PERANG SIBER di ERA KONEKTIVITAS TINGGI: KONVERGENSI JARINGAN KOMUNIKASI DATA dan KONFLIK DIGITAL

Muhammad Rizky Habibie[1], Putri Nabila[2], Aufa Zakiya Faizza[3], Rakhmatan Lil Alamin Arrasyid[4], Anjar Sulistyani[5]
Institut Agama Islam Al-Zaytun Indonesia
[1]rizkyhabibie331@gmail.com, [2]putrinabilaaa0308@gmail.com, [3]fazakiya31@gmail.com, [4]Rahmatanlilalamin219@gmail.com, [5]anjar@iai-alzaytun.ac.id

ABSTRACT

This study analyzes the relationship between data communication network convergence and the escalation of global cyber warfare in the high-connectivity era. The integration of Internet of Things (IoT), cloud computing, edge computing, and 5G networks has created efficient yet vulnerable communication ecosystems. Using a qualitative comparative case study on SolarWinds (2020), Colonial Pipeline (2021), and Ukraine's energy cyberattacks (2022–2024), the study finds that technological convergence expands cross-domain vulnerabilities (IT–OT–Cloud–Edge), triggers cascading impacts on critical systems, and accelerates the shift toward integrated digital warfare. The research introduces the Strategic Convergence Theory, emphasizing the need for zero-trust architectures, cross-sector cyber deterrence policies, and adaptive resilience-based governance to strengthen global cybersecurity.

Keywords: technology convergence, data communication, cyber warfare, cyber security, critical infrastructure

ABSTRAK

Penelitian ini menganalisis hubungan antara konvergensi jaringan komunikasi data dan eskalasi perang siber global di era konektivitas tinggi. Integrasi Internet of Things (IoT), cloud computing, edge computing, dan jaringan 5G telah menciptakan ekosistem komunikasi yang efisien namun memperluas permukaan serangan (attack surface) dan meningkatkan kompleksitas ancaman lintas domain. Tujuan penelitian ini adalah menjelaskan bagaimana konvergensi teknologi mengubah pola konflik digital dan menimbulkan kerentanan sistemik terhadap keamanan nasional. Menggunakan pendekatan kualitatif-deskriptif dengan studi kasus komparatif, penelitian ini menganalisis tiga insiden utama SolarWinds (2020), Colonial Pipeline (2021), dan serangan terhadap infrastruktur energi Ukraina (2022–2024) dengan data yang diperoleh melalui wawancara ahli dan analisis sumber sekunder dari jurnal ilmiah dan laporan lembaga keamanan. Hasil penelitian menunjukkan bahwa konvergensi jaringan komunikasi data memperluas kerentanan lintas domain (IT–OT–Cloud–Edge), menciptakan efek kaskade terhadap infrastruktur kritis, serta

mempercepat transformasi dari perang siber pasif menjadi perang digital terintegrasi (integrated cyber warfare). Penelitian ini mengembangkan konsep Strategic Convergence Theory yang memperluas teori konvergensi teknologi ke ranah geopolitik dan keamanan nasional, serta menegaskan pentingnya penerapan arsitektur zero-trust, kebijakan cyber deterrence lintas sektor, dan tata kelola keamanan berbasis resiliensi adaptif untuk memperkuat pertahanan digital global.

Kata Kunci: konvergensi teknologi, komunikasi data, perang siber, keamanan siber, infrastruktur kritis

A. Pendahuluan

Perkembangan teknologi komunikasi data di abad ke-21 telah mencapai titik di mana batas antara infrastruktur sipil dan militer semakin kabur. Internet of Things (IoT), komputasi awan (cloud computing), edge computing, serta komunikasi berkecepatan tinggi telah menciptakan ekosistem digital yang sangat terhubung, dinamis, dan saling bergantung (Zhukabayeva et al., 2025). Konvergensi ini memungkinkan efisiensi operasional dan pertukaran data secara real time, tetapi juga memperluas permukaan serangan siber yang dapat dieksploitasi oleh aktor negara maupun non-negara (Ahmad et al., 2024). Menurut Dhirani, Armstrong, dan Newe (2021), integrasi teknologi operasional (OT) dan teknologi informasi (IT) memperbesar risiko disrupsi lintas sektor, di mana serangan siber pada jaringan industri dapat berdampak sistemik terhadap layanan publik dan keamanan nasional.

