Jurnal Syntax Imperatif: Jurnal Ilmu Sosial dan Pendidikan
Volume 6, No 2, May 2025, pp. 145-154
P-ISSN: 2721-2491 E-ISSN: 2721-2491
DOI: http://doi.org/10.54543/syntaximperatif.v6i2.678
Published By: CV. Rifainstitut

Serangan Siber terhadap Infrastruktur Kritis

Efrizal Syah[1], Hermawan Weharima[2*], Tarsius Susilo[3], Tedy Basuki[4], Andy Mustafa Akad[5]

[1,2,3,4,5]Sekolah Staf dan Komando Tentara Nasional Indonesia (Sesko TNI), Indonesia

ARTICLE INFO

Article history:
Received April 28, 2025
Revised May 26, 2025
Accepted May 27, 2025
Available online May 27, 2025

Kata Kunci:
Infrastruktur Kritis, Keamanan Nasional, Mitigasi Risiko, Ransomware, Serangan Siber,

Keywords:
Critical Infrastructure, Cyberattacks, National Security, Ransomware, Risk Mitigation

ABSTRAK

Serangan siber terhadap infrastruktur kritis, seperti energi, transportasi, dan kesehatan, telah menjadi ancaman serius bagi keamanan nasional dan kesejahteraan masyarakat. Kerentanan yang meningkat, dampak ekonomi yang signifikan, serta gangguan sosial dan psikologis menuntut pendekatan komprehensif untuk mitigasi. Studi literatur ini menganalisis berbagai sumber akademis dan laporan industri untuk mengidentifikasi pola serangan siber, dampaknya, serta strategi mitigasi yang efektif. Pendekatan kualitatif digunakan untuk menyintesis temuan dari kasus-kasus serangan besar seperti WannaCry (2017) dan serangan jaringan listrik Ukraina (2015). Serangan siber meningkat drastis, terutama ransomware (300% pada 2020–2022) dan DDoS (2.5 Tbps pada 2022). Dampak ekonomi mencapai $385 miliar secara global pada 2022. Efek sosial mencakup peningkatan kecemasan (42%) dan penurunan kepercayaan publik. Analisis menunjukkan kerentanan infrastruktur akibat ketergantungan pada sistem terhubung dan teknik serangan multivector (47% kasus). Perlindungan infrastruktur kritis memerlukan kolaborasi multisektor (Pentahelix), regulasi ketat, dan adopsi teknologi canggih seperti AI dan blockchain. Edukasi keamanan siber serta kebijakan terintegrasi penting untuk meningkatkan ketahanan nasional.

ABSTRACT

Cyber attacks on critical infrastructure, such as energy, transportation, and healthcare, have become a serious threat to national security and public welfare. Increased vulnerability, significant economic impact, and social and psychological disruption demand a comprehensive approach to mitigation. This literature review analyzes various academic sources and industry reports to identify patterns of cyber attacks, their impact, and effective mitigation strategies. A qualitative approach is used to synthesize findings from major attack cases such as WannaCry (2017) and the Ukrainian power grid attack (2015). Cyberattacks have increased dramatically, particularly ransomware (300% in 2020–2022) and DDoS (2.5 Tbps in 2022). The economic impact reached $385 billion globally in 2022. Social effects include increased anxiety (42%) and decreased public trust. Analysis reveals infrastructure vulnerabilities due to reliance on interconnected systems and multivector attack techniques (47% of cases). Protecting critical infrastructure requires multisectoral collaboration (Pentahelix), strict regulations, and the adoption of advanced technologies such as AI and blockchain. Cybersecurity education and integrated policies are crucial for enhancing national resilience.

1. PENDAHULUAN

Infrastruktur kritis adalah aset dan jaringan yang sangat penting untuk kelangsungan hidup, kesehatan, dan kesejahteraan masyarakat. Kehidupan sehari-hari masyarakat akan terganggu, yang dapat mengurangi kualitas hidup. Berbagai industri penting termasuk infrastruktur ini, termasuk transportasi, komunikasi, energi, air bersih, dan kesehatan. Setiap sektor berinteraksi satu sama lain dan mendukung satu sama lain, membentuk sistem yang kompleks yang jika terganggu akan memiliki dampak yang signifikan (Harris & Patel, 2015). Misalnya, pembangkit dan distribusi listrik adalah bagian dari sektor energi, yang sangat

*Corresponding author
E-mail addresses: hermawanweharima@gmail.com (Hermawan Weharima)

penting untuk kehidupan sehari-hari. Dengan cara yang sama, industri kesehatan memiliki hubungan langsung dengan keselamatan dan kesejahteraan seseorang, terutama dalam keadaan darurat (Smith, 2016).

