Indonesian Journal of Interdisciplinary Research in Science and Technology (MARCOPOLO)
Vol. 3, No. 9, 2025 : 915 - 932

Cyber Leadership in the Digital Age: Building a Resilient Indonesian Defense in Cyberspace

Ansori[1]*, Kharis Ali [2], Tarsisius Susilo[3], Bungkus Hadisuseno[4], Cahyadi Amperawan[5]
Sekolah Staff dan Komando TNI
Corresponding Author: Ansori ansoridikregtni54@gmail.com

A R T I C L E I N F O

Keywords : Leadership, Digital, Defense, Indonesia

Received : 03 August 2025
Revised : 25 August 2025
Accepted: 27 September 2025

A B S T R A C T

Cyberspace has evolved into a new warfare domain, on par with land, sea, air, and space. The rapid development of digital technology has expanded the attack surface, making cyberspace an arena rife with vulnerabilities. The primary objective of this article is to analyze the urgency of cyber leadership as a strategic factor in building a resilient Indonesian defense in the digital era. The research methodology in this article uses a literature review approach by examining academic literature, policy documents, and official reports relevant to the issue of cyber leadership and digital defense. Cyber leadership in the digital era is a strategic necessity for Indonesia in facing increasingly complex cyber threats, whether in the form of technical attacks, digital espionage, disinformation, or threats to critical infrastructure. Effective cyber leadership must emphasize adaptive and transformational leadership, capable of responding to threat dynamics while providing a long-term vision for the development of Indonesia's digital sovereignty.

Cyber Leadership di Era Digital: Membangun Pertahanan Indonesia yang Tangguh di Dunia Maya

Ansori[1]*, Kharis Ali [2], Tarsisius Susilo[3], Bungkus Hadisuseno[4], Cahyadi Amperawan[5]
Sekolah Staff dan Komando TNI
Corresponding Author: Ansori ansoridikregtni54@gmail.com

A R T I C L E I N F O

Kata Kunci: Leadership, Digital, Pertahanan, Indonesia

Received : 03 Agustus 2025
Revised : 25 Agustus 2025
Accepted: 27 September 2025

A B S T R A K

Ruang siber telah berkembang menjadi domain peperangan baru yang setara dengan darat, laut, udara, dan ruang angkasa. Perkembangan teknologi digital yang sangat cepat telah memperluas permukaan serangan, menjadikan ruang siber sebagai arena yang sarat dengan kerentanan. Tujuan utama artikel ini adalah menganalisis urgensi cyber leadership sebagai faktor strategis dalam membangun pertahanan Indonesia yang tangguh di era digital. Metodologi penelitian dalam artikel ini menggunakan pendekatan studi pustaka (literature review) dengan menelaah literatur akademik, dokumen kebijakan, serta laporan resmi yang relevan dengan isu kepemimpinan siber dan pertahanan digital. Cyber leadership di era digital merupakan kebutuhan strategis bagi Indonesia dalam menghadapi ancaman siber yang semakin kompleks, baik dalam bentuk serangan teknis, spionase digital, disinformasi, maupun ancaman terhadap infrastruktur kritis. Cyber leadership yang efektif harus menekankan pada kepemimpinan adaptif dan transformasional, yang mampu merespons dinamika ancaman sekaligus memberikan visi jangka panjang bagi pembangunan kedaulatan digital Indonesia.

PENDAHULUAN

Transformasi digital telah menjadi ciri utama perkembangan global di abad ke-21. Percepatan digitalisasi dalam berbagai sektor kehidupan, mulai dari pemerintahan, ekonomi, pendidikan hingga pertahanan, telah menempatkan teknologi informasi dan komunikasi sebagai infrastruktur strategis yang menopang aktivitas masyarakat modern. Di Indonesia, digitalisasi semakin dipercepat oleh tingginya penetrasi internet, adopsi layanan digital, dan kebijakan pemerintah yang mendorong pembangunan ekonomi digital nasional. Menurut laporan *We Are Social* dan Kepios tahun 2024, jumlah pengguna internet di Indonesia mencapai lebih dari 213 juta orang, menempatkan Indonesia sebagai salah satu pasar digital terbesar di dunia (Kepios, 2024). Kondisi ini menunjukkan bahwa infrastruktur digital bukan lagi sekadar pendukung, melainkan fondasi utama dalam aktivitas sosial, ekonomi, dan pertahanan negara.

Ketergantungan terhadap infrastruktur siber membawa implikasi ganda: di satu sisi mendorong efisiensi dan produktivitas, namun di sisi lain meningkatkan kerentanan terhadap ancaman siber. Serangan ransomware, kebocoran data, hingga manipulasi informasi telah menjadi isu yang mengemuka dalam lima tahun terakhir. Badan Siber dan Sandi Negara (BSSN) mencatat lebih dari 361 juta upaya serangan siber di Indonesia sepanjang tahun 2023, dengan mayoritas menyasar sektor pemerintahan, keuangan, dan infrastruktur kritis (BSSN, 2023). Tingginya angka ini menegaskan bahwa transformasi digital tanpa strategi keamanan yang memadai berpotensi melemahkan stabilitas nasional.

Dalam konteks pertahanan, ruang siber telah berkembang menjadi domain peperangan baru yang setara dengan darat, laut, udara, dan ruang angkasa. Konsep cyber power yang dikemukakan Nye, menegaskan bahwa kekuatan sebuah negara tidak hanya ditentukan oleh kapabilitas militernya secara konvensional, tetapi juga oleh kapasitasnya dalam mengelola, melindungi, dan memanfaatkan ruang siber (Nye, 2022). Indonesia sebagai negara dengan populasi besar dan posisi geopolitik strategis di kawasan Indo-Pasifik, menghadapi tantangan signifikan dalam memastikan kedaulatan digitalnya tetap terjaga. Oleh karena itu, kepemimpinan dalam ranah siber (cyber leadership) menjadi elemen penting untuk mengintegrasikan kebijakan, teknologi, dan sumber daya manusia dalam menghadapi spektrum ancaman baru.

Lebih jauh, cyber leadership tidak hanya menyoal kemampuan teknis dalam mengendalikan infrastruktur digital, tetapi juga kepiawaian dalam membangun budaya keamanan, koordinasi lintas sektor, dan penguatan literasi digital di masyarakat. Model kepemimpinan siber yang adaptif, kolaboratif, dan visioner diperlukan agar Indonesia mampu memperkuat daya tahan di dunia maya. Tanpa kepemimpinan yang kuat, transformasi digital yang masif justru berisiko menjerumuskan Indonesia ke dalam kerentanan sistemik. Oleh sebab itu, membangun pertahanan Indonesia yang tangguh di dunia maya bukan hanya persoalan teknologi, melainkan juga strategi kepemimpinan dalam mengelola risiko dan peluang di era digital (Singer & Friedman, 2019).