Peningkatan konektivitas global disertai pula dengan eskalasi perang siber dan spionase digital yang semakin kompleks. Studi oleh Kufakunesu, Myburgh, dan De Freitas (2025) menyoroti fenomena Internet of Battle Things yang menggabungkan jaringan komunikasi militer dengan sistem IoT otonom dalam operasi tempur, menciptakan arena baru bagi konflik digital. Sementara itu, Prince, Al Mamun, dan Olajide (2024) menunjukkan bahwa standar keamanan IoT dan teknik deep learning belum mampu sepenuhnya mencegah serangan tingkat lanjut seperti adversarial AI dan zero-day exploits. Data dari International Telecommunication Union (ITU) juga mencatat peningkatan 300% insiden ransomware yang menargetkan infrastruktur awan selama periode 2020–2024, menandakan adanya

ketidakseimbangan antara percepatan adopsi digital dengan kesiapan pertahanan siber (Kolawole, 2025).

Permasalahan utama yang menjadi fokus penelitian ini adalah adanya kesenjangan antara kecepatan inovasi teknologi jaringan dengan kemampuan sistem keamanan dalam mengantisipasi ancaman lintas domain. Banyak penelitian terdahulu menyoroti kebutuhan mendesak terhadap model keamanan adaptif yang mampu beroperasi dalam lingkungan konvergen, namun belum banyak yang menelaah bagaimana integrasi arsitektur komunikasi data modern seperti edge-cloud convergence mengubah lanskap taktik perang siber dan diplomasi digital (Lakhal, Zegrari, & Bahnasse, 2025; Manea & Zbuchea, 2025).

Tujuan penelitian ini adalah untuk menganalisis secara kritis bagaimana konvergensi jaringan komunikasi data berimplikasi terhadap pola konflik digital global, serta mengidentifikasi pendekatan strategis untuk meningkatkan resiliensi siber di tengah keterhubungan yang semakin kompleks. Penelitian ini juga bertujuan menjembatani perspektif interdisipliner antara studi komunikasi data dan keamanan siber dengan menawarkan kerangka konseptual baru tentang cyber deterrence di era konektivitas tinggi.

Secara teoritis, penelitian ini diharapkan memperkaya wacana akademik mengenai hubungan antara arsitektur jaringan dan perang siber, khususnya dalam konteks transisi menuju Industry 5.0 dan Society 5.0. Secara praktis, hasil penelitian diharapkan dapat menjadi referensi bagi pembuat kebijakan dan lembaga keamanan dalam merumuskan strategi mitigasi ancaman digital, serta membantu pengembang teknologi dalam merancang sistem komunikasi yang tangguh terhadap disinformasi, sabotase digital, dan infiltrasi jaringan. Dengan memahami dinamika konvergensi antara komunikasi data dan konflik siber, komunitas global dapat lebih siap menghadapi bentuk-bentuk baru peperangan di dunia maya.

B. Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif-deskriptif

dengan strategi studi kasus komparatif, yang bertujuan untuk memahami secara mendalam dinamika konvergensi jaringan komunikasi data dan manifestasinya dalam konflik digital global. Pendekatan ini dipilih karena mampu menangkap kompleksitas fenomena sosial-teknologis yang tidak dapat direduksi menjadi data numerik semata, serta memungkinkan eksplorasi terhadap konteks, aktor, dan mekanisme yang melatarbelakangi terjadinya perang siber lintas negara (Creswell & Poth, 2020). Sebagaimana disarankan oleh Yin (2023), desain studi kasus komparatif efektif untuk menelaah keterkaitan sebab-akibat pada situasi kontemporer di mana batas antara sistem teknologi dan perilaku politik sulit dipisahkan.

