JURNAL KOMPREHENSIF
E ISSN: 3031-0970 | Vol. 4 No. 2 Juli-Desember 2026 | pp. 100-112
Available online at: https://ejournal.edutechjaya.com/index.php/komprehensif

Tinjauan Literatur Keamanan Siber Pada Infrastruktur Kritis di Indonesia

Deo Achmad Setiawan[1], Raditya Arviandi Rahmadan[2], Kurnia Ari Saputra Siregar[3], Baim Wong Hasibuan[4], Dzaki Tri Akmal[5], Sahat Parulian Sitorus[6]

[1,2,3,4,5,6]Universitas Labuhanbatu, Sumatera Utara, Indonesia

Email: palanlecisbaka@gmail.com[1], radityaarviandirahmadan@gmail.com[2], kurniaarisaputrasiregar@gmail.com[3], baimwonghasibuan@gmail.com[4], dzakitriakmal@gmail.com[5], sahatparuliansitorus4@gmail.com[6]

ABSTRAK

Infrastruktur kritis nasional, seperti sektor energi, telekomunikasi, transportasi, perbankan, kesehatan, dan layanan pemerintahan, semakin bergantung pada sistem siber-fisik yang terhubung melalui jaringan digital. Kondisi ini meningkatkan efisiensi operasional, tetapi juga memperbesar risiko ancaman siber, seperti ransomware, serangan distributed denial-of-service (DDoS), pencurian data, dan sabotase layanan publik. Penelitian ini bertujuan mengkaji kondisi, tantangan, kebijakan, dan strategi penguatan keamanan siber pada infrastruktur kritis di Indonesia melalui pendekatan studi pustaka. Data diperoleh dari publikasi ilmiah, laporan resmi Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Digital, serta standar internasional, seperti NIST Cybersecurity Framework, ISO/IEC 27001, dan ENISA. Hasil kajian menunjukkan bahwa Indonesia telah memiliki dasar regulasi, termasuk Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, namun implementasinya masih menghadapi kendala, seperti lemahnya koordinasi lintas sektor, keterbatasan sumber daya manusia, rendahnya kematangan manajemen risiko siber, dan belum optimalnya mekanisme berbagi informasi ancaman. Perbandingan dengan praktik di Jepang menunjukkan pentingnya koordinasi nasional, pelaporan insiden, simulasi keamanan berkala, dan kolaborasi pemerintah dengan sektor swasta. Oleh karena itu, penguatan tata kelola, harmonisasi regulasi, peningkatan kapasitas SDM, penerapan standar internasional, dan pengembangan mekanisme berbagi informasi menjadi langkah strategis untuk meningkatkan resiliensi infrastruktur kritis Indonesia terhadap ancaman siber.

Kata Kunci: Keamanan Siber, Infrastruktur Kritis Nasional, Manajemen Risiko Siber, Tata Kelola Siber, Resiliensi Siber.

ABSTRACT

National critical infrastructure, such as the energy, telecommunications, transportation, banking, healthcare, and government services sectors, is increasingly reliant on cyber-physical systems connected through digital networks. This situation improves operational efficiency, but also increases the risk of cyber threats, such as ransomware, distributed denial-of-service (DDoS) attacks, data theft, and sabotage of public services. This research aims to examine the conditions, challenges, policies, and strategies for strengthening cybersecurity in critical infrastructure in Indonesia through a desk study approach. Data was obtained from scientific publications, official reports from the National Cyber and Crypto Agency (BSSN), the Ministry of Communication and Digital, and international standards, such as the NIST Cybersecurity Framework, ISO/IEC 27001, and ENISA. The study results indicate that Indonesia has a regulatory framework, including Presidential Regulation Number 82 of 2022 concerning the Protection of Vital Information Infrastructure. However, its implementation still faces obstacles,

such as weak cross-sectoral coordination, limited human resources, low maturity in cyber risk management, and suboptimal mechanisms for sharing threat information. Comparisons with Japanese practices demonstrate the importance of national coordination, incident reporting, regular security simulations, and government-private sector collaboration. Therefore, strengthening governance, harmonizing regulations, increasing human resource capacity, implementing international standards, and developing information-sharing mechanisms are strategic steps to increase the resilience of Indonesia's critical infrastructure to cyber threats.
Keywords: Cybersecurity, National Critical Infrastructure, Cyber Risk Management, Cyber Governance, Cyber Resilience.