Ancaman dunia maya saat ini telah berkembang menjadi salah satu isu keamanan paling signifikan dalam konteks global maupun nasional. Perkembangan teknologi digital yang sangat cepat telah memperluas permukaan serangan (attack surface), menjadikan ruang siber sebagai arena yang sarat dengan kerentanan. Serangan siber tidak lagi terbatas pada individu atau kelompok kecil, melainkan melibatkan aktor negara maupun non-negara dengan motivasi politik, ekonomi, maupun ideologis. Menurut laporan Cybersecurity Ventures (2023), kerugian ekonomi global akibat serangan siber diperkirakan mencapai USD 10,5 triliun pada 2025, menjadikannya ancaman keamanan yang bersifat sistemik dan lintas batas (Ventures, 2023). Hal ini memperlihatkan bahwa serangan siber bukan hanya masalah teknis, melainkan persoalan strategis yang dapat melemahkan stabilitas negara.

Salah satu bentuk ancaman paling menonjol adalah spionase digital, di mana informasi sensitif dari institusi pemerintah, militer, maupun perusahaan swasta dicuri untuk kepentingan strategis. Fenomena ini semakin marak seiring meningkatnya ketergantungan pada sistem penyimpanan data berbasis cloud dan perangkat Internet of Things (IoT). Penelitian Rid (2020) menegaskan bahwa spionase digital telah menjadi instrumen utama dalam kompetisi geopolitik modern, karena informasi kini merupakan aset strategis yang setara nilainya dengan sumber daya alam atau kekuatan militer (Rid, 2020). Dalam konteks Indonesia, kebocoran data yang berulang kali terjadi menunjukkan lemahnya mekanisme perlindungan data nasional, sehingga memperbesar peluang terjadinya eksploitasi oleh pihak eksternal.

Selain itu, disinformasi dan manipulasi opini publik di ruang digital menjadi ancaman non-teknis yang berdampak langsung terhadap kohesi sosial dan stabilitas politik. Disinformasi dapat dimanfaatkan sebagai senjata dalam perang informasi (information warfare), yang berpotensi menciptakan polarisasi, menurunkan kepercayaan masyarakat terhadap institusi negara, serta melemahkan legitimasi pemerintah. Menurut Bradshaw dan Howard (2019), kampanye disinformasi telah digunakan secara sistematis oleh berbagai aktor politik di lebih dari 70 negara, termasuk Indonesia, untuk mempengaruhi persepsi publik dan hasil politik (Bradshaw & Howard, 2019). Hal ini menegaskan bahwa ancaman dunia maya tidak hanya berdimensi teknis, tetapi juga psikologis dan sosial.

Ancaman yang tidak kalah serius adalah serangan terhadap infrastruktur kritis seperti sistem energi, transportasi, telekomunikasi, dan layanan keuangan. Infrastruktur ini menjadi tulang punggung kehidupan masyarakat sekaligus penopang pertahanan negara. Serangan siber terhadap infrastruktur kritis dapat menimbulkan gangguan luas, bahkan krisis nasional. Studi Carrapico dan Farrand (2021) menekankan bahwa serangan semacam ini berpotensi menimbulkan cascade effect, di mana kegagalan pada satu sektor memicu keruntuhan di sektor lain (Carrapico & Farrand, 2021). Indonesia sebagai negara dengan tingkat digitalisasi yang terus meningkat, termasuk pada sistem kelistrikan dan transportasi, sangat rentan terhadap ancaman ini. Oleh karena itu, membangun kepemimpinan siber yang kuat menjadi krusial untuk

merancang strategi mitigasi, meningkatkan ketahanan digital, serta memastikan pertahanan nasional yang tangguh di era digital.

Posisi Indonesia dalam indeks global keamanan siber menunjukkan adanya perkembangan positif, namun tetap menyisakan tantangan mendasar dalam membangun kedaulatan digital. Berdasarkan laporan Global Cybersecurity Index (GCI) yang diterbitkan oleh International Telecommunication Union (ITU) pada 2021, Indonesia menempati peringkat ke-24 dari 194 negara dengan skor 94,88, naik signifikan dari peringkat 41 pada 2018 (ITU, 2021). Peningkatan ini mencerminkan kemajuan dalam regulasi, kerangka kerja kelembagaan, serta implementasi strategi keamanan siber nasional melalui peran Badan Siber dan Sandi Negara (BSSN). Meski demikian, jika dibandingkan dengan negara-negara maju seperti Amerika Serikat, Singapura, dan Inggris yang selalu berada di lima besar, Indonesia masih menghadapi kesenjangan kapabilitas baik dalam aspek teknis maupun koordinasi kebijakan lintas sektor.

Tantangan utama dalam membangun kedaulatan digital Indonesia terletak pada ketergantungan terhadap teknologi asing. Infrastruktur digital nasional, termasuk perangkat keras, perangkat lunak, dan layanan cloud, sebagian besar masih mengandalkan produk dan layanan dari luar negeri. Kondisi ini menimbulkan kerentanan strategis karena membuka peluang terjadinya supply chain attack atau intervensi teknologi oleh aktor eksternal. Dominasi teknologi asing dalam infrastruktur siber suatu negara berpotensi melemahkan kedaulatan digital karena menurunkan kontrol penuh negara terhadap data dan sistem vitalnya (Timmers, 2022). Hal ini menjadi dilema bagi Indonesia yang sedang mendorong transformasi digital secara cepat, namun belum mampu menciptakan ekosistem teknologi domestik yang kuat.

Selain itu, keterbatasan sumber daya manusia siber yang kompeten masih menjadi hambatan serius. Data BSSN (2023) menunjukkan bahwa Indonesia membutuhkan lebih dari 100.000 tenaga ahli siber untuk memenuhi kebutuhan keamanan digital nasional, sementara kapasitas perguruan tinggi dan lembaga pelatihan belum sepenuhnya mampu menyuplai tenaga kerja dengan keterampilan setara standar global. Kesenjangan literasi digital di masyarakat juga memperburuk kondisi ini, karena rendahnya kesadaran akan praktik keamanan digital menjadikan pengguna internet mudah terekspos terhadap serangan phishing, malware, atau manipulasi informasi. Hal ini menegaskan bahwa pembangunan kedaulatan digital bukan hanya persoalan infrastruktur, tetapi juga penguatan kompetensi manusia sebagai faktor penentu utama.

Lebih jauh, aspek geopolitik turut memengaruhi upaya Indonesia dalam memperkuat pertahanan siber. Kawasan Indo-Pasifik kini menjadi arena persaingan kekuatan besar, di mana isu keamanan siber kerap digunakan sebagai instrumen diplomasi maupun kompetisi strategis. Indonesia dituntut untuk mampu memainkan peran aktif dalam tata kelola siber global (global cyber governance), sekaligus memastikan bahwa kepentingan nasional tidak terpinggirkan. Dalam konteks inilah cyber leadership menjadi kunci pemimpin siber yang visioner, adaptif, dan kolaboratif diperlukan untuk mengintegrasikan kebijakan nasional, memperkuat posisi Indonesia dalam forum internasional,

dan membangun kedaulatan digital yang tangguh di tengah dinamika global yang penuh ketidakpastian (Susanti & Fitriani, 2022).