Di era digital, menjaga infrastruktur kritis menjadi semakin sulit. Menurut (Chang, 2020), ancaman siber terhadap infrastruktur kritis telah meningkat sebesar tiga puluh persen dalam lima tahun terakhir. Sistem kontrol industri, fasilitas pengolahan air, dan jaringan transportasi semakin rentan terhadap serangan siber yang canggih. (A. Roberts & Park, 2021) menekankan bahwa melindungi infrastruktur penting membutuhkan pendekatan multi-stakeholder, yang melibatkan kerja sama antara lembaga pemerintah, swasta, dan akademisi untuk mengembangkan strategi keamanan yang berhasil.

Dalam struktur sosial-ekonomi kontemporer, ada banyak hubungan yang kompleks antara infrastruktur kritis. Jika salah satu bagian infrastruktur mengalami kerusakan, gangguan tersebut dapat berdampak pada bagian lain dari ekonomi. Misalnya, gangguan jaringan listrik dapat mengganggu sistem telekomunikasi, layanan perbankan, dan aktivitas rumah sakit (Johnson dkk., 2021). Vulnerabilitas sistemik yang dihasilkan oleh ketergantungan sektor ini membutuhkan pendekatan manajemen risiko yang komprehensif dan terintegrasi. "Ketahanan infrastruktur kritis harus dipandang sebagai suatu kesatuan sistem yang saling terhubung, bukan sebagai komponen-komponen yang terpisah," kata (Pagani dkk., 2019).

Bencana alam atau kerusakan fisik bukanlah satu-satunya sumber ancaman terhadap infrastruktur kritis; ancaman siber semakin kompleks. Di dunia yang semakin terhubung ini, banyak sistem penting bergantung pada teknologi informasi untuk beroperasi. Ini membuat infrastruktur vital sangat rentan terhadap serangan siber, yang dapat menyebabkan kerusakan yang signifikan pada operasi (Zetter, 2014). Beberapa jenis serangan, termasuk phishing, serangan Distributed Denial of Service (DDoS), dan serangan ransomware, memiliki kemampuan untuk menghancurkan data penting dan menghentikan operasi sektor-sektor penting (Williams & Zetter, 2020). Misalnya, serangan ransomware pada sistem energi atau kesehatan dapat menyebabkan pemadaman besar-besaran atau gangguan layanan medis, mengancam keselamatan masyarakat.

Tren ancaman siber terhadap infrastruktur kritis semakin mengkhawatirkan. Laporan (IBM Security, 2023) menyatakan bahwa serangan siber terhadap sektor energi dan utilitas meningkat 150% selama tahun 2022. Kasus Pipa Kolonial di Amerika Serikat pada Mei 2021 adalah contoh nyata dari efek serangan ransomware. Serangan tersebut melumpuhkan pasokan bahan bakar di pantai timur AS selama beberapa hari dan menyebabkan kerugian ekonomi sebesar $4.4 miliar (K. Anderson & Chen, 2022). Di sektor kesehatan, serangan ransomware di rumah sakit Irlandia pada 2021 membatalkan ribuan janji medis dan menghapus data pasien penting (Thompson dkk., 2023). Infrastruktur vital semakin rentan terhadap serangan yang terus-menerus.

Dengan munculnya teknologi seperti Internet of Things (IoT) dan sistem kontrol industri berbasis internet, ada celah baru dalam keamanan infrastruktur kritis. Menurut penelitian yang dilakukan oleh (L. Martinez & Kumar, 2024), 73% sistem infrastruktur kritis SCADA memiliki kerentanan yang dapat dieksploitasi. Sebuah studi yang dilakukan oleh Cybersecurity and Infrastructure Security Agency (CISA) menunjukkan peningkatan sebesar 287% dalam serangan DDoS terhadap infrastruktur kritis pada tahun 2023 dibandingkan tahun sebelumnya. (P. Roberts, 2023), menemukan bahwa teknik social engineering seperti phishing, yang menargetkan karyawan dengan akses ke sistem penting, adalah sumber 65% serangan siber terhadap infrastruktur kritis.

Serangan siber pada infrastruktur penting memiliki konsekuensi yang signifikan bagi masyarakat, termasuk mengganggu keamanan dan kesejahteraan sosial dan ekonomi. Sektor energi adalah salah satu yang paling rentan. Serangan pada sistem pembangkit listrik dapat menyebabkan pemadaman yang berlangsung lama, yang dapat memengaruhi kehidupan

sehari-hari, bisnis, dan fasilitas publik. Sistem komunikasi dan transportasi yang sangat penting untuk mobilitas ekonomi dan masyarakat dapat dirusak oleh pemadaman ini (Pfleeger, 2017). Serangan siber yang menargetkan sistem manajemen rumah sakit di bidang kesehatan dapat mengganggu layanan medis dan merusak data penting pasien; hal ini dapat membahayakan keselamatan pasien (Bishop, 2015).