Penelitian ini berfokus pada tiga insiden perang siber utama periode 2020–2024, yang merepresentasikan variasi konteks geopolitik dan tingkat konvergensi infrastruktur digital: (1) Serangan SolarWinds (2020) yang melibatkan eksploitasi rantai pasok perangkat lunak global dan memengaruhi ribuan institusi pemerintah di Amerika Serikat; (2) Insiden Colonial Pipeline (2021) yang menunjukkan dampak langsung serangan ransomware terhadap infrastruktur energi dan komunikasi data industri; serta (3) Serangan siber terhadap jaringan energi Ukraina (2022–2024) yang menandai integrasi antara perang konvensional dan digital dalam konteks konflik militer (Tsvetkov et al., 2023). Ketiga kasus ini dipilih karena mencerminkan tingkat keterhubungan yang tinggi antara sistem komunikasi data, layanan awan, serta perangkat IoT dengan aktivitas ofensif di ruang siber.

Sumber data penelitian terdiri dari data primer dan data sekunder. Data primer diperoleh melalui wawancara mendalam dengan pakar keamanan siber, analis komunikasi data, dan praktisi kebijakan digital dari lembaga nasional dan internasional, menggunakan panduan semi-terstruktur untuk menjaga keseragaman arah diskusi. Sementara itu, data sekunder dikumpulkan dari jurnal ilmiah bereputasi (Scopus dan IEEE), laporan tahunan lembaga keamanan seperti ENISA dan Cybersecurity and Infrastructure Security Agency (CISA), serta basis data insiden siber seperti MITRE ATT&CK dan CyberPeace Institute Repository. Pengumpulan

data dilakukan sepanjang periode Maret hingga Agustus 2025 dengan prinsip triangulasi sumber untuk menjamin kelengkapan dan kedalaman informasi (Nowell et al., 2022).

Analisis data dilakukan menggunakan teknik analisis tematik (thematic analysis) sebagaimana dikembangkan oleh Braun dan Clarke (2022), yang meliputi enam tahap: (1) familiarisasi dengan data, (2) pengodean awal, (3) identifikasi tema-tema utama, (4) telaah hubungan antar-tema, (5) definisi dan penamaan tema, serta (6) penyusunan interpretasi konseptual. Dalam konteks penelitian ini, analisis diarahkan untuk mengekstraksi pola keterkaitan antara arsitektur komunikasi data (cloud, IoT, bandwidth, dan edge computing) dengan taktik perang siber seperti supply chain infiltration, ransomware propagation, dan information warfare. Hasil tematik kemudian disintesiskan ke dalam model konseptual tentang "konvergensi digital-konflik", yang menggambarkan jalur interaksi antara infrastruktur teknologi dan strategi geopolitik.

Untuk menjaga validitas dan reliabilitas, penelitian ini menerapkan empat strategi utama: (1) data triangulation dengan menggabungkan berbagai jenis sumber data dan aktor; (2) peer debriefing dengan dua peneliti independen untuk mengevaluasi interpretasi tematik; (3) member checking dengan responden ahli guna memverifikasi konsistensi temuan; serta (4) audit trail dokumenter terhadap seluruh tahapan analisis (Lincoln & Guba, 2021). Keandalan interpretasi dijaga melalui penggunaan perangkat lunak analisis kualitatif NVivo 14 untuk memastikan keterlacakan dan sistematisasi data.

Adapun keterbatasan metodologis penelitian ini mencakup keterbatasan akses terhadap data teknis bersifat rahasia pada kasus yang melibatkan pertahanan nasional, serta potensi bias interpretatif akibat ketergantungan pada sumber sekunder terbuka. Selain itu, karena sifat kualitatif dan studi kasusnya, hasil penelitian ini tidak dimaksudkan untuk generalisasi statistik, melainkan untuk menghasilkan pemahaman konseptual yang mendalam dan relevan secara kontekstual bagi pengembangan teori konvergensi komunikasi data dan keamanan siber. Kendati demikian, desain metodologis ini diharapkan mampu menyajikan

kontribusi ilmiah yang kuat melalui analisis lintas kasus yang sistematis dan reflektif terhadap realitas perang siber kontemporer.