Rumusan masalah utama dalam kajian ini adalah Mengapa cyber leadership menjadi aspek strategis dalam memperkuat pertahanan Indonesia di era digital?. Berangkat dari kenyataan bahwa transformasi digital telah menciptakan ketergantungan yang tinggi terhadap infrastruktur siber, sekaligus membuka ruang bagi munculnya ancaman multidimensional. Serangan siber, spionase digital, manipulasi informasi, hingga serangan terhadap infrastruktur kritis menunjukkan bahwa ruang siber telah menjadi domain strategis yang memengaruhi kedaulatan negara. Dalam situasi ini, pertanyaan mendasar yang muncul adalah bagaimana Indonesia dapat merespons ancaman tersebut secara efektif? Jawaban atas pertanyaan ini tidak hanya bergantung pada kecanggihan teknologi, tetapi juga pada adanya kepemimpinan siber (cyber leadership) yang mampu mengintegrasikan strategi nasional, membangun koordinasi lintas sektor, serta memperkuat kesadaran masyarakat. Seperti ditegaskan Nye (2022), cyber power suatu negara tidak semata-mata ditentukan oleh infrastruktur teknis, tetapi juga oleh kapasitas kepemimpinan dalam mengelola sumber daya informasi dan membangun legitimasi politik di ruang digital (Nye, 2022).

Dalam konteks Indonesia, cyber leadership menjadi aspek strategis karena tantangan pertahanan siber bersifat lintas sektoral, kompleks, dan terus berkembang. Kebijakan keamanan siber Indonesia masih menghadapi keterbatasan koordinasi, tumpang tindih regulasi, dan lemahnya integrasi antar lembaga (Susanti & Fitriani, 2022). Hal ini menegaskan pentingnya sosok atau model kepemimpinan siber yang visioner, adaptif, dan kolaboratif dalam menyatukan kepentingan militer, pemerintah, industri, akademisi, dan masyarakat sipil. Tanpa kepemimpinan yang mampu menjembatani kompleksitas tersebut, upaya membangun pertahanan digital hanya akan berjalan parsial dan tidak berkelanjutan. Dengan demikian, pertanyaan "mengapa cyber leadership menjadi aspek strategis" tidak hanya berfungsi sebagai pijakan akademik, tetapi juga sebagai kerangka analisis untuk merumuskan strategi pertahanan Indonesia yang tangguh di dunia maya.

Tujuan utama artikel ini adalah menganalisis urgensi cyber leadership sebagai faktor strategis dalam membangun pertahanan Indonesia yang tangguh di era digital. Artikel ini berupaya menguraikan secara konseptual hubungan antara kepemimpinan siber, transformasi digital, dan kebutuhan pertahanan nasional, serta menekankan bagaimana cyber leadership dapat menjadi instrumen kunci dalam menghadapi ancaman dunia maya yang semakin kompleks. Dengan merujuk pada praktik global dan membandingkannya dengan kondisi aktual di Indonesia, artikel ini diharapkan mampu memberikan gambaran teoretis dan praktis mengenai model kepemimpinan siber yang sesuai dengan kebutuhan Indonesia. Dengan demikian, penelitian ini bertujuan tidak hanya memperkuat pemahaman akademik tentang konsep kepemimpinan dalam ranah digital, tetapi juga memberikan landasan untuk merumuskan strategi nasional yang lebih komprehensif.

Kontribusi artikel ini terletak pada dua ranah utama, yakni akademik dan kebijakan. Pada ranah akademik, artikel ini memperkaya diskursus tentang

keamanan siber dengan memasukkan dimensi kepemimpinan sebagai variabel penting, sesuatu yang masih jarang dibahas dalam literatur mengenai pertahanan digital di Indonesia. Artikel ini juga memberikan kerangka analisis yang dapat digunakan untuk penelitian lebih lanjut mengenai hubungan antara cyber leadership, tata kelola siber, dan ketahanan nasional. Pada ranah kebijakan, artikel ini diharapkan dapat menjadi masukan bagi pemerintah, khususnya Kementerian Pertahanan, BSSN, serta lembaga terkait lainnya, dalam merumuskan strategi pertahanan siber yang lebih terintegrasi dan berorientasi pada kedaulatan digital. Dengan menekankan peran kepemimpinan siber, artikel ini berkontribusi pada penguatan kebijakan pertahanan nasional yang adaptif terhadap dinamika ancaman global serta responsif terhadap kebutuhan domestik.

TINJAUAN PUSTAKA

Kajian mengenai keamanan siber dalam literatur internasional menempatkan ruang siber sebagai domain strategis yang semakin penting dalam pertahanan nasional. Nye (2022) memperkenalkan konsep cyber power, yang menekankan bahwa kekuatan suatu negara di era digital tidak hanya bergantung pada infrastruktur teknologinya, tetapi juga pada kemampuan untuk mengelola, melindungi, dan memanfaatkan informasi (Nye, 2022). Dalam perspektif ini, keamanan siber dipandang sebagai instrumen kekuasaan yang memengaruhi kedaulatan, stabilitas, dan diplomasi. Pandangan ini menegaskan bahwa penguatan pertahanan digital bukan sekadar urusan teknis, melainkan bagian integral dari strategi politik dan pertahanan negara.

Seiring berkembangnya konsep tersebut, muncul gagasan cyber leadership sebagai variabel penting dalam mengelola keamanan digital. Menurut Kellerman (2020), cyber leadership merujuk pada kemampuan pemimpin untuk mengintegrasikan teknologi digital dengan strategi kepemimpinan, menciptakan visi yang jelas, serta membangun kolaborasi lintas sektor dalam menghadapi risiko siber (Kellerman, 2020). Kepemimpinan ini berbeda dengan model tradisional karena menuntut kemampuan adaptasi cepat terhadap perubahan teknologi dan dinamika ancaman. Dalam konteks pertahanan, cyber leadership mencakup dimensi strategis (penentuan kebijakan dan arah nasional), teknis (pemahaman atas infrastruktur dan mekanisme keamanan), serta sosial (membangun literasi dan kesadaran masyarakat).

Studi internasional menunjukkan bahwa negara-negara yang berhasil membangun ketahanan siber biasanya memiliki model kepemimpinan yang kuat dalam domain digital. Estonia, misalnya, berhasil mengembangkan sistem pertahanan siber nasional pasca serangan besar pada 2007 dengan membangun kepemimpinan yang terkoordinasi antara pemerintah, militer, akademisi, dan sektor swasta (Madise & Martens, 2021). Singapura juga menjadi contoh di Asia Tenggara, di mana strategi pertahanan sibernya didukung oleh kepemimpinan visioner yang menempatkan keamanan digital sebagai prioritas nasional (Chong, 2020). Studi kasus ini memperlihatkan bahwa peran kepemimpinan menjadi kunci dalam menyinergikan berbagai aktor serta memastikan keberlanjutan kebijakan siber.