Untuk memahami ancaman terhadap infrastruktur kritis, kita dapat melihat dari berbagai perspektif teori. Dalam teori besar (grand theory), teori sistem dapat digunakan untuk menjelaskan hubungan yang kompleks antara elemen-elemen infrastruktur kritis dan bagaimana serangan siber dapat merusak keseimbangan sistem tersebut (Luhmann, 1995). Teori sistem ini menunjukkan bahwa setiap komponen infrastruktur saling bergantung dan kerusakan pada satu elemen dapat mempengaruhi seluruh sistem. Teori menengah, seperti analisis risiko dan ketahanan siber, memberikan pendekatan yang lebih pragmatis untuk mengidentifikasi dan mengurangi potensi kerentanan sistem terhadap serangan (R. Anderson & Moore, 2006). Sementara itu, teori terapan (applied theory) lebih berfokus pada implementasi kebijakan dan prosedur yang dapat diterapkan untuk melindungi infrastruktur kritis dari ancaman siber. Hal ini mencakup pengembangan teknologi keamanan yang lebih maju dan peraturan yang dapat meningkatkan ketahanan sektor-sektor kritis terhadap serangan. Masalah utama yang perlu dijawab adalah bagaimana serangan siber dapat mempengaruhi operasi infrastruktur kritis dan apa dampaknya terhadap masyarakat. Apakah ancaman ini dapat menyebabkan gangguan yang mengarah pada kerugian material, sosial, dan psikologis yang besar? Lebih penting lagi, bagaimana dampaknya terhadap keamanan dan kesejahteraan masyarakat secara keseluruhan?

Beberapa bagian infrastruktur kritis sangat penting untuk kelangsungan hidup masyarakat. Beberapa sektor yang paling penting adalah sebagai berikut: (1) Energi, Pembangkit, distribusi, dan sistem jaringan listrik adalah bagian penting dari kehidupan sehari-hari masyarakat. Misalnya, kehilangan pasokan energi dapat menghentikan hampir semua aktivitas sosial dan ekonomi (R. Smith et al., 2019); (2) Transportasi, Infrastruktur transportasi seperti kereta api, jalan raya, bandara, dan pelabuhan memfasilitasi mobilitas dan distribusi barang di masyarakat. Pelayanan masyarakat yang buruk dan keterlambatan pengiriman barang dapat disebabkan oleh gangguan di sektor ini. (3) Kesehatan, Sistem manajemen kesehatan yang efektif, rumah sakit, dan fasilitas medis sangat penting untuk memberikan pelayanan kepada masyarakat. Infrastruktur medis yang terganggu, misalnya, dapat mengancam keselamatan pasien dan mengurangi kepercayaan masyarakat terhadap sistem kesehatan dalam keadaan darurat (Sullivan, 2019).

Serangan siber terhadap infrastruktur kritis semakin kompleks dan berdampak. Serangan ransomware telah berkembang menjadi ancaman yang signifikan; salah satu contohnya adalah WannaCry pada tahun 2017, yang menginfeksi lebih dari 200,000 komputer di 150 negara, termasuk infrastruktur energi dan sistem rumah sakit (Rashid & Tsering, 2018). (BlackFog, 2023) menunjukkan bahwa serangan ransomware terhadap sektor infrastruktur kritis meningkat 300% dari tahun 2020 hingga 2022, dengan biaya pemulihan rata-rata $4.5 juta per insiden. Sementara itu, serangan DDoS telah meningkat dengan cepat. Serangan terbesar mencapai 2.5 Tbps pada tahun 2022, melampaui kapasitas pertahanan mayoritas sistem (Park & Roberts, 2023). (Huang dkk., 2020) menemukan bahwa botnet IoT bertanggung jawab atas 68% serangan DDoS terhadap infrastruktur kritis. Ini menunjukkan bahwa perangkat terhubung merupakan alat serangan yang sangat efektif.