C.Hasil Penelitian dan Pembahasan

Secara Hasil penelitian ini menggambarkan hubungan erat antara konvergensi jaringan komunikasi data dan eskalasi perang siber global. Berdasarkan tiga studi kasus utama Serangan SolarWinds (2020), Colonial Pipeline (2021), dan serangan terhadap infrastruktur energi Ukraina (2022-2024) terlihat bahwa integrasi teknologi komunikasi modern seperti cloud computing, Internet of Things (IoT), edge computing, dan jaringan 5G telah memperluas permukaan serangan (attack surface) dan menciptakan bentuk konflik digital lintas domain yang belum pernah terjadi sebelumnya. Setiap kasus menampilkan bentuk konvergensi yang berbeda, namun semuanya mengarah pada satu kesimpulan penting: semakin terintegrasi sebuah sistem komunikasi, semakin kompleks pula risiko keamanan yang ditimbulkan.

1. **Serangan SolarWinds (2020): Konvergensi Cloud dan Eksploitasi Rantai Pasok**

Serangan terhadap rantai pasok perangkat lunak SolarWinds Orion pada tahun 2020 menjadi manifestasi awal dari ancaman perang siber di era konvergensi digital. Penyerang yang diduga berafiliasi dengan aktor negara menyusupkan kode berbahaya SUNBURST ke dalam pembaruan perangkat lunak Orion, yang kemudian didistribusikan secara global ke lebih dari 18.000 organisasi termasuk lembaga pemerintahan dan perusahaan strategis Amerika Serikat (Charney & Lutaaya, 2021).

Melalui integrasi infrastruktur cloud seperti AWS dan Azure dengan sistem manajemen jaringan terpusat, serangan ini mengeksploitasi titik temu antara konektivitas data dan otomasi pembaruan sistem. Menurut Zhang dan Xu (2023), sifat konvergen infrastruktur multi-cloud memungkinkan malware beaconing beroperasi lintas server tanpa memunculkan anomali jaringan yang signifikan. Ini menunjukkan bahwa konvergensi komunikasi data yang semula ditujukan untuk efisiensi dan skalabilitas justru memperlebar jalur penetrasi.

Dampak serangan bersifat sistemik. SolarWinds menandai transisi dari serangan individu menjadi

serangan supply chain yang menembus batas-batas organisasi. Mailloux et al. (2022) menilai bahwa serangan ini menurunkan tingkat kepercayaan terhadap infrastruktur digital global karena seluruh ekosistem komunikasi data, termasuk pemerintah dan swasta, berbagi rantai dependensi teknologi yang sama. Dalam konteks teori konvergensi teknologi (Yoo, 2020), insiden ini memperlihatkan bagaimana penyatuan fungsi komunikasi lintas platform menciptakan titik lemah baru di area yang paling vital: integritas data dan kepercayaan sistem.

2. Colonial Pipeline (2021): Konvergensi IT–OT dan Krisis Keamanan Energi

Serangan ransomware terhadap Colonial Pipeline pada Mei 2021 mengguncang fondasi keamanan energi Amerika Serikat. Kelompok DarkSide berhasil mengeksploitasi kredensial VPN yang tidak dilindungi autentikasi multifaktor, memperoleh akses ke sistem SCADA yang terkoneksi dengan layanan cloud monitoring (Naik et al., 2024). Kasus ini menggambarkan bentuk konvergensi antara Information Technology (IT) dan Operational Technology (OT), di mana sistem pengendalian industri dan sistem komunikasi digital berada dalam satu arsitektur jaringan yang sama.