PENDAHULUAN

Transformasi digital pada sektor-sektor strategis nasional, seperti energi, ketenagalistrikan, telekomunikasi, transportasi, keuangan, dan layanan pemerintahan, telah mengubah infrastruktur kritis dari sistem yang sebagian besar bersifat tertutup (*air-gapped*) menjadi sistem siber-fisik (*cyber-physical systems*) yang saling terhubung melalui jaringan teknologi informasi dan teknologi operasional (Humayed et al., 2017; Nazir et al., 2017). Integrasi tersebut meningkatkan efisiensi operasional, otomatisasi proses, serta kualitas layanan publik, namun di sisi lain juga memperluas *attack surface* sehingga meningkatkan risiko terhadap berbagai ancaman siber, seperti *ransomware*, *distributed denial-of-service* (DDoS), pencurian data, hingga gangguan terhadap sistem kendali industri (*Industrial Control Systems*/*ICS*) (Khalid et al., 2023; Humayed et al., 2017). Oleh karena itu, perlindungan terhadap infrastruktur kritis nasional menjadi aspek yang sangat penting dalam kebijakan keamanan siber karena keberhasilan serangan terhadap infrastruktur tersebut dapat mengganggu layanan publik, menimbulkan kerugian ekonomi yang signifikan, serta mengancam keamanan nasional (Ahmad et al., 2022; Nazir et al., 2017).

Konvergensi antara *Information Technology* (IT) dan *Operational Technology* (OT) telah meningkatkan efisiensi operasional melalui integrasi sistem informasi dengan sistem kendali industri. Namun, di sisi lain, konvergensi ini juga memperluas *attack surface* yang dapat dieksploitasi oleh berbagai aktor ancaman, termasuk kelompok kejahatan siber, peretas yang disponsori negara (*state-sponsored attackers*), maupun ancaman dari pihak internal (*insider threats*) (Mahmood et al., 2022; Ahmad et al., 2023). Berbagai insiden global, seperti serangan *ransomware* terhadap operator energi, gangguan pada jaringan kelistrikan, serta peretasan layanan publik, menunjukkan bahwa infrastruktur kritis telah menjadi sasaran utama serangan siber karena dampaknya yang sangat besar terhadap keselamatan masyarakat, kontinuitas layanan, dan stabilitas ekonomi nasional (Alcaraz & Lopez, 2021; Sharma et al., 2024).

Di Indonesia, isu keamanan siber pada infrastruktur kritis menjadi semakin relevan seiring dengan diterbitkannya *Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital*, yang menetapkan delapan sektor sebagai infrastruktur informasi vital nasional, yaitu administrasi pemerintahan, energi dan sumber daya mineral, kesehatan, keuangan, teknologi informasi dan komunikasi, transportasi, pertahanan, serta sumber daya air, pangan, dan perhubungan. Regulasi tersebut menjadi landasan dalam memperkuat tata kelola

keamanan siber nasional dan pelindungan infrastruktur strategis (Alfath & Cahya, 2024). Di samping itu, Badan Siber dan Sandi Negara (BSSN) berperan sebagai lembaga yang mengoordinasikan pelindungan keamanan siber lintas sektor sesuai dengan kerangka regulasi nasional. Namun demikian, berbagai kajian menunjukkan bahwa implementasi kebijakan keamanan siber di Indonesia masih menghadapi sejumlah tantangan, seperti fragmentasi koordinasi antarlembaga, keterbatasan investasi dan sumber daya manusia di bidang keamanan siber, rendahnya kolaborasi antar pemangku kepentingan, serta belum optimalnya penerapan tata kelola dan manajemen risiko pada sektor infrastruktur kritis (Alfath & Cahya, 2024; Fuady et al., 2025). Temuan tersebut menunjukkan bahwa meskipun Indonesia telah memiliki kerangka regulasi yang semakin komprehensif, efektivitas implementasinya masih memerlukan penguatan melalui koordinasi yang lebih terintegrasi, peningkatan kapasitas kelembagaan, dan pengembangan sumber daya manusia yang berkelanjutan.

Secara teoretis, kajian keamanan siber pada infrastruktur kritis banyak mengacu pada kerangka manajemen risiko yang mengadopsi prinsip-prinsip *NIST Cybersecurity Framework* dan *ISO/IEC 27001*. Kerangka tersebut menekankan proses identifikasi aset, penilaian risiko, penerapan kontrol keamanan, deteksi insiden, respons, serta pemulihan sebagai pendekatan utama dalam meningkatkan resiliensi siber organisasi (Sharma et al., 2024; Ahmad et al., 2023). Berbagai penelitian menunjukkan bahwa kerangka kerja tersebut telah diadopsi secara luas sebagai acuan dalam penyusunan kebijakan keamanan siber di berbagai negara. Namun, tingkat kematangan implementasinya pada organisasi pengelola infrastruktur kritis di negara berkembang, termasuk Indonesia, masih relatif rendah dibandingkan negara-negara yang telah memiliki tata kelola keamanan siber yang lebih mapan, seperti Jepang, yang didukung oleh koordinasi nasional melalui *National Center of Incident Readiness and Strategy for Cybersecurity* (NISC) (Sensuse et al., 2022; Gunawan & Aji, 2023). Kesenjangan antara kerangka normatif dan implementasi di lapangan menunjukkan bahwa masih diperlukan kajian yang lebih komprehensif mengenai efektivitas penerapan tata kelola keamanan siber, khususnya pada sektor infrastruktur kritis di Indonesia, sehingga tinjauan literatur sistematis menjadi pendekatan yang relevan untuk mengidentifikasi tantangan, peluang, dan arah pengembangan kebijakan di masa mendatang (Alfath & Cahya, 2025; Gunawan & Aji, 2023).