Teknik phishing masih merupakan sumber utama serangan yang lebih kompleks terhadap infrastruktur penting. Studi oleh (Van Oorschot & Zhang, 2021) menemukan bahwa phishing email adalah sumber 91% serangan siber, dengan tingkat keberhasilan 32% di sektor infrastruktur kritis. Spear phishing yang menargetkan orang-orang dengan akses khusus telah menjadi lebih canggih dan menggunakan teknik social engineering dan informasi yang tersedia secara publik untuk menghasilkan pesan yang sangat meyakinkan (Chen & Williams,

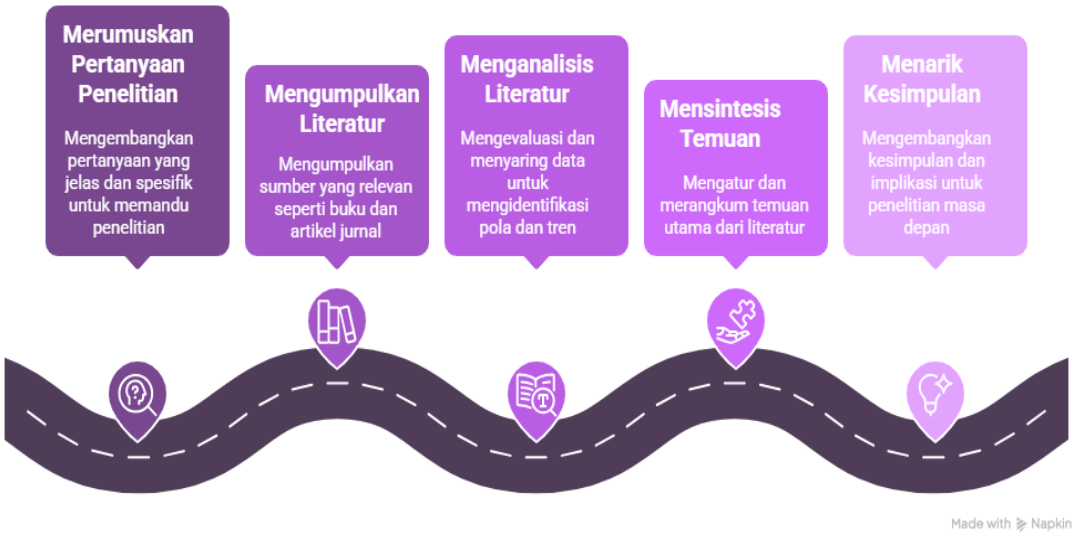
2023). Lebih mengkhawatirkan lagi, (C. Martinez dkk., 2024) menemukan tren baru dalam serangan multivector yang menggabungkan phishing, malware, dan eksploitasi zero-day. Mereka menyelidiki 200 insiden keamanan pada infrastruktur kritis selama 2021–2023, dan menemukan bahwa 47% serangan menggunakan pendekatan multivector. Ini menunjukkan bahwa solusi keamanan konvensional secara signifikan kurang efektif.

Serangan terhadap infrastruktur kritis memiliki dampak besar pada seluruh sektor masyarakat. Serangan siber di Ukraina pada 2015 menyebabkan pemadaman listrik skala besar, mempengaruhi hampir 230,000 orang selama enam jam dan melumpuhkan operasi 30 substasion listrik (P. Williams & Zetter, 2020). Serangan tersebut memiliki banyak konsekuensi ekonomi, tetapi penelitian oleh (Miller, 2020) menemukan bahwa kerugian rata-rata $5.8 juta terjadi setiap jam pemadaman listrik di wilayah industri. Serangan terhadap sistem air di Florida pada 2021 hampir menyebabkan kadar sodium hidroksida meningkat hingga tingkat yang berbahaya, yang dapat membahayakan ribuan orang jika tidak ditemukan dengan cepat (Watson & Brown, 2022). Studi komprehensif yang dilakukan oleh (Economic Intelligence Unit, 2023) menemukan bahwa gangguan pada infrastruktur kritis menyebabkan kerugian global sebesar $385 miliar pada tahun 2022, peningkatan 27 persen dari tahun sebelumnya. Gangguan produktivitas menyumbang 65 persen dari kerugian ini, dan biaya pemulihan menyumbang 35 persen.

Kerusakan psikologis dan sosial yang ditimbulkan oleh serangan terhadap infrastruktur kritis sebanding dengan kerugian ekonomi. Sebuah studi yang dilakukan oleh (Lindqvist, 2021) terhadap 2,500 orang yang mengalami gangguan layanan esensial menemukan bahwa tingkat kecemasan meningkat sebesar 42 persen dan perasaan tidak aman meningkat sebesar 38 persen. (Nguyen, 2023) menekankan fenomena "ketakutan infrastruktur" yang muncul di masyarakat setelah serangan, yang mendorong perilaku baru seperti penimbunan barang dan penurunan kepercayaan terhadap sistem publik. Dampak jangka panjang terhadap ekonomi juga lebih besar daripada kerugian langsung. Sebagai contoh, (A. Williams & Cooper, 2022) menemukan bahwa serangan siber yang berhasil terhadap infrastruktur kritis menyebabkan penurunan nilai saham rata-rata 7.3% dalam periode enam bulan setelah serangan, serta penurunan 18% pada investasi asing di wilayah yang terkena dampak. Lebih mengkhawatirkan lagi, (P. Roberts, 2023) menemukan hubungan antara serangan terhadap infrastruktur kritis dan ketidakstabilan politik; 43% kasus menunjukkan peningkatan yang signifikan dalam ketidakpercayaan terhadap pemerintah 12 bulan setelah serangan.