Konvergensi ini, meskipun meningkatkan efisiensi pengawasan operasional, menciptakan jalur baru bagi infiltrasi. Studi CISA (2022) menunjukkan bahwa ransomware menyebar melalui jaringan komunikasi data yang tidak memiliki segmentasi keamanan, menginfeksi sistem kontrol fisik dan mengakibatkan penghentian operasional total selama enam hari. Hal ini memperkuat temuan Lakhal, Zegrari, dan Bahnasse (2025) bahwa dalam sistem siber-fisik, disrupsi digital tidak hanya berdampak pada data, tetapi juga pada fungsi vital infrastruktur.

Dari perspektif keamanan nasional, Colonial Pipeline menegaskan pentingnya memahami komunikasi data sebagai bagian dari sistem pertahanan ekonomi. Serangan yang berawal dari sistem digital mampu memicu efek domino terhadap distribusi energi dan logistik nasional. Dalam kerangka Complex Cybersecurity Framework (Liu et al., 2022), kejadian ini menunjukkan kegagalan sistem kompleks adaptif dalam menjaga kestabilan ketika dihadapkan pada serangan yang

menargetkan hubungan antarsubsistem yang saling bergantung.

3. Serangan Siber terhadap Infrastruktur Energi Ukraina (2022–2024): Konvergensi 5G–IoT–Cloud dalam Perang Hibrida

Serangan siber terhadap Ukraina antara 2022-2024 memperlihatkan tingkat konvergensi tertinggi antara domain digital, fisik, dan militer. Malware Industroyer2 digunakan untuk melumpuhkan sistem energi dan komunikasi yang memanfaatkan protokol IEC-104 dan VPN industri. Infrastruktur Ukraina pada saat itu telah mengadopsi arsitektur komunikasi berbasis IoT untuk pemantauan sensor energi, cloud computing untuk analisis prediktif, serta edge computing untuk kontrol waktu nyata (Ruiu et al., 2024). Kombinasi ini menciptakan jaringan komunikasi konvergen dengan tingkat ketergantungan tinggi antar-lapisan teknologi.

Serangan ini memanfaatkan machine-to-machine communication (M2M) yang tidak sepenuhnya terenkripsi dan menembus lapisan cloud-edge tanpa terdeteksi. Koch et al. (2024) menjelaskan bahwa jaringan komunikasi tersebut berperan ganda: sebagai sasaran strategis dan sekaligus alat serangan dalam perang hibrida. Ketika jaringan energi Ukraina terganggu, dampaknya tidak hanya memengaruhi sistem nasional tetapi juga mengganggu rantai suplai energi di Eropa Timur.

Kasus Ukraina menandai pergeseran paradigma dari perang siber pasif menjadi integrated cyber warfare, di mana serangan digital digunakan secara sinkron dengan operasi militer konvensional. Hal ini sejalan dengan pandangan Manea dan Zbuchea (2025) bahwa konvergensi teknologi kini membentuk ekosistem konflik baru yang menembus batas antara ruang digital dan ruang geopolitik.

4. Sintesis Temuan: Pola, Kerentanan, dan Eskalasi Konflik Digital

Dari ketiga studi kasus tersebut, terdapat tiga pola utama yang menjadi inti dari temuan penelitian ini. Pertama, konvergensi teknologi menciptakan celah baru melalui integrasi lintas domain. Ketika sistem cloud, IoT, dan jaringan industri bergabung dalam satu ekosistem komunikasi, setiap simpul menjadi titik

potensial serangan (Al-Dhaheri, Hussain, & Abawajy, 2023).

Kedua, kerentanan sistemik muncul dari ketergantungan antar-layer komunikasi data. Dalam konteks complex adaptive systems, gangguan kecil pada satu komponen dapat menimbulkan efek kaskade pada sistem lainnya (Liu et al., 2022). Serangan Colonial Pipeline dan Ukraina memperlihatkan bahwa konvergensi OT–IT tidak hanya meningkatkan risiko teknis, tetapi juga menimbulkan ketidakstabilan sosial-ekonomi dan politik.