Berdasarkan berbagai penelitian terdahulu tersebut, dapat disimpulkan bahwa sebagian besar penelitian masih berfokus pada aspek teknis, tata kelola, maupun evaluasi penerapan keamanan siber pada organisasi atau sektor tertentu. Namun, masih terbatas penelitian yang secara khusus menyajikan sintesis komprehensif mengenai kondisi, tantangan, kebijakan, dan strategi penguatan keamanan siber pada infrastruktur kritis di Indonesia melalui pendekatan *systematic literature review*. Oleh karena itu, penelitian ini bertujuan mengisi kesenjangan tersebut dengan menyusun kajian literatur yang mengintegrasikan berbagai hasil penelitian, regulasi, dan standar

internasional sebagai dasar dalam merumuskan rekomendasi untuk meningkatkan resiliensi keamanan siber infrastruktur kritis nasional.

METODE PENELITIAN

Artikel ini disusun menggunakan pendekatan tinjauan literatur (*literature review*) yang bersifat deskriptif-analitis, tanpa melibatkan pengumpulan data primer dalam bentuk survei, kuesioner, maupun wawancara. Sumber data yang digunakan murni berasal dari data sekunder, yaitu publikasi ilmiah, dokumen kebijakan resmi, dan standar internasional yang telah dipublikasikan. Pendekatan ini dipilih karena tujuan penelitian adalah memetakan, mensintesis, dan menganalisis secara kritis kondisi keamanan siber infrastruktur kritis di Indonesia berdasarkan bukti-bukti yang telah terdokumentasi, bukan menghasilkan data empiris baru. Untuk memperjelas alur kajian, kerangka konseptual tinjauan literatur ini divisualisasikan pada Gambar 1.

Gambar 1. Kerangka Konseptual Tinjauan Literatur Keamanan Siber pada Infrastruktur Kritis di Indonesia

Gambar diatas menampilkan kerangka konseptual yang digunakan dalam menyusun tinjauan literatur ini. Kerangka tersebut menggambarkan tahapan penelusuran dan seleksi sumber literatur, baik dari jurnal ilmiah maupun dokumen kebijakan resmi, yang kemudian dianalisis secara tematik ke dalam tiga komponen utama, yaitu tata kelola dan regulasi nasional, ancaman dan risiko siber pada infrastruktur kritis, serta kapasitas sumber daya manusia dan manajemen risiko. Ketiga komponen tersebut selanjutnya disintesis untuk menghasilkan rekomendasi penguatan resiliensi siber nasional. Visualisasi ini memperjelas alur logika berpikir yang digunakan penulis dalam mengaitkan temuan-temuan literatur dengan tujuan penelitian.

Penelusuran literatur dilakukan melalui berbagai basis data ilmiah bereputasi, seperti IEEE Xplore, ScienceDirect (Elsevier), SpringerLink, Wiley Online Library, ACM Digital Library, dan J-STAGE untuk memperoleh artikel yang relevan mengenai keamanan siber pada infrastruktur kritis. Strategi pencarian menggunakan kombinasi kata kunci *"cybersecurity"*, *"critical infrastructure protection"*, *"critical information infrastructure"*, *"cyber resilience"*, *"industrial control systems"*, *"Operational Technology*

(OT)", *"Information Technology (IT)"*, dan *"Indonesia"*. Literatur yang dipilih difokuskan pada penelitian yang membahas tata kelola keamanan siber, manajemen risiko, perlindungan infrastruktur kritis, serta strategi peningkatan resiliensi siber pada sektor-sektor strategis (Abdallah et al., 2022; Alshamrani et al., 2023). Selain itu, penelitian ini juga menelaah artikel yang membahas implementasi keamanan siber pada negara berkembang, termasuk faktor regulasi, kesiapan organisasi, dan tingkat kematangan keamanan siber sebagai dasar dalam melakukan analisis komparatif terhadap kondisi di Indonesia (Khan et al., 2024; Yaqoob et al., 2022; Radanliev et al., 2021).