Dalam konteks Indonesia, kajian akademik menegaskan bahwa kebijakan keamanan siber masih menghadapi kendala dalam koordinasi antar lembaga dan keterbatasan kapasitas teknis. Fitriani (2021) dan Susanti & Fitriani (2022) mencatat bahwa meskipun Indonesia telah menunjukkan kemajuan melalui pembentukan BSSN dan peningkatan peringkat dalam Global Cybersecurity Index, tantangan dalam membangun kedaulatan digital masih besar. Rendahnya literasi digital, ketergantungan pada teknologi asing, serta lemahnya integrasi kebijakan menuntut adanya model kepemimpinan yang lebih adaptif dan inklusif. Dengan demikian, literatur yang ada menunjukkan kesenjangan kajian: peran kepemimpinan siber dalam konteks pertahanan Indonesia masih belum banyak dieksplorasi secara mendalam. Artikel ini berusaha mengisi celah tersebut dengan menganalisis cyber leadership sebagai aspek strategis dalam memperkuat pertahanan nasional di era digital.

METODOLOGI

Metodologi penelitian dalam artikel ini menggunakan pendekatan studi pustaka (literature review) dengan menelaah secara kritis berbagai literatur akademik, dokumen kebijakan, serta laporan resmi yang relevan dengan isu kepemimpinan siber dan pertahanan digital. Sumber data utama mencakup regulasi nasional seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), kebijakan Badan Siber dan Sandi Negara (BSSN), serta dokumen strategis Kementerian Pertahanan, yang kemudian dikomparasikan dengan laporan internasional dari lembaga seperti International Telecommunication Union (ITU), NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), dan studi kasus dari negara-negara yang berhasil membangun ketangguhan siber. Analisis dilakukan dengan pendekatan analisis isi untuk mengidentifikasi tema, pola, serta gap dalam kebijakan nasional, dan dilanjutkan dengan analisis komparatif guna menilai kesesuaian serta potensi adopsi praktik terbaik internasional dalam konteks Indonesia. Dengan metode ini, penelitian diharapkan dapat menyajikan pemahaman komprehensif mengenai urgensi cyber leadership sekaligus memberikan rekomendasi strategis yang berbasis bukti akademik.

HASIL PENELITIAN

Langkah – langkah yang dilakukan dalam penelitian ini:

1. **Identifikasi masalah dan perumusan pertanyaan penelitian** Menentukan fokus kajian melalui telaah pustaka terkini untuk menemukan *research gap* yang relevan.
2. **Perancangan metode penelitian** Menetapkan desain, variabel, teknik pengumpulan data, dan strategi analisis yang sesuai untuk menjamin validitas dan reliabilitas.
3. **Pengumpulan data** Melaksanakan prosedur pengumpulan data (survei, wawancara, eksperimen, atau studi dokumenter) dengan memperhatikan prinsip etika penelitian.
4. **Analisis data** Mengolah dan menafsirkan data menggunakan teknik analisis kualitatif, kuantitatif, atau campuran untuk menemukan pola dan hubungan yang signifikan.

5. **Penarikan kesimpulan dan pelaporan** Menyajikan hasil penelitian, mengaitkannya dengan teori, menguraikan implikasi, serta memberikan rekomendasi dan batasan penelitian.

PEMBAHASAN

Dinamika Ancaman Siber di Indonesia

Ruang ancaman siber saat ini ditandai oleh eskalasi kuantitatif dan kualitatif: selain peningkatan frekuensi serangan, teknik yang digunakan menjadi lebih terotomatisasi, terstandardisasi (sebagai layanan), dan terfokus pada eksfiltrasi data bernilai tinggi. Laporan-laporan ancaman internasional menegaskan pergeseran ini *ransomware as a service, phishing as a service,* dan profesionalisasi kelompok penjahat siber mengubah karakter ancaman dari opportunistic ke targeted, sementara aktor negara memanfaatkan kapabilitas advanced persistent threats (APT) untuk spionase dan gangguan operasi. Konsekuensinya, kemampuan nasional untuk melakukan deteksi cepat, berbagi intelijen kontekstual, serta menegakkan mitigasi berbasis bukti menjadi determinan utama tingkat kerentanan negara.

Dalam bingkai tipologi ancaman, empat kategori menonjol secara konsisten di data global dan regional: serangan ransomware yang mengunci atau mengancam publikasi data; serangan berbasis rekayasa sosial seperti phishing dan business email compromise; eksfiltrasi melalui titik-titik lemah dalam rantai pasok perangkat lunak dan jasa (supply-chain compromise); serta serangan terhadap sistem operasi industri dan kontrol (OT/ICS) yang memengaruhi layanan kritis. Pola supply-chain attacks yang terobservasi baru-baru ini (termasuk operasi yang memanfaatkan vendor pihak ketiga) menambah dimensi risiko strategis karena kompromi satu vendor dapat menyebar ke banyak entitas. Mitigasi efektif terhadap pola-pola ini menuntut kebijakan keamanan yang memasukkan pengelolaan risiko rantai pasok sebagai bagian tak terpisahkan dari arsitektur nasional.

Gambaran empiris untuk Indonesia memperlihatkan eksposur nyata: Badan Siber dan Sandi Negara (BSSN) melaporkan jumlah anomali trafik yang sangat besar pada 2023 angka yang diterjemahkan media sebagai ratusan juta upaya serangan/anomali pada periode tertentu yang mencerminkan tingginya volume dan frekuensi probe terhadap aset-aset domestik. Statistik ini bukan hanya angka; ia mengindikasikan lonjakan percobaan kompromi pada berbagai layer (aplikasi publik, API, layanan backend) sehingga menuntut peningkatan kapasitas monitoring serta pemrosesan insiden pada skala nasional. Data ini juga mempertegas bahwa ancaman bersifat kontinu dan memerlukan pendekatan berkelanjutan, bukan respons ad-hoc.

Serangan berlapis terhadap infrastruktur pemerintah pada paruh pertama 2024 memperlihatkan konsekuensi praktis dari kerentanan struktural: insiden ransomware yang memengaruhi fasilitas pusat data pemerintah menyebabkan gangguan layanan publik (termasuk imigrasi dan layanan bandara), memicu perintah audit oleh pimpinan negara dan evaluasi kebijakan backup serta kontinuitas layanan. Kasus ini memperjelas dua hal: pertama, bahwa konsekuensi serangan bisa berskala nasional; kedua, bahwa kelemahan tata

kelola, inventaris aset, dan kebijakan cadangan data memainkan peran kunci dalam memperbesar dampak insiden.

Analisis sektoral menunjukkan pola kerentanan yang berbeda-beda. Sektor publik sering terjebak pada sistem warisan (legacy), integrasi yang tidak konsisten antar-instansi, dan anggaran pemeliharaan yang terbatas sehingga patching dan backup tidak selalu terjamin; sektor swasta—terutama UKM dan lembaga keuangan kecil—mengalami tekanan biaya sehingga adopsi praktik keamanan dasar (MFA, segmentasi jaringan, enkripsi backup) rendah; sementara institusi pertahanan menghadapi masalah interoperabilitas sistem C3I (command, control, communication, intelligence) dan permukaan serangan pada subsistem OT yang mengontrol aset fisik, di mana kompromi dapat berdampak pada operasi militer dan keselamatan. Untuk masing-masing sektor diperlukan paket kebijakan yang disesuaikan: repositori aset & katalog risiko untuk publik, insentif regulatif dan pembiayaan keamanan untuk swasta, serta protokol hardening dan isolasi jaringan untuk entitas militer.