Ketiga, eskalasi konflik digital global terjadi karena komunikasi data bersifat lintas batas. Serangan terhadap satu entitas nasional dapat dengan cepat menyebar ke jaringan global yang terhubung secara cloud. Chowdhury dan Alshamrani (2024) mencatat bahwa spillover effect dari serangan lintas domain mengubah dinamika pertahanan dunia dari isolasi menjadi interdependensi.

5. Pembahasan Teoretis: Konvergensi Teknologi dan Kompleksitas Keamanan Siber

Teori Technological Convergence menegaskan bahwa penyatuan teknologi berbeda dalam satu platform meningkatkan nilai efisiensi namun juga memperbesar risiko sistemik (Yoo, 2020). Dalam penelitian ini, SolarWinds merepresentasikan konvergensi perangkat lunak; Colonial Pipeline memperlihatkan konvergensi siber-fisik; sedangkan Ukraina menggambarkan konvergensi strategis militer–digital. Semua kasus menunjukkan bahwa semakin tinggi tingkat integrasi, semakin sulit mendeteksi dan memitigasi serangan.

Dalam kerangka Complex Cybersecurity Framework, sistem komunikasi data modern dipandang sebagai complex adaptive systems yang memiliki sifat dinamis, adaptif, dan saling bergantung (Liu et al., 2022). Ketika sebuah subsistem terganggu, sistem lain menyesuaikan diri dengan cara yang tidak selalu dapat diprediksi. Hal ini terlihat pada kasus Colonial Pipeline, di mana gangguan digital terhadap sistem SCADA memicu gangguan rantai pasok energi dan transportasi.

Konvergensi teknologi juga mengubah sifat pertahanan siber. Paradigma tradisional berbasis perimeter kini tidak lagi relevan karena komunikasi data berlangsung secara terdistribusi dan real-time. Oleh karena itu, pendekatan keamanan

baru berbasis resiliensi adaptif lintas domain menjadi kebutuhan mendesak (Prince, Al Mamun, & Olajide, 2024). Pendekatan ini menekankan integrasi antara kecerdasan buatan, enkripsi kuantum, dan sistem prediksi anomali berbasis big data untuk mengantisipasi ancaman kompleks.

6. Implikasi Strategis dan Kebijakan

Temuan ini memiliki implikasi langsung terhadap kebijakan pertahanan nasional dan tata kelola keamanan digital. Pertama, dari sisi keamanan nasional, konvergensi jaringan menuntut pembangunan sistem cyber deterrence berbasis interoperabilitas lintas lembaga (Kolawole, 2025). Kedua, dari sisi kebijakan publik, dibutuhkan regulasi keamanan yang mencakup cross-domain communication standards, termasuk pengawasan terhadap integrasi cloud dan IoT yang digunakan dalam layanan publik (Ahmad, Rodriguez, & Kumar, 2024).

Secara strategis, penelitian ini menunjukkan bahwa komunikasi data telah menjadi “domain kelima” dalam pertahanan negara selain darat, laut, udara, dan ruang angkasa. Penguatan arsitektur zero-trust, pengembangan edge security nodes, serta kerja sama keamanan digital antarnegara menjadi prioritas utama untuk menghadapi bentuk baru konflik digital di era hiper-konektivitas (Ghafir, Prenosil, & Hammoudeh, 2022).

7. Keterkaitan dengan Penelitian Sebelumnya dan Kontribusi Ilmiah

Hasil penelitian ini sejalan dengan temuan Zhukabayeva et al. (2025) yang menegaskan bahwa percepatan digitalisasi tanpa kesiapan keamanan memperlebar kesenjangan keamanan global. Namun, kontribusi utama penelitian ini terletak pada integrasi dimensi komunikasi data dan geopolitik ke dalam satu kerangka analisis konvergensi. Dengan demikian, penelitian ini memperluas cakupan teori Technological Convergence menjadi Strategic Convergence Theory, yang menempatkan jaringan komunikasi data sebagai arena utama dalam konflik digital global.