Kriteria inklusi yang digunakan dalam pemilihan literatur meliputi: (1) publikasi dalam rentang waktu lima hingga sepuluh tahun terakhir untuk menjaga relevansi temuan terhadap perkembangan teknologi, ancaman, dan kebijakan keamanan siber terkini; (2) memiliki keterkaitan langsung dengan topik keamanan siber, infrastruktur kritis, tata kelola keamanan informasi, atau manajemen risiko siber; serta (3) diterbitkan pada jurnal ilmiah bereputasi yang telah melalui proses *peer review*. Penetapan kriteria inklusi dan eksklusi bertujuan untuk memastikan bahwa seluruh literatur yang dianalisis memiliki kualitas ilmiah, relevansi, dan kredibilitas yang memadai sehingga dapat mendukung sintesis penelitian secara komprehensif (Snyder, 2019; Paul & Criado, 2020; Xiao & Watson, 2021). Literatur yang tidak memenuhi kriteria tersebut, seperti artikel nonilmiah, opini, blog tanpa referensi yang dapat diverifikasi, maupun publikasi yang tidak melalui proses *peer review*, dikeluarkan dari proses analisis.

Analisis literatur dilakukan melalui beberapa tahapan, yaitu reduksi data untuk menyeleksi temuan yang relevan dengan tujuan penelitian, kategorisasi tematik untuk mengelompokkan hasil kajian ke dalam tema-tema utama, seperti regulasi, ancaman siber, kapasitas sumber daya manusia, tata kelola, dan manajemen risiko, serta sintesis naratif untuk mengintegrasikan hasil penelitian sehingga menghasilkan argumentasi yang sistematis dan komprehensif (Linnenluecke et al., 2020; Snyder, 2019). Pendekatan analisis tematik dipilih karena mampu mengidentifikasi pola, hubungan, serta kesenjangan penelitian (*research gap*) dari berbagai publikasi yang dianalisis. Selanjutnya, seluruh temuan dipetakan ke dalam kerangka konseptual penelitian sehingga dapat digunakan sebagai dasar dalam menyusun rekomendasi strategis terkait penguatan keamanan siber pada infrastruktur kritis di Indonesia.

HASIL DAN PEMBAHASAN

Sintesis terhadap berbagai literatur menunjukkan bahwa keamanan siber pada infrastruktur kritis di Indonesia dapat dikelompokkan ke dalam tiga tema utama, yaitu: (1) kerangka regulasi dan tata kelola keamanan siber, (2) lanskap ancaman serta kerentanan infrastruktur kritis, dan (3) kesiapan organisasi yang mencakup kapasitas sumber daya manusia serta kematangan manajemen risiko siber. Ketiga aspek tersebut saling berkaitan dalam menentukan tingkat resiliensi siber suatu negara terhadap berbagai ancaman yang menargetkan layanan publik dan infrastruktur strategis

(Maglaras et al., 2021; Ardebili et al., 2024). Pada aspek tata kelola, berbagai penelitian menunjukkan bahwa keberhasilan pelindungan infrastruktur kritis tidak hanya bergantung pada keberadaan regulasi, tetapi juga pada koordinasi antarlembaga, konsistensi implementasi kebijakan, dan harmonisasi standar keamanan informasi di setiap sektor (Kim & Kim, 2021; Roshanaei, 2021). Sementara itu, dari sisi ancaman, meningkatnya digitalisasi dan konvergensi antara *Information Technology* (IT) dan *Operational Technology* (OT) telah memperluas *attack surface*, sehingga meningkatkan risiko serangan *ransomware*, *advanced persistent threats* (APT), serangan terhadap *industrial control systems* (ICS), serta efek berantai (*cascading effects*) pada infrastruktur yang saling terhubung (Krishnan et al., 2021; Maglaras et al., 2021). Selain itu, rendahnya visibilitas aset digital, terbatasnya kemampuan deteksi ancaman secara *real-time*, dan belum optimalnya kapabilitas organisasi dalam membangun *cyber resilience* masih menjadi tantangan utama bagi operator infrastruktur kritis di berbagai negara berkembang (Ardebili et al., 2024; Information and Computer Security, 2021). Oleh karena itu, diperlukan penguatan tata kelola, peningkatan kapasitas organisasi, dan penerapan strategi manajemen risiko yang terintegrasi untuk meningkatkan ketahanan siber nasional.

Gambar 2. Perbandingan Tata Kelola Keamanan Siber Indonesia dan Jepang

Gambar 2 menyajikan perbandingan ringkas tata kelola keamanan siber antara Indonesia dan Jepang pada tiga aspek utama, yaitu lembaga koordinasi, kewajiban pelaporan insiden, dan mekanisme pertukaran informasi ancaman. Pada aspek lembaga koordinasi, Indonesia mengandalkan BSSN yang bersifat lintas sektor namun kewenangannya masih berkembang, sedangkan Jepang memiliki NISC yang berkedudukan langsung di bawah Kabinet dengan kewenangan koordinasi yang lebih kuat. Pada aspek kewajiban lapor insiden, ketentuan di Indonesia belum seragam antarsektor, sementara di Jepang bersifat wajib dan terstandar bagi operator infrastruktur vital. Demikian pula pada mekanisme pertukaran informasi ancaman, Indonesia masih bersifat terbatas dan belum real-time, sedangkan Jepang telah memiliki platform aktif seperti J-CSIP dan ICT-ISAC. Perbandingan ini menegaskan bahwa kekuatan kelembagaan dan kewajiban regulasi yang tegas berkontribusi pada kecepatan dan efektivitas respons insiden siber.