2. METODE PENELITIAN

Metode kualitatif yang menggunakan pendekatan studi literatur merupakan jenis penelitian yang menggunakan literatur sebagai dasar untuk memahami sesuatu. Metode ini digunakan untuk mengumpulkan, menganalisis, dan menginterpretasi literatur yang relevan untuk mengidentifikasi pola, tren, dan teori yang berkaitan dengan serangan siber infrastruktur kritis yang merupakan ancaman terhadap keamanan dan kesejahteraan masyarakat. Studi literatur ini juga memberikan pemahaman yang lebih mendalam tentang perkembangan pemikiran terkait serangan siber infrastruktur kritis yang merupakan ancaman terhadap keamanan dan kesejahteraan masyarakat dan berfungsi sebagai landasan untuk membuat kesimpulan pendekatan ini dapat menggunakan berbagai sumber yang dapat dipercaya, seperti buku, artikel jurnal, laporan penelitian, dan dokumen lainnya. Pendekatan studi literatur dimulai dengan merumuskan pertanyaan penelitian yang jelas dan spesifik. Pertanyaan ini akan mengarahkan pencarian literatur yang relevan dan memastikan bahwa sumber yang digunakan mendukung tujuan. Setelah menentukan kriteria pemilihan literatur, peneliti mencari literatur yang mencakup berbagai teori seperti gambar 2.1 dibawah ini:



Gambar 1. Proses Penelitian Studi Literatur (Sumber: Data diolah)

Setelah literatur yang relevan ditemukan, langkah berikutnya adalah menganalisis secara menyeluruh setiap sumber yang tersedia serta membaca dan menyaring data untuk mengevaluasi tesis yang dibuat oleh penulis lain. Dalam proses ini, metode yang digunakan adalah untuk mengevaluasi, apakah hasilnya dapat digunakan secara luas, dan seberapa besar kontribusi mereka terhadap pemahaman serangan siber infrastruktur kritis yang merupakan ancaman terhadap keamanan dan kesejahteraan masyarakat. Peneliti juga mencari celah atau topik yang belum dibahas secara menyeluruh dalam literatur yang ada.

Langkah berikutnya adalah menyusun hasil analisis literatur. Di sini, peneliti memberikan kesimpulan penting dari literatur yang telah dibaca dan menyusun hubungan antara konsep, teori, dan hasil. Tujuan dari sintesis ini adalah untuk memberikan gambaran umum tentang kemajuan penelitian. Terakhir, peneliti membuat kesimpulan dari penelitian literatur dan membuat saran atau implikasi untuk penelitian masa depan. Kesimpulan ini menguraikan temuan utama dan menjelaskan bagaimana temuan tersebut dapat memberikan wawasan baru atau memperluas pemahaman tentang subjek yang diteliti. Peneliti juga dapat menemukan bidang penelitian yang memerlukan penelitian tambahan. Oleh karena itu, penelitian kualitatif yang didasarkan pada studi literatur tidak hanya memberikan pemahaman yang lebih baik tentang topik tertentu, tetapi juga menunjukkan jalan untuk penelitian masa depan.

3. HASIL DAN PEMBAHASAN

Dampak Serangan Siber terhadap Infrastruktur Kritis

Serangan siber terhadap infrastruktur kritis dapat berdampak besar pada banyak bidang kehidupan, terutama sektor energi. Jika sistem energi mengalami kerusakan, seperti serangan terhadap jaringan distribusi listrik atau infrastruktur energi lainnya, pemadaman listrik yang meluas dapat terjadi. Tidak hanya kehidupan sehari-hari yang terganggu oleh pemadaman ini, tetapi juga berdampak pada industri dan bidang lain, seperti manufaktur dan transportasi. Salah satu contoh nyata adalah serangan pada jaringan listrik Ukraina pada 2015, yang menyebabkan pemadaman listrik selama beberapa jam. Mengingat ketergantungan kita yang besar pada energi untuk menjalankan aktivitas ekonomi dan sosial, keamanan cyber di bidang ini semakin penting (J. Smith, 2016).