Ancaman non-teknis terutama disinformasi dan manipulasi informasi memperbesar risiko strategis dengan cara yang berbeda: ia menurunkan kepercayaan publik, memecah kohesi sosial, dan merusak efektivitas respons publik pada krisis. Di Indonesia, pola disinformasi yang terorganisir di platform sosial telah menjadi masalah struktural selama siklus pemilu dan isu-isu publik penting; ini menuntut penggabungan strategi kontra-disinformasi yang melibatkan upaya platform, literasi publik, serta prosedur klarifikasi resmi cepat dari institusi negara. Langkah-langkah semacam ini harus dioperasionalisasikan sebagai bagian dari kesiapsiagaan nasional, bukan semata-mata respons komunikasi publik.

Agar penilaian kemajuan bisa objektif, negara perlu indikator operasional dan kapabilitas yang jelas. Indikator operasional minimum meliputi Mean Time To Detect (MTTD) dan Mean Time To Respond (MTTR) untuk insiden berisiko tinggi; persentase titik akhir yang terkelola dan dipatch dalam jangka waktu tertentu; rasio aset kritis yang lulus audit keamanan; serta jumlah insiden berakibat sistemik per 10.000 aset. Indikator kapabilitas mencakup jumlah tenaga bersertifikat per 100.000 penduduk, ketersediaan SOC/CSIRT sektoral, serta skor Global Cybersecurity Index (GCI) sebagai tolok ukur komitmen nasional.

Solusi yang komprehensif harus bersifat multi-dimensional: regulasi yang mencerabut fragmentasi kelembagaan dan mewajibkan CISO berwenang di level kementerian/lembaga, investasi berkelanjutan pada SOC/CSIRT dan pusat threat-intelligence nasional, serta program literasi digital nasional yang terukur untuk mengurangi dampak disinformasi. Secara teknis, adopsi prinsip zero-trust, skema manajemen risiko rantai pasok (vendor security assessments, SBOM), serta kebijakan cadangan terdistribusi untuk data pemerintah adalah langkah prioritas. Di samping itu, pembangunan kapasitas talenta melalui pendidikan formal, pelatihan praktis, dan skema retensi talenta strategis adalah investasi jangka panjang yang harus diberi target kuantitatif. Implementasi solusi-solusi ini perlu diiringi mekanisme pemantauan KPI nasional yang transparan dan audit independen berkala agar kemajuan dapat diukur dan dipertanggungjawabkan.

Dimensi	Indikator Utama	Target Ideal 2025-2030
Deteksi	MTTD insiden kritis	< 24 jam
Respons	MTTR insiden kritis	< 72 jam
Kepatuhan Teknis	Persentase endpoint terpatch	≥ 90%
Audit Keamanan	Rasio aset kritis lulus audit	≥ 85%
Kapasitas SDM	Tenaga bersertifikasi (per 100k penduduk)	≥ 150
Infrastruktur SOC	Jumlah SOC/CSIRT sektoral aktif	1 per sektor strategis
Indeks Global	Posisi GCI	Top 25 dunia

Solusi Strategis	Indikator Keberhasilan	Otoritas Pelaksana
Penunjukan CISO di tiap K/L	% K/L dengan CISO aktif	KemenPAN-RB, BSSN
SOC/CSIRT Nasional & Sektoral	Jumlah SOC/CSIRT beroperasi	BSSN, Kemenkominfo, sektor industri
Literasi Digital Nasional	Persentase masyarakat melek keamanan digital	Kemendikbudristek, Kominfo
Kebijakan *Zero Trust*	Implementasi ZTA pada 80% layanan publik	Kemenkominfo, BSSN
Manajemen Risiko Rantai Pasok	Vendor bersertifikat keamanan ≥ 70%	LKPP, BSSN
Talenta Siber Nasional	Jumlah tenaga bersertifikasi meningkat 20% per tahun	BSSN, Perguruan Tinggi
Diplomasi Siber	Partisipasi aktif forum global / perjanjian bilateral	Kemlu, BSSN

Urgensi Cyber Leadership

Kepemimpinan siber atau cyber leadership menjadi elemen strategis dalam memastikan ketahanan nasional di ranah digital karena ia tidak hanya terkait dengan kemampuan teknis, melainkan juga kapasitas untuk menumbuhkan visi, arah, dan koordinasi lintas sektor. Dalam konteks Indonesia, peran kepemimpinan ini sangat penting untuk mengatasi fragmentasi kelembagaan dan kesenjangan sumber daya manusia yang selama ini menjadi kendala. Seorang cyber leader harus mampu merancang strategi jangka panjang yang berlandaskan pada integrasi kepentingan nasional, sambil menjamin bahwa setiap kebijakan yang diambil berbasis pada prinsip-prinsip keberlanjutan, inklusivitas, dan adaptabilitas terhadap dinamika ancaman global.

Salah satu urgensi utama cyber leadership adalah pembangunan budaya keamanan siber nasional yang menyeluruh. Budaya ini mencakup kesadaran individu, etika organisasi, serta kerangka regulasi yang konsisten, sehingga setiap lapisan masyarakat memahami perannya dalam menjaga ruang digital. Tanpa kepemimpinan yang visioner, kesadaran ini sulit diwujudkan karena kebijakan sering kali berhenti pada tingkat teknis tanpa menyentuh aspek perilaku dan kesadaran kolektif. Cyber leader berfungsi sebagai penggerak transformasi sosial—menjadikan keamanan digital bukan sekadar urusan teknis,

tetapi nilai bersama yang diinternalisasi ke dalam kehidupan sehari-hari warga negara.

Lebih jauh, cyber leadership memainkan peran sebagai jembatan antara tiga pilar utama: teknologi, kebijakan, dan sumber daya manusia. Dari sisi teknologi, kepemimpinan harus memastikan bahwa adopsi inovasi (AI, 5G, cloud, dan IoT) berjalan seiring dengan kerangka keamanan yang memadai. Dari sisi kebijakan, cyber leader harus mampu menerjemahkan dinamika teknis yang kompleks ke dalam regulasi yang jelas, mudah dipatuhi, serta responsif terhadap perkembangan global. Dari sisi sumber daya manusia, kepemimpinan diperlukan untuk mengatasi kesenjangan talenta melalui strategi rekrutmen, pelatihan, dan retensi yang terarah. Sinergi ketiga aspek ini menentukan seberapa tangguh ekosistem digital Indonesia dalam menghadapi ancaman.

Dalam praktiknya, kepemimpinan siber tidak bisa dilepaskan dari diplomasi strategis di arena internasional. Indonesia membutuhkan figur dan institusi kepemimpinan yang mampu memposisikan negara sebagai aktor aktif dalam perumusan norma global, perjanjian bilateral, dan kerjasama multilateral terkait keamanan siber. Tanpa kepemimpinan yang memiliki legitimasi dan kapasitas diplomasi, Indonesia akan tetap berada pada posisi defensif, bergantung pada kebijakan negara lain, dan rentan kehilangan kedaulatan digitalnya. Oleh karena itu, cyber leadership harus dibangun dengan perspektif ganda: penguatan domestik sekaligus proyeksi internasional.