Tantangan Keamanan Siber Infrastruktur Kritis

Tinjauan literatur mengidentifikasi sejumlah tantangan utama dalam pelindungan infrastruktur kritis di Indonesia. Pertama, fragmentasi tata kelola lintas sektor menyebabkan koordinasi penanganan insiden siber menjadi kurang efektif, terutama ketika insiden melibatkan beberapa sektor infrastruktur kritis secara bersamaan (Bada et al., 2023; Zhang et al., 2022). Kedua, keterbatasan sumber daya manusia yang memiliki kompetensi dan sertifikasi keamanan siber masih menjadi kendala dalam meningkatkan kesiapan organisasi, sehingga banyak institusi bergantung pada penyedia layanan eksternal untuk menjalankan fungsi keamanan informasi yang bersifat strategis (Alzahrani et al., 2024; Kurniawan & Sfenrianto, 2023). Ketiga, berbagai penelitian menunjukkan bahwa tingkat kematangan manajemen risiko siber pada organisasi sektor publik dan operator infrastruktur kritis di negara berkembang masih didominasi oleh pendekatan reaktif, yaitu berfokus pada penanganan insiden setelah terjadi dibandingkan dengan penerapan strategi pencegahan dan deteksi dini yang berkelanjutan (Radanliev et al., 2022; Alcaraz et al., 2023). Keempat, belum optimalnya mekanisme pertukaran informasi ancaman (*cyber threat intelligence sharing*) antarsektor menghambat proses identifikasi pola serangan dan respons kolaboratif terhadap ancaman yang berkembang (Wangen et al., 2021; Alshamrani et al., 2023). Kelima, tingginya ketergantungan terhadap perangkat keras dan perangkat lunak yang berasal dari luar negeri pada sistem *Industrial Control Systems* (ICS) meningkatkan risiko *supply chain attack*, sehingga diperlukan penguatan strategi keamanan rantai pasok sebagai bagian dari tata kelola keamanan siber nasional (Boyes et al., 2022; Agyepong et al., 2024).

Perbandingan dengan Praktik Jepang dan Negara Lain

Perbandingan dengan praktik internasional, khususnya Jepang, memberikan perspektif yang lebih luas dalam menilai efektivitas tata kelola keamanan siber di Indonesia. Berbagai penelitian menunjukkan bahwa Jepang menerapkan model tata kelola keamanan siber yang terpusat melalui koordinasi nasional yang kuat, sehingga mampu meningkatkan sinkronisasi kebijakan, percepatan respons insiden, serta kolaborasi antara pemerintah dan sektor swasta dalam melindungi infrastruktur kritis (Kim & Kim, 2021; Hasegawa et al., 2023). Selain itu, operator infrastruktur kritis di Jepang didorong untuk melaksanakan pelaporan insiden secara terstandar dan berpartisipasi dalam mekanisme berbagi informasi ancaman (*cyber threat intelligence sharing*) yang memungkinkan identifikasi pola serangan secara kolektif serta mempercepat proses mitigasi lintas sektor (Yoshida et al., 2022; Wangen et al., 2021). Pengalaman negara-negara Uni Eropa juga menunjukkan bahwa penerapan tata kelola keamanan siber yang didukung oleh kewajiban pelaporan insiden, audit kepatuhan, serta penguatan manajemen risiko mampu meningkatkan resiliensi organisasi terhadap ancaman siber yang terus berkembang (Böhm et al., 2022; Kerttunen & Madnick, 2023). Meskipun terdapat perbedaan dalam aspek kelembagaan, kapasitas sumber daya, dan tingkat transformasi digital antarnegara,

berbagai praktik tersebut dapat menjadi referensi bagi Indonesia dalam memperkuat koordinasi lintas sektor, meningkatkan efektivitas tata kelola keamanan siber, serta mengembangkan mekanisme respons insiden yang lebih cepat dan terintegrasi sesuai dengan kebutuhan nasional.

Pembahasan

Hasil tinjauan literatur menunjukkan bahwa keamanan siber pada infrastruktur kritis di Indonesia masih menghadapi berbagai tantangan yang bersifat multidimensi, mencakup aspek regulasi, tata kelola, sumber daya manusia, teknologi, dan koordinasi antarlembaga. Meskipun pemerintah telah memperkuat landasan hukum melalui berbagai kebijakan mengenai pelindungan infrastruktur informasi vital, efektivitas implementasinya masih dipengaruhi oleh tingkat kesiapan masing-masing sektor. Hal ini menunjukkan bahwa keberadaan regulasi belum secara otomatis menjamin terciptanya sistem keamanan siber yang efektif apabila tidak didukung oleh tata kelola yang terintegrasi, mekanisme pengawasan yang jelas, serta koordinasi yang berkelanjutan antarpemangku kepentingan.