Sebagai tambahan pada sektor energi, sektor transportasi juga dapat menjadi sasaran serangan siber. Serangan siber pada sistem transportasi, seperti sistem navigasi, pengendalian

lalu lintas, atau logistik, dapat menyebabkan gangguan yang signifikan dalam pergerakan barang dan manusia. Serangan siber pada sistem transportasi di Amerika Serikat pada tahun 2017 mengganggu sistem perkeretaapian dan bandara, mengganggu operasional perjalanan. Serangan seperti ini dapat memperlambat distribusi produk, meningkatkan biaya logistik, dan mengganggu kehidupan ekonomi secara keseluruhan. Karena rentannya terhadap serangan dan kemampuan untuk menyebabkan gangguan besar-besaran, infrastruktur transportasi yang terhubung dengan internet sering kali menjadi sasaran utama (Zhang dkk., 2018).

Serangan siber dapat berdampak besar pada banyak industri, termasuk sektor kesehatan. Serangan siber pada rumah sakit, pusat medis, atau sistem kesehatan lainnya dapat mengganggu layanan kesehatan penting dan bahkan menghapus data medis pasien. Serangan siber di sektor ini dapat menyebabkan gangguan operasional dan pencurian data medis yang sangat sensitif. Kasus ransomware yang menyerang sistem rumah sakit Inggris pada tahun 2017 (serangan WannaCry) menunjukkan betapa rentannya industri ini terhadap ancaman dunia maya. Pencurian data medis dapat merusak kepercayaan pasien terhadap sistem kesehatan dan memicu pelanggaran privasi yang sangat berbahaya (Huang dkk., 2020).

Terakhir, serangan siber sangat berbahaya bagi industri keuangan. Serangan yang merusak bank dan lembaga keuangan lainnya dapat mengganggu aliran dana dan transaksi ekonomi penting. Pencurian data nasabah yang dapat digunakan untuk penipuan dan pencucian uang, serta serangan terhadap sistem perbankan atau pertukaran mata uang kripto dapat menyebabkan kerugian besar. Data nasabah yang dicuri dapat digunakan untuk melakukan transaksi ilegal atau kegiatan kriminal lainnya. Sebuah penelitian yang dilakukan oleh (Kumar & Agrawal, 2019) menemukan bahwa serangan siber pada sektor perbankan dapat menyebabkan masyarakat kehilangan kepercayaan terhadap stabilitas sistem keuangan, yang pada gilirannya dapat mengganggu ekonomi nasional.

Implikasi Bagi Keamanan dan Kesejahteraan Masyarakat

Serangan siber terhadap infrastruktur penting dapat membahayakan keamanan nasional secara signifikan. Mereka sangat rentan terhadap serangan dunia maya karena memiliki masalah di bidang penting seperti energi, transportasi, dan kesehatan. Serangan terhadap infrastruktur kritis dapat merusak stabilitas nasional, mengganggu ketertiban sosial, dan mengganggu kemampuan negara untuk memberikan layanan dasar. Misalnya, serangan terhadap jaringan listrik atau sistem transportasi dapat memengaruhi distribusi barang dan mobilitas umum, yang dapat mengganggu perekonomian secara keseluruhan. Dalam situasi yang lebih buruk, serangan pada sektor-sektor penting ini dapat menimbulkan ketegangan atau konflik internasional serta mengancam keamanan negara (Hathaway & Crootof, 2017).

Selain itu, dampak serangan siber pada ekonomi tidak dapat diabaikan. Serangan siber dapat menyebabkan kerugian moneter yang signifikan, baik secara langsung maupun tidak langsung. Produksi ekonomi dapat menurun jika layanan rusak di bidang penting seperti perbankan, energi, dan transportasi. Selain itu, pemulihan sistem akan sangat mahal. Biaya pemulihan dapat mencakup perbaikan infrastruktur, penggantian perangkat keras yang rusak, dan biaya operasional karena gangguan atau kehilangan data. Sebagai contoh, serangan ransomware yang melumpuhkan rumah sakit atau perusahaan besar dapat menyebabkan kerugian yang signifikan, termasuk kerusakan fisik atau kehilangan data serta penurunan produktivitas dan pendapatan (Zohar & Magen, 2020).

Serangan siber memiliki konsekuensi sosial-psikologis yang signifikan selain berdampak ekonomi. Serangan dunia maya yang merusak infrastruktur atau data pribadi sering menyebabkan ketakutan, kecemasan, dan kehilangan rasa aman. Stabilitas sosial dapat terganggu jika orang kehilangan kepercayaan pada sistem yang biasa digunakan orang untuk menjalankan aktivitas sehari-hari, seperti sistem perbankan dan layanan kesehatan. Tidak hanya individu yang terkena dampak ketidakpastian ini, tetapi juga institusi dan kelompok

yang bergantung pada kepercayaan publik. Dalam dunia digital, kepercayaan adalah salah satu hal yang paling penting, dan serangan terhadap infrastruktur penting yang mengancam kepercayaan ini dapat memperburuk ketidakpastian sosial (Carvalho dkk., 2018).