Indikator penilaian terhadap efektivitas cyber leadership dapat diturunkan dari dimensi internal dan eksternal. Dimensi internal mencakup tingkat partisipasi masyarakat dalam program literasi siber, integrasi kebijakan antar-kementerian/lembaga, serta peningkatan jumlah tenaga kerja digital dengan keahlian keamanan. Dimensi eksternal dapat dilihat dari keterlibatan Indonesia dalam forum internasional, kontribusi dalam penyusunan standar global, serta posisi dalam indeks keamanan siber global. Indikator-indikator ini dapat digunakan untuk menilai apakah kepemimpinan yang dibangun benar-benar membawa dampak transformasional atau hanya simbolik.

Solusi strategis untuk memperkuat cyber leadership mencakup penguatan kapasitas institusional, penciptaan pusat kepemimpinan siber nasional (national cyber leadership center), dan program kaderisasi pemimpin siber lintas sektor. Program ini harus mencetak individu dengan keahlian multidisipliner—memahami teknologi, kebijakan, serta dinamika geopolitik. Selain itu, skema kolaborasi publik–swasta perlu diperluas sehingga kepemimpinan tidak hanya terkonsentrasi di pemerintahan, tetapi juga lahir dari sektor industri, akademisi, dan komunitas digital. Dengan demikian, cyber leadership dapat berfungsi sebagai katalis integrasi ekosistem keamanan siber Indonesia.

Dimensi	Indikator Utama	Target Ideal 2025–2030
Budaya Keamanan	Persentase masyarakat mengikuti program literasi siber	≥ 70%
Integrasi Kebijakan	Jumlah kebijakan lintas K/L yang terintegrasi	≥ 80%
SDM Keamanan	Tenaga kerja digital bersertifikasi keamanan	≥ 200 per 100k penduduk
Diplomasi Global	Partisipasi aktif dalam forum siber internasional	≥ 10 forum utama per tahun
Indeks Global	Peringkat Indonesia dalam GCI	Top 25 dunia

Solusi Strategis	Indikator Keberhasilan	Otoritas Pelaksana
Pembentukan *National Cyber Leadership Center*	Pusat operasional berfungsi pada 2026	BSSN, Kemenkominfo
Program Kaderisasi Pemimpin Siber	Jumlah lulusan per tahun ≥ 200	Kemendikbudristek, BSSN
Literasi Siber Nasional	Partisipasi masyarakat ≥ 70%	Kemendikbudristek, Kominfo
Diplomasi Siber Proaktif	Partisipasi aktif & kontribusi dalam ≥ 10 forum global	Kemlu, BSSN
Kolaborasi Publik–Swasta	Jumlah MoU/kerjasama strategis ≥ 50	BSSN, Asosiasi Industri TI

Karakteristik Cyber Leadership yang Relevan untuk Indonesia

Kepemimpinan siber di Indonesia harus memiliki karakter visioner yang mampu mengarahkan transformasi digital nasional ke arah kemandirian dan ketahanan. Seorang pemimpin siber visioner bukan hanya fokus pada mitigasi ancaman, tetapi juga memiliki imajinasi strategis untuk memproyeksikan masa depan ekosistem digital Indonesia dalam 10–20 tahun mendatang. Hal ini mencakup kemampuan membaca tren global seperti kecerdasan buatan, quantum computing, dan geopolitik siber, serta mengintegrasikannya dengan kebutuhan nasional. Tanpa visi jangka panjang, kebijakan siber cenderung reaktif dan sporadis, sehingga sulit membangun kedaulatan digital yang berkelanjutan.

Karakter kedua yang penting adalah kemampuan berkoordinasi lintas sektor. Ruang siber tidak mengenal batas administratif seperti dunia fisik, sehingga pengelolaannya tidak bisa hanya mengandalkan pemerintah atau militer. Pemimpin siber Indonesia harus mampu menjembatani kepentingan antara pemerintah, sektor pertahanan, industri teknologi, akademisi, hingga masyarakat sipil. Kolaborasi multipihak ini menciptakan ecosystem of trust yang memungkinkan informasi mengalir lebih cepat, respons ancaman lebih efisien, serta inovasi lebih mudah diadopsi. Koordinasi lintas sektor juga menjadi kunci dalam mengatasi fragmentasi kebijakan yang sering kali melemahkan respons negara terhadap insiden siber.

Karakter ketiga adalah responsivitas terhadap dinamika ancaman yang cepat berubah. Serangan siber berkembang dengan kecepatan yang jauh lebih tinggi dibandingkan ancaman konvensional. Oleh karena itu, cyber leadership harus bersifat adaptif, memanfaatkan intelijen real-time, serta menerapkan prinsip agile governance dalam kebijakan. Respons yang lambat atau birokratis hanya akan memperbesar kerugian ekonomi, reputasi, maupun stabilitas nasional. Seorang cyber leader yang responsif tidak hanya cepat bereaksi terhadap insiden, tetapi juga mampu mengantisipasi pola ancaman baru melalui pendekatan prediktif berbasis data dan kecerdasan buatan.

Karakter keempat adalah kemampuan menumbuhkan literasi digital dan ketahanan sosial. Kepemimpinan siber tidak berhenti pada level teknis dan kebijakan, tetapi juga harus menjangkau ranah sosial. Literasi digital masyarakat menjadi fondasi pertahanan siber karena ancaman seperti disinformasi dan manipulasi psikologis hanya dapat diatasi dengan kesadaran kolektif. Pemimpin siber yang efektif adalah mereka yang mampu mendorong program literasi digital inklusif, memanfaatkan jalur pendidikan formal maupun komunitas lokal, serta menginternalisasikan budaya keamanan digital ke dalam kehidupan sehari-hari warga negara.

Dalam konteks Indonesia, keempat karakteristik ini harus diintegrasikan ke dalam model kepemimpinan yang khas, yang memperhatikan keragaman sosial-budaya dan dinamika politik domestik. Misalnya, visi transformasi digital harus memperhitungkan kesenjangan digital antarwilayah; koordinasi lintas sektor harus memperhatikan kerangka hukum yang jelas untuk pembagian peran; responsivitas harus mengatasi birokrasi yang lambat; dan literasi digital harus relevan dengan karakter masyarakat Indonesia yang beragam. Dengan demikian, cyber leadership Indonesia tidak hanya mengadopsi praktik global, tetapi juga menyesuaikannya dengan konteks lokal.

Indikator untuk menilai karakteristik cyber leadership dapat dibangun berdasarkan empat dimensi tadi. Visi dapat diukur melalui keberadaan strategi jangka panjang yang terpublikasi dan konsisten. Koordinasi lintas sektor dapat dievaluasi melalui jumlah mekanisme formal kolaborasi yang aktif berjalan. Responsivitas dapat dinilai melalui kecepatan deteksi dan respons insiden (MTTD/MTTR) serta efektivitas tim tanggap darurat siber nasional. Sementara literasi digital dapat diukur melalui tingkat partisipasi masyarakat dalam program literasi serta survei kesadaran publik mengenai keamanan digital.