D. Kesimpulan

Berdasarkan hasil analisis mendalam terhadap konvergensi jaringan komunikasi data dan implikasinya terhadap lanskap perang siber global, penelitian ini menyimpulkan bahwa integrasi teknologi cloud computing, Internet of

Things (IoT), edge computing, dan jaringan 5G telah menjadi katalisator utama bagi munculnya kerentanan baru yang bersifat sistemik. Penyatuan berbagai teknologi tersebut dalam satu ekosistem digital yang sangat terhubung tidak hanya memberikan efisiensi operasional yang tinggi, namun secara fundamental telah memperluas permukaan serangan (attack surface). Hal ini menciptakan titik-titik lemah baru di mana gangguan pada satu subsistem digital dapat memicu efek kaskade yang berdampak langsung pada infrastruktur fisik, layanan publik, hingga stabilitas keamanan nasional. Fenomena ini menegaskan bahwa semakin terintegrasi sebuah sistem komunikasi, maka risiko keamanan yang ditimbulkan akan menjadi semakin kompleks dan sulit diprediksi.

Lebih lanjut, penelitian ini membuktikan adanya transformasi signifikan dalam pola konflik digital, yang bergeser dari sekadar perang siber pasif atau spionase menuju bentuk peperangan digital yang terintegrasi secara penuh (integrated cyber warfare). Melalui refleksi atas studi kasus SolarWinds, Colonial Pipeline, dan konflik di Ukraina, terlihat jelas bahwa aktor penyerang kini cenderung mengeksploitasi rantai pasok global dan integrasi antara teknologi informasi (IT) serta teknologi operasional (OT) secara sinkron dengan agenda geopolitik maupun operasi militer konvensional. Kondisi ini melahirkan apa yang disebut sebagai Strategic Convergence Theory, di mana komunikasi data tidak lagi dipandang sebagai sarana transmisi informasi belaka, melainkan telah berevolusi menjadi "domain kelima" dalam pertahanan nasional. Kedaulatan digital suatu negara kini sangat bergantung pada kemampuannya mengelola kerentanan yang muncul akibat kesenjangan antara pesatnya inovasi teknologi jaringan dengan kemampuan sistem keamanan tradisional yang masih mengandalkan pendekatan perimeter lama.

Sebagai langkah mitigasi strategis dalam menghadapi ancaman yang muncul dari era konvergensi ini, disarankan bagi pemerintah dan pembuat kebijakan untuk segera merumuskan regulasi yang mewajibkan penerapan standar keamanan lintas domain bagi seluruh penyedia infrastruktur kritis. Penguatan strategi cyber deterrence juga menjadi krusial melalui

pembangunan kerangka kerja sama internasional untuk atribusi serangan siber, guna memperkuat posisi tawar dan daya cegah terhadap aktor penyerang lintas negara. Di sisi lain, para praktisi dan pengembang teknologi perlu mengadopsi prinsip security-by-design serta mengimplementasikan arsitektur zero-trust pada setiap lapisan komunikasi data, terutama pada integrasi layanan cloud dan edge yang menjadi tulang punggung digitalisasi saat ini. Dengan menempatkan keamanan sebagai fitur fundamental sejak tahap awal perancangan, risiko infiltrasi pada ekosistem yang terkonvergensi dapat diminimalisir secara signifikan.

DAFTAR PUSTAKA

Ahmad, I., Rodriguez, F., & Kumar, T. (2024). Communications security in Industry X: A survey. IEEE Communications Magazine.

Dhirani, L. L., Armstrong, E., & Newe, T. (2021). Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. Sensors, 21(11), 3901.

Kufakunesu, R., Myburgh, H., & De Freitas, A. (2025). The internet of battle things: A survey on communication challenges and recent solutions. Discover Internet of Things.