Serangan siber juga menimbulkan ketidakpastian di masyarakat. Ketidakpastian ini termasuk pertanyaan tentang masa depan, kemampuan negara atau perusahaan untuk menangani ancaman serupa di masa depan, dan kesiapan untuk memperbaiki kerusakan. Seseorang dapat merasa tidak aman dan kehilangan kepercayaan terhadap sektor publik dan swasta. Selain itu, keraguan terhadap teknologi yang semakin banyak digunakan dalam kehidupan sehari-hari dapat menyebabkan masyarakat kurang nyaman menggunakannya untuk keperluan profesional dan pribadi. Ketidakpastian ini dapat meningkatkan kecemasan masyarakat dan menurunkan kualitas hidup (R. Smith dkk., 2019).

Masyarakat harus memiliki pertahanan dalam menghadapi serangan siber. Ketahanan ini mencakup perlindungan infrastruktur oleh pemerintah dan bisnis serta pendidikan masyarakat. Orang-orang yang mengetahui lebih banyak tentang ancaman dunia maya dan bagaimana melindungi data pribadi dan menemukan potensi serangan akan lebih siap untuk menghadapi dan menanggapi ancaman tersebut. Langkah penting untuk meningkatkan ketahanan sosial terhadap ancaman dunia maya adalah meningkatkan kesadaran tentang keamanan siber dan memberikan pelatihan dasar untuk melindungi diri secara online. Terdidik dapat membantu masyarakat mencegah serangan siber yang berbahaya (Sutton et al., 2018).

Kolaborasi antara pemerintah, sektor swasta, dan masyarakat sipil sangat penting untuk meningkatkan ketahanan masyarakat. Semua orang harus dididik tentang keamanan siber sejak dini, baik di sekolah maupun dalam program pelatihan pekerja di berbagai sektor. Program yang meningkatkan kesadaran publik tentang cara melindungi data pribadi dan menghindari penipuan siber dapat mengurangi jumlah serangan yang berhasil. Selain itu, pemerintah harus bekerja sama dengan sektor swasta untuk membuat kebijakan yang mengutamakan perlindungan data dan pengamanan infrastruktur penting dari ancaman dunia maya (Böhme et al., 2015).

Upaya Mitigasi

Untuk mendukung upaya mitigasi dalam meningkatkan keamanan siber dan melindungi infrastruktur penting, beberapa strategi berikut dapat digunakan:

1. Peningkatan Keamanan Siber melalui Teknologi Canggih Peningkatan keamanan siber melalui penerapan teknologi yang lebih canggih dan fleksibel diperlukan untuk menghadapi ancaman siber yang terus berkembang. Meskipun sangat canggih, sistem keamanan saat ini seringkali tidak cukup untuk mencegah serangan yang semakin kompleks. Oleh karena itu, untuk meningkatkan sistem keamanan, teknologi seperti kecerdasan buatan (AI), blockchain, dan algoritma enkripsi canggih harus diterapkan. Misalnya, sistem berbasis kecerdasan buatan dapat membantu mendeteksi dan menanggapi ancaman dengan lebih cepat dan akurat (Yin & Xie, 2021).
2. Dengan kerjasama Pentahelix, keamanan siber tidak dapat ditangani hanya oleh satu sektor. Oleh karena itu, kerja sama antar sektor sangat penting untuk membangun sistem yang lebih aman dan efisien. Model kerjasama pentahelix, yang melibatkan sektor pemerintah, masyarakat, dunia usaha, akademisi, dan media, adalah cara yang bagus untuk bekerja sama dan mendukung satu sama lain dalam mengatasi tantangan keamanan siber. Kerja sama ini tidak hanya meningkatkan pemahaman dan kesadaran orang, tetapi juga memperkuat mekanisme yang digunakan untuk menangani insiden siber (Haryanto, 2020).
3. Regulasi dan Kebijakan yang Ketat: Untuk melindungi infrastruktur kritis dari serangan siber, negara harus membuat kebijakan yang lebih tegas untuk melindungi

data sensitif dan memastikan bahwa penyedia layanan dan pengelola infrastruktur kritis memiliki protokol keamanan yang jelas dan dapat diterapkan. Untuk mencegah kebocoran data dan serangan yang merusak, diperlukan penguatan kebijakan, seperti pembentukan peraturan operasional keamanan siber dan pengawasan yang lebih intensif terhadap pelaksanaan kebijakan ini (Widodo, 2021).