Solusi komprehensif untuk mewujudkan karakteristik ini mencakup pembentukan national cyber leadership curriculum untuk mencetak pemimpin visioner, penguatan forum lintas sektor seperti cybersecurity roundtable, penggunaan AI dalam sistem deteksi ancaman nasional, serta integrasi program literasi digital ke dalam kurikulum pendidikan formal maupun non-formal. Pendekatan ini harus bersifat berlapis, dari level kebijakan hingga akar rumput, agar kepemimpinan siber benar-benar memiliki daya transformasional.

Karakteristik cyber leadership yang relevan untuk Indonesia harus dilihat sebagai satu kesatuan, bukan elemen yang terpisah. Visioner tanpa koordinasi akan kehilangan eksekusi; koordinasi tanpa responsivitas akan menghasilkan kebijakan lamban; responsivitas tanpa literasi sosial akan membuat masyarakat

tetap rentan; dan literasi tanpa visi akan berjalan tanpa arah. Oleh karena itu, pembentukan kepemimpinan siber Indonesia harus diarahkan pada model integratif yang menyatukan keempat karakteristik ini dalam satu kerangka strategis.

Strategi Penguatan Pertahanan Siber melalui Cyber Leadership

Integrasi kepemimpinan siber ke dalam doktrin pertahanan nasional harus menjadi titik awal strategis: Peraturan Presiden No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional (SKSN) dan Manajemen Krisis Siber menegaskan bahwa aspek governance, kesiapsiagaan, perlindungan infrastruktur, kemandirian kriptografi, dan kapasitas SDM adalah fokus nasional yang memerlukan otoritas koordinatif. Oleh karena itu, cyber leadership harus ditempatkan pada level doktrinal—bukan sebagai lampiran teknis—dengan mandat eksplisit untuk mengharmonisasikan kebijakan, prosedur operasi, dan rencana kontinjensi antar-kementerian/lembaga serta komponen pertahanan. Integrasi semacam ini memungkinkan pergeseran dari respons reaktif ke kesiapsiagaan yang diarahkan oleh komando strategis yang memahami implikasi geopolitik dan operasional di ranah siber (Peraturan Presiden No. 47/2023; BSSN).

Pengharmonisasian doktrin harus menggunakan kerangka manajemen risiko yang diakui internasional: NIST CSF 2.0, dengan penambahan fungsi Govern, menawarkan peta jalan praktis untuk memasukkan fungsi tata kelola (govern), identifikasi aset, proteksi, deteksi, respons, dan pemulihan ke dalam doktrin militer dan sipil. Doktrin yang terintegrasi perlu mengatur hubungan komando-kontrol (C2) untuk operasi siber, melampaui sekat sipil-militer sehingga kebijakan penggunaan efek siber, aturan keterlibatan, dan skenario eskalasi dikodifikasikan dengan jelas. Penggunaan NIST CSF 2.0 sebagai referensi taksonomi memungkinkan menetapkan KPI taktikal (MTTD/MTTR, tingkat patching, coverage SOC) yang dapat diadopsi lintas lembaga untuk memonitor efektivitas doktrin.

Operationalisasi doktrin menuntut pula pembaruan perangkat hukum dan prosedur manajemen krisis: penunjukan koordinator nasional untuk krisis siber (sebagaimana SKSN mendelegasikan peran koordinatif kepada BSSN), skenario tanggap darurat yang teruji lewat latihan bersama (tabletop, full-scale war games), dan transparansi peran di sektor kritis. Cyber leadership harus memimpin penyusunan playbook operasional—termasuk protokol eskalasi, interoperabilitas intelijen ancaman, dan perjanjian layanan darurat—agar saat krisis terjadi, keputusan strategis dapat diambil cepat, terukur, dan akuntabel. Praktik-praktik semacam ini selaras dengan pengalaman negara-negara yang mengintegrasikan domain siber ke doktrin pertahanan mereka.

Pembangunan sumber daya manusia (SDM) siber adalah pilar kedua yang membutuhkan kepemimpinan strategis. Kajian regional menunjukkan celah tenaga ahli yang signifikan di Asia Tenggara; Indonesia menghadapi kebutuhan besar untuk talenta yang tidak hanya teknis tetapi juga mampu memimpin (hybrid skills: teknis–manajerial–strategis). Cyber leadership harus memprioritaskan program pembelajaran seumur hidup: kurikulum formal di

perguruan tinggi, program sertifikasi profesional, jalur karier sipil–militer, serta skema insentif retensi untuk mengurangi "brain drain". Tanpa kebijakan HR yang diarahkan oleh pemimpin siber yang memahami kebutuhan strategis, kapasitas operasional nasional akan tetap terfragmentasi.

Implementasi pendidikan dan pelatihan harus bersifat praktik-berbasis dan terukur: model case-based learning dan latihan red-team/blue-team terbukti efektif untuk membentuk kemampuan pengambilan keputusan dalam konteks tekanan operasional. Sebagai solusi, cyber leadership perlu menginisiasi National Cyber Leadership Academy dan program magang/rotasi antar-institusi untuk mempercepat pematangan pemimpin siber. Selain itu, standar kompetensi nasional (aligned dengan kebijakan SKSN) dan skema akreditasi sertifikasi akan menormalkan metrik kualitas SDM sehingga indikator seperti jumlah tenaga bersertifikat per 100k penduduk atau jam latihan tahunan dapat dijadikan target kebijakan

Kolaborasi internasional dan diplomasi siber adalah dimensi strategis ketiga; Indonesia harus memanfaatkan diplomasi untuk akses intelijen ancaman, kerjasama capacity building, dan keterlibatan dalam penetapan norma internasional. Praktik diplomasi siber mencakup perjanjian bilateral untuk pertukaran informasi, kontribusi pada norma perilaku negara di forum multilater al, serta partisipasi aktif dalam koalisi teknis seperti ISAC/ISAO di tingkat regional. Cyber leadership harus memimpin delegasi teknokrat-diplomatik yang memadukan kapasitas teknis BSSN dan legitimasi politik Kemlu untuk memastikan manfaat praktis—bukan sekadar retorika—dari hubungan internasional. Penguatan posisi Indonesia di arena global juga meningkatkan bargaining power dalam isu transfer teknologi dan dukungan krisis.

Model tata kelola yang direkomendasikan adalah multi-stakeholder governance yang mengkombinasikan otoritas negara dengan peran swasta, akademia, dan masyarakat sipil. Penelitian dan panduan praktis menunjukkan bahwa keterlibatan berlapis mempercepat sharing threat-intelligence, memperluas kapasitas deteksi, dan memperkuat legitimasi kebijakan. Dalam kerangka ini, cyber leadership berfungsi sebagai fasilitator: menginisiasi mekanisme formal (ISAC sektoral, MoU publik–swasta, forum reguler), memastikan perlindungan data dan mitigasi konflik kepentingan, serta memelihara ekosistem yang mendorong inovasi lokal. Tata kelola multi-aktor yang efektif mengurangi fragmen kebijakan dan memperbaiki efisiensi respons nasional.