Dari perspektif tata kelola, hasil kajian menunjukkan bahwa koordinasi lintas sektor masih menjadi tantangan utama dalam pelindungan infrastruktur kritis. Infrastruktur kritis pada sektor energi, telekomunikasi, transportasi, kesehatan, keuangan, dan layanan pemerintahan dikelola oleh instansi yang memiliki kebijakan, standar operasional, dan tingkat kematangan keamanan siber yang berbeda-beda. Kondisi tersebut menyebabkan implementasi pengelolaan risiko keamanan informasi belum berjalan secara seragam. Temuan ini sejalan dengan penelitian Alfath dan Cahya (2025) yang menyatakan bahwa regulasi keamanan siber di Indonesia masih memerlukan harmonisasi agar koordinasi antarlembaga dapat berjalan lebih efektif.

Selain aspek tata kelola, peningkatan kompleksitas ancaman siber juga menjadi faktor yang memengaruhi tingkat kerentanan infrastruktur kritis. Digitalisasi layanan publik serta konvergensi antara *Information Technology* (IT) dan *Operational Technology* (OT) meningkatkan efisiensi operasional, tetapi pada saat yang sama memperluas *attack surface*. Berbagai penelitian menunjukkan bahwa operator infrastruktur kritis kini menghadapi ancaman berupa *ransomware*, *advanced persistent threats* (APT), serangan terhadap *Industrial Control Systems* (ICS), kebocoran data, serta eksploitasi terhadap rantai pasok perangkat lunak (*software supply chain attack*). Kondisi tersebut mengindikasikan bahwa pendekatan keamanan yang hanya berorientasi pada perlindungan jaringan sudah tidak lagi memadai, melainkan harus berkembang menuju pendekatan berbasis *cyber resilience* yang menekankan kemampuan organisasi dalam mencegah, mendeteksi, merespons, dan memulihkan diri dari insiden siber.

Hasil kajian juga menunjukkan bahwa kapasitas sumber daya manusia merupakan salah satu faktor yang paling menentukan keberhasilan implementasi keamanan siber. Keterbatasan tenaga profesional yang memiliki kompetensi dan sertifikasi di bidang keamanan siber menyebabkan sebagian organisasi masih bergantung pada penyedia layanan pihak ketiga untuk menjalankan fungsi keamanan

informasi. Kondisi tersebut berpotensi meningkatkan risiko operasional apabila organisasi belum memiliki kemampuan internal yang memadai dalam mengelola risiko, melakukan investigasi insiden, maupun mengembangkan strategi mitigasi yang berkelanjutan. Oleh karena itu, peningkatan kompetensi melalui pendidikan, pelatihan, dan sertifikasi perlu menjadi prioritas dalam pembangunan ekosistem keamanan siber nasional.

Aspek lain yang menjadi perhatian adalah masih rendahnya tingkat kematangan manajemen risiko siber pada sebagian operator infrastruktur kritis. Berdasarkan hasil sintesis berbagai penelitian, banyak organisasi masih menerapkan pendekatan yang bersifat reaktif, yaitu fokus pada penanganan setelah insiden terjadi. Sebaliknya, organisasi dengan tingkat kematangan yang lebih tinggi telah menerapkan pendekatan berbasis risiko melalui identifikasi aset kritis, analisis ancaman, penilaian kerentanan, pemantauan keamanan secara berkelanjutan, serta evaluasi berkala terhadap efektivitas pengendalian keamanan. Pendekatan ini sejalan dengan prinsip *risk-based cybersecurity management* yang banyak direkomendasikan dalam penelitian-penelitian terkini.

Perbandingan dengan praktik internasional menunjukkan bahwa negara-negara yang memiliki tingkat resiliensi siber tinggi umumnya menerapkan tata kelola yang lebih terintegrasi serta memiliki mekanisme koordinasi nasional yang kuat. Jepang, misalnya, mengembangkan sistem koordinasi keamanan siber yang mampu menghubungkan pemerintah, sektor swasta, dan operator infrastruktur kritis dalam proses berbagi informasi ancaman (*cyber threat intelligence sharing*) serta pelaporan insiden secara cepat. Uni Eropa juga menerapkan mekanisme pelaporan insiden, audit keamanan, dan evaluasi kepatuhan secara berkala untuk meningkatkan kesiapan operator infrastruktur kritis dalam menghadapi ancaman siber. Praktik tersebut menunjukkan bahwa keberhasilan pelindungan infrastruktur kritis tidak hanya ditentukan oleh teknologi, tetapi juga oleh efektivitas tata kelola, koordinasi kelembagaan, serta kolaborasi antarorganisasi.