4. Pendidikan dan Kesadaran Publik tentang Keamanan Siber Harus diberikan dari tingkat dasar hingga profesional. Program pelatihan yang menyeluruh bagi masyarakat, mulai dari individu hingga perusahaan, akan membantu meningkatkan kesadaran dan keterampilan dalam menjaga data organisasi dan pribadi. Hal ini sangat penting untuk mencegah bahaya yang biasanya berasal dari kelalaian manusia, seperti penggunaan kata sandi yang tidak akurat dan mengabaikan pembaruan perangkat lunak (Rahmawati, 2022).
5. Penguatan Infrastruktur Teknologi Informasi: Selain peningkatan teknologi keamanan, penguatan infrastruktur teknologi informasi juga penting untuk mencegah ancaman terhadap integritas data dan sistem. Infrastruktur yang kuat dan berbasis teknologi terkini dapat menurunkan kerentanannya terhadap serangan dunia maya. Untuk mengurangi dampak serangan, penerapan pusat data yang terdesentralisasi dan sistem cadangan yang lebih baik adalah salah satu tindakan yang dapat diambil (Sari & Gunawan, 2023).

Kebijakan Keamanan Siber yang Terintegrasi: Pemerintah harus berpartisipasi aktif dalam pembuatan dan pelaksanaan kebijakan keamanan siber yang terintegrasi yang melindungi berbagai sektor penting, seperti energi, kesehatan, dan keuangan. Adanya kebijakan yang terintegrasi memungkinkan setiap sektor untuk mengikuti protokol dan standar yang sama untuk melindungi data dan informasi penting yang mereka kelola (Harsono, 2021).

4. KESIMPULAN

Serangan siber terhadap infrastruktur kritis telah berkembang menjadi ancaman multidimensi yang mengancam stabilitas ekonomi, keamanan nasional, dan kesejahteraan sosial. Data menunjukkan peningkatan 150% serangan pada sektor energi dan utilitas di tahun 2022 serta kerugian ekonomi global mencapai $385 miliar akibat gangguan infrastruktur. Ketergantungan antar sektor seperti energi, transportasi, dan kesehatan menciptakan efek domino di mana gangguan pada satu elemen berdampak sistemik.

Perkembangan teknologi seperti IoT dan sistem SCADA justru memperluas permukaan serangan, dengan 73% sistem infrastruktur kritis memiliki kerentanan yang dapat dieksploitasi. Teknik serangan multivector yang menggabungkan phishing, malware, dan zero-day exploits (47% kasus) mengungguli solusi keamanan konvensional. Studi CISA mencatat kenaikan 287% serangan DDoS pada 2023, sementara serangan ransomware meningkat 300% periode 2020-2022.

Gangguan layanan esensial memicu "ketakutan infrastruktur" dengan peningkatan 42% tingkat kecemasan masyarakat. Kasus seperti serangan di Ukraina (2015) dan Florida (2021) menunjukkan potensi krisis kemanusiaan, sementara gangguan rumah sakit di Irlandia (2021) mengancam keselamatan pasien. Dampak jangka panjang termasuk penurunan 18% investasi asing dan ketidakpercayaan politik (+43% dalam 12 bulan pasca-serangan).

Pendekatan Pentahelix—melibatkan pemerintah, swasta, akademisi, media, dan masyarakat—dibutuhkan untuk membangun ketahanan sistematis. Implementasi AI, blockchain, dan enkripsi canggih perlu diimbangi dengan desentralisasi pusat data dan pelatihan SDM. Regulasi ketat seperti standar operasional keamanan siber dan pengawasan terintegrasi menjadi kunci.

Pembangunan kerangka kerja kolaboratif berbasis risiko (risk-based approach) harus memprioritaskan: (1) R&D teknologi deteksi ancaman real-time, (2) Program literasi siber menyeluruh dari sekolah hingga pelatihan profesional, dan (3) Skema respons insiden terstandar antar-negara. Perlindungan infrastruktur kritis bukan lagi isu teknis semata, tetapi prasyarat ketahanan nasional di era digital

5. REFERENSI

Anderson, K., & Chen, R. (2022). Economic Impact Analysis of the Colonial Pipeline Ransomware Attack. *Journal of Critical Infrastructure Protection*, *18*(2), 89–104.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610–613.

Bishop, M. (2015). Cybersecurity and the healthcare sector: A critical infrastructure review. *International Journal of Critical Infrastructure Protection*, *8*(2), 58–65.

BlackFog. (2023). *State of Ransomware 2023 Annual Report*. BlackFog Inc.

Böhme, R., Christin, N., Clayton, R., & Pfeiffer, M. (2015). *Security Metrics for Cyber Attacks and Cybersecurity Systems*. Springer.

Carvalho, M., Ribeiro, M., & Oliveira, P. (2018). Cybersecurity Risks and Social Implications: A Literature Review. *Journal of Cybersecurity*, *4*(2), 98–112.

Chang, R. (2020). Cybersecurity Threats to Critical Infrastructure: A Comprehensive Analