://peraturan.bpk.go.id/Home/Details/38665/uu-no-11-tahun-2008

Sugiyono. (2019). *Metode Penelitian Kualitatif, Kuantitatif dan R&D* (Edisi ke-2). Bandung: Alfabeta.

Stallings, W. (2018). *Effective cybersecurity: a guide to using best practices and standards*. Addison-Wesley Professional.