Secara sintetis, strategi penguatan pertahanan siber melalui cyber leadership mensyaratkan empat garis aksi terukur: mengkodifikasi siber dalam doktrin pertahanan dan playbook krisis, mengakselerasi kapasitas SDM melalui pendidikan dan pelatihan praktik, memperluas diplomasi teknis untuk intelijen dan norma internasional, serta mempraktikkan tata kelola multi-stakeholder untuk integrasi kapasitas nasional. Indikator-indikator terukur (dokumen doktrinal, jumlah latihan bersama, jumlah tenaga bersertifikat, MoU internasional/ISAC, dan frekuensi pembagian intelijen) harus menjadi basis

evaluasi berkala yang dipimpin oleh otoritas nasional—dengan peran sentral cyber leadership sebagai pengarah dan pengawal implementasi.

KESIMPULAN DAN REKOMENDASI

Cyber leadership di era digital merupakan kebutuhan strategis bagi Indonesia dalam menghadapi ancaman siber yang semakin kompleks, baik dalam bentuk serangan teknis, spionase digital, disinformasi, maupun ancaman terhadap infrastruktur kritis. Ketergantungan Indonesia pada ekosistem digital global memperbesar risiko, sementara kapasitas domestik masih menghadapi kendala pada aspek kelembagaan, koordinasi, serta ketersediaan sumber daya manusia. Dalam konteks ini, kepemimpinan siber bukan hanya menyangkut penguasaan teknologi, melainkan kemampuan strategis untuk mengintegrasikan kebijakan, memperkuat tata kelola lintas sektor, serta membangun ketahanan sosial melalui literasi digital dan kesadaran kolektif.

Cyber leadership yang efektif harus menekankan pada kepemimpinan adaptif dan transformasional, yang mampu merespons dinamika ancaman sekaligus memberikan visi jangka panjang bagi pembangunan kedaulatan digital Indonesia. Keberhasilan strategi ini dapat diukur melalui indikator terukur seperti kecepatan deteksi dan respons insiden (MTTD/MTTR), tingkat kepatuhan audit keamanan, jumlah talenta bersertifikasi, serta posisi Indonesia dalam indeks global keamanan siber. Dengan mengintegrasikan aspek teknis, regulatif, dan sosial, Indonesia dapat bergerak menuju pertahanan siber yang tangguh dan berdaulat.

Pertama, Indonesia perlu memperkuat arsitektur kelembagaan pertahanan siber dengan membangun mekanisme koordinasi terpadu antar lembaga negara, sektor swasta, dan masyarakat sipil. Hal ini mencakup penunjukan Chief Information Security Officer (CISO) di setiap kementerian dan lembaga, serta pembentukan Dewan Keamanan Siber Nasional yang berada langsung di bawah koordinasi Presiden untuk memastikan efektivitas pengambilan keputusan.

Kedua, pembangunan kapasitas sumber daya manusia harus diprioritaskan melalui pembentukan National Cyber Leadership Academy yang berfokus pada pelatihan teknis, kepemimpinan strategis, dan diplomasi siber. Investasi dalam pendidikan formal, pelatihan non-formal, dan program sertifikasi harus ditingkatkan untuk menciptakan ekosistem talenta yang berkelanjutan.

Ketiga, Indonesia perlu mengembangkan kemandirian digital melalui insentif riset dan pengembangan teknologi lokal, kemitraan dengan industri dalam negeri, serta regulasi yang mewajibkan penggunaan solusi keamanan lokal pada infrastruktur kritis. Hal ini akan memperkuat kedaulatan digital sekaligus mendorong pertumbuhan industri teknologi nasional.

Keempat, penguatan literasi digital masyarakat harus menjadi agenda nasional untuk meningkatkan ketahanan sosial terhadap disinformasi dan manipulasi digital. Program literasi harus bersifat inklusif, menjangkau kelompok rentan, serta memanfaatkan pendekatan berbasis komunitas agar pesan keamanan digital dapat diterima secara luas.

Kelima, diplomasi siber perlu ditingkatkan melalui keterlibatan aktif Indonesia dalam forum internasional seperti ASEAN, PBB, dan kerjasama multilateral lainnya. Hal ini penting untuk memperkuat posisi Indonesia dalam menetapkan norma internasional, meningkatkan akses pada intelijen ancaman global, serta memperluas kerja sama transfer teknologi.

PENELITIAN LANJUTAN

Setiap penelitian secara inheren memiliki keterbatasan yang tidak dapat dihindari. Oleh karena itu, diperlukan kajian lanjutan yang mampu memperdalam analisis serta memperluas cakupan pemahaman terhadap topik ini. Penelitian selanjutnya diharapkan dapat membuka perspektif baru, menguji temuan yang ada, dan memperkaya wacana ilmiah melalui pendekatan yang lebih komprehensif.

UCAPAN TERIMA KASIH

Sebagai penutup, penulis menyampaikan apresiasi yang tulus kepada semua pihak yang telah memberikan dukungan, masukan, dan kontribusi berharga dalam proses penyusunan hingga terbitnya artikel ini. Penghargaan yang sama juga diberikan kepada para pembaca yang telah meluangkan waktu untuk menyimak dan mengapresiasi hasil penelitian ini.

DAFTAR PUSTAKA

Bradshaw, S., & Howard, P. N. (2019). *The global disinformation order: 2019 global inventory of organized social media manipulation.* Oxford: Oxford Internet Institute.

BSSN. (2023). *Laporan Tahunan Keamanan Siber Indonesia 2023.* Jakarta: Badan Siber dan Sandi Negara.

Carrapico, H., & Farrand, B. (2021). *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy.* London: Palgrave Macmillan.

Chong, A. (2020). Singapore's approach to cybersecurity: A model for small states? *Journal of Cyber Policy*.

ITU. (2021). *Global Cybersecurity Index (GCI) 2020.* Geneva: International Telecommunication Union.

Kellerman, A. (2020). *Leadership in the Digital Age: Cyber Leadership for the 21st Century.* London: Routledge.

Kepios, W. A. (2024). *Digital 2024: Indonesia.*

Madise, Ü., & Martens, T. (2021). Cybersecurity and e-governance in Estonia: Lessons for small states. *Government Information Quarterly*.

Nye, J. S. (2022). The Digital Age and Cyber Power. *International Security, 1*(47), 53–78.

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfar.* New York: Farrar, Straus and Giroux.

Singer, P. W., & Friedman, A. (2019). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford: Oxford University Press.

Susanti, R., & Fitriani, E. (2022). Cybersecurity policy in Indonesia: Between ambition and capacity. *Contemporary Southeast Asia, 2*(44), 261–287.

Timmers, P. (2022). European strategic autonomy in cybersecurity. *Journal of Cyber Policy*.

Ventures, C. (2023). *Cybercrime Report 2023.* Diambil kembali dari https://cybersecurityventures.com