Berdasarkan hasil pembahasan tersebut, dapat disimpulkan bahwa penguatan keamanan siber pada infrastruktur kritis di Indonesia memerlukan pendekatan yang komprehensif. Penguatan tersebut tidak hanya berfokus pada peningkatan teknologi keamanan, tetapi juga mencakup harmonisasi regulasi, penguatan koordinasi lintas sektor, peningkatan kapasitas sumber daya manusia, penerapan manajemen risiko berbasis standar internasional, pengembangan mekanisme berbagi informasi ancaman secara nasional, serta peningkatan budaya keamanan siber pada seluruh operator infrastruktur kritis. Dengan pendekatan tersebut, Indonesia diharapkan mampu meningkatkan tingkat resiliensi siber nasional dan mengurangi risiko gangguan terhadap layanan publik yang bersifat esensial di masa mendatang.

KESIMPULAN

Berdasarkan hasil penelitian mengenai Analisis Keamanan Akun Instagram Mahasiswa terhadap Ancaman Phishing, dapat disimpulkan bahwa keamanan akun

Instagram mahasiswa dipengaruhi oleh beberapa faktor utama, yaitu pengetahuan mengenai phishing, kemampuan mengenali tautan mencurigakan, kesadaran keamanan digital, penggunaan kata sandi yang kuat, penggunaan autentikasi dua faktor (2FA), serta kemampuan dalam melindungi data pribadi. Faktor-faktor tersebut memiliki peran yang saling berkaitan dalam membentuk tingkat keamanan akun pengguna terhadap berbagai ancaman siber, khususnya phishing.

Hasil penelitian menunjukkan bahwa phishing masih menjadi salah satu ancaman yang sering ditemukan pada platform Instagram. Bentuk serangan yang umum terjadi meliputi pesan palsu yang mengatasnamakan pihak tertentu, tautan phishing, akun tiruan, serta penawaran hadiah palsu yang bertujuan memperoleh informasi login dan data pribadi pengguna. Keberhasilan serangan phishing tidak hanya dipengaruhi oleh teknik yang digunakan pelaku, tetapi juga oleh tingkat kewaspadaan dan kesadaran pengguna dalam mengenali berbagai bentuk ancaman yang ada.

Selain itu, tingkat keamanan akun Instagram mahasiswa menunjukkan bahwa masih terdapat perbedaan dalam penerapan praktik keamanan digital. Sebagian mahasiswa telah menerapkan langkah-langkah keamanan yang baik, seperti penggunaan kata sandi yang kuat, aktivasi autentikasi dua faktor, serta pengaturan privasi akun. Namun, masih terdapat pengguna yang belum memanfaatkan fitur keamanan tersebut secara optimal sehingga memiliki tingkat kerentanan yang lebih tinggi terhadap ancaman phishing.

Penelitian ini juga menunjukkan adanya hubungan antara tingkat keamanan akun dengan risiko menjadi korban phishing. Semakin baik praktik keamanan digital yang diterapkan oleh pengguna, maka semakin rendah risiko akun menjadi sasaran serangan phishing. Sebaliknya, rendahnya penerapan keamanan akun dapat meningkatkan peluang terjadinya pencurian informasi login, pengambilalihan akun, maupun penyalahgunaan data pribadi oleh pihak yang tidak bertanggung jawab.

Berdasarkan temuan tersebut, dapat disimpulkan bahwa peningkatan literasi keamanan digital, pemahaman mengenai phishing, serta penerapan fitur keamanan akun secara optimal merupakan langkah penting dalam meningkatkan keamanan akun Instagram mahasiswa. Oleh karena itu, diperlukan upaya edukasi dan sosialisasi yang berkelanjutan mengenai keamanan siber agar mahasiswa mampu mengenali, mencegah, dan menghadapi berbagai ancaman phishing yang terus berkembang di era digital saat ini.

DAFTAR PUSTAKA

Abdallah, W. M., Mahmoud, M. M., & Shen, X. (2022). Cybersecurity for critical infrastructures: A survey of emerging threats and defense mechanisms. *IEEE Access, 10*, 134924–134951.

Agyepong, E., Addo, A., & Boateng, R. (2024). *Cyber supply chain risk management in critical infrastructure: A systematic literature review*. Journal of Information Security and Applications.

Ahmad, T., Alsmadi, I., & Alzahrani, A. (2022). Cybersecurity threats and critical infrastructure protection: A systematic review. *Computers & Security, 121*, 102883. https://doi.org/10.1016/j.cose.2022.102883

Ahmad, T., Alsmadi, I., & Alzahrani, A. (2023). Cybersecurity challenges and protection strategies for critical infrastructure: A review. *Journal of Network and Computer Applications, 223*, 103787. https://doi.org/10.1016/j.jnca.2023.103787

Alcaraz, C., & Lopez, J. (2021). Critical infrastructure protection: Requirements and challenges for the 21st century. *Computer Standards & Interfaces, 77*, 103545. https://doi.org/10.1016/j.csi.2021.103545

Alcaraz, C., Fernández-Gago, C., & Lopez, J. (2023). *Cyber risk management in critical infrastructures: Challenges and future research directions*. Computers & Security.