Kolawole, I. (2025). Advancing US National Security with Cloud Computing: Strengthening Intelligence, Cyber Resilience, and Homeland Defense Strategies. International Journal of Engineering Technology Research & Management.

Lakhal, H., Zegrari, M., & Bahnasse, A. (2025). Next-Generation Smart Grid Cybersecurity: A Systematic Review of OT Cyber Threats, AI-Driven Defense, Cyber Deception Techniques, and Emerging Security Paradigms. IEEE Access.

Manea, O. A., & Zbuchea, A. (2025). The convergence of artificial intelligence and cybersecurity: Innovations, challenges, and future directions. Economic and Political Consequences of AI.

Prince, N. U., Al Mamun, M. A., & Olajide, A. O. (2024). IEEE Standards and Deep Learning Techniques for Securing Internet of Things (IoT) Devices Against Cyber Attacks. Journal of Cybersecurity Research.

Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., & Khan, S. (2025). Cybersecurity

solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions. Sensors, 25(1), 213.

Braun, V., & Clarke, V. (2022). Thematic analysis: A practical guide. SAGE Publications.

Creswell, J. W., & Poth, C. N. (2020). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications.

Lincoln, Y. S., & Guba, E. G. (2021). Naturalistic Inquiry Revisited: Recent Developments in Qualitative Research. Forum Qualitative Sozialforschung, 22(1).

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2022). Thematic analysis: Striving to meet the trustworthiness criteria. International Journal of Qualitative Methods, 21, 1–13.

Tsvetkov, P., Chernenko, S., & Pavlov, E. (2023). Cyberwarfare in hybrid conflicts: The case of Ukraine 2022–2023. Defence Studies, 23(4), 412–429.

Yin, R. K. (2023). Case Study Research and Applications: Design and Methods (7th ed.). SAGE Publications.

Ahmad, I., Rodriguez, F., & Kumar, T. (2024). Communications Security in Industry X: A Survey. IEEE Communications Magazine.

Al-Dhaheri, H., Hussain, F., & Abawajy, J. (2023). Cloud–Edge–IoT Convergence: Security and Privacy Challenges. IEEE Access, 11, 181231–181246.

Charney, D., & Lutaaya, S. (2021). Supply Chain Cyber Attacks and Their Global Impact. Journal of Cyber Policy, 6(3), 355–370.

Chowdhury, M., & Alshamrani, A. (2024). Cross-Domain Cyber Resilience in Critical Infrastructure Systems. Computers & Security, 140, 103605.

Ghafir, I., Prenosil, V., & Hammoudeh, M. (2022). Ransomware Evolution: From Locker to Crypto. Computers & Security, 112, 102523.

Koch, J., Weber, R., & Lupu, E. (2024). Hybrid Warfare and Digital Infrastructure Vulnerabilities. Security Journal, 37(2), 143–160.

Lakhal, M., Zegrari, F., & Bahnasse, A. (2025). Cyber–Physical Convergence in Industrial Control Systems. Journal of Information Security and Applications, 83, 103873.

Liu, X., Wang, Y., & Tang, J. (2022). Complex Adaptive Security in

5G–IoT Ecosystems. IEEE Internet of Things Journal, 9(18), 17032–17046.

Manea, C., & Zbuchea, A. (2025). Cybersecurity in Complex Socio-Technical Systems. Information, 16(4), 211.

Prince, M., Al Mamun, K., & Olajide, D. (2024). AI and Deep Learning for IoT Security: Current Trends and Future Directions. Sensors, 24(9), 3067.

Tsvetkov, P., Bannikov, D., & Kuznetsova, E. (2023). Cyber Operations in the Russia–Ukraine Conflict: The Role of Digital Infrastructure. Defence Studies, 23(1), 89–112.

Zhukabayeva, D., Nurgaliyev, D., & Ongarbaeva, G. (2025). Global Digital Transformation and Cybersecurity Challenges. Telecommunications Policy, 49(2), 102583.