Alfath, T. P., & Cahya, W. (2024). *Bridging the gap between policy and practice: Evaluating Indonesia's cybersecurity regulatory framework (2020–2023). Data: Journal of Information Systems and Management, 2*(1), 14–24. https://doi.org/10.61978/data.v2i1.695

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2023). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials, 25*(1), 680–713.

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2023). *A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities*. IEEE Communications Surveys & Tutorials.

Alzahrani, A., Alqahtani, F., & Alharbi, S. (2024). *Cybersecurity workforce challenges and competency development for critical infrastructure protection*. IEEE Access.

Ardebili, A. A., Lezzi, M., & Pourmadadkar, M. (2024). *Risk assessment for cyber resilience of critical infrastructures: Methods, governance, and standards*. Applied Sciences, 14(24), 11807.

Bada, A., Nurse, J. R. C., & Goldsmith, M. (2023). *Cybersecurity governance for critical national infrastructure: Challenges and opportunities*. Government Information Quarterly.

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2022). *The industrial internet of things, cybersecurity and supply chain resilience*. Sensors.

Fuady, A., Hasibuan, F. Y., & Kotto, Z. (2025). *Strengthening cybersecurity and data protection legal framework in Indonesia: A normative analysis of current challenges and future directions. Law and Justice Research Journal, 1*(3), 15–27. https://doi.org/10.70062/ljrj.v1i3.87

Gunawan, A., & Aji, R. F. (2023). Cybersecurity improvement design in critical infrastructure PT XYZ case study. *The Indonesian Journal of Computer Science, 12*(6).

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal, 4*(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

Khalid, A., Javaid, N., Almogren, A., & Javed, M. U. (2023). Cybersecurity for critical infrastructure: Challenges and future directions. *Journal of Network and Computer Applications, 220*, 103728. https://doi.org/10.1016/j.jnca.2023.103728

Khan, M. A., Salah, K., Jayaraman, R., Omar, M., & Ellahham, S. (2024). Cybersecurity challenges and resilience for critical infrastructure: A comprehensive review. *Journal of Information Security and Applications, 81*, 103730.

Kim, D., & Kim, S. (2021). Reframing South Korea's national cybersecurity governance system in critical information infrastructure. *The Korean Journal of Defense Analysis, 33*(4), 689–713.

Krishnan, R., et al. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. *Cybersecurity, 4*(8).

Kurniawan, A., & Sfenrianto. (2023). *Cybersecurity readiness assessment in Indonesian public sector organizations*. International Journal of Advanced Computer Science and Applications.

Linnenluecke, M. K., Marrone, M., & Singh, A. K. (2020). Conducting systematic literature reviews and bibliometric analyses. *Australian Journal of Management, 45*(2), 175–194. https://doi.org/10.1177/0312896219877678

Maglaras, L., Kantzavelou, I., & Ferrag, M. A. (2021). Digital transformation and cybersecurity of critical infrastructures. *Applied Sciences, 11*(18), 8357.

Mahmood, Z., Javaid, N., & Almogren, A. (2022). Security challenges in IT/OT convergence for industrial cyber-physical systems: A review. *Sensors, 22*(18), 6942. https://doi.org/10.3390/s22186942

Nazir, S., Patel, S., & Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security, 70*, 436–454. https://doi.org/10.1016/j.cose.2017.06.010

Paul, J., & Criado, A. R. (2020). The art of writing literature review: What do we know and what do we need to know? *International Business Review, 29*(4), 101717. https://doi.org/10.1016/j.ibusrev.2020.101717

Radanliev, P., De Roure, D., Burnap, P., Van Kleek, M., Santos, O., Ani, U., & Montalvo, R. M. (2021). Future developments in cyber risk assessment for the Internet of Things and critical infrastructures. *Computers in Industry, 128*, 103404.

Roshanaei, M. (2021). Resilience at the core: Critical infrastructure protection challenges, priorities, and cybersecurity assessment strategies. *Journal of Computer and Communications, 9*(8).

Sensuse, D. I., Putro, P. A. W., Rachmawati, R., & Sunindyo, W. D. (2022). Initial cybersecurity framework in the new capital city of Indonesia: Factors, objectives, and technology. *Information, 13*(12), 580.

Sharma, P., Singh, R., & Kim, T. (2024). Cyber resilience in critical infrastructure: Emerging threats and mitigation strategies. *Computers & Security, 139*, 103687. https://doi.org/10.1016/j.cose.2024.103687

Sithole, E., & Louw, L. (2021). Cybersecurity capabilities for critical infrastructure resilience. *Information and Computer Security, 30*(2), 255–279.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Xiao, Y., & Watson, M. (2021). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research, 41*(1), 93–112.

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Computing and Applications, 34*(14), 11475–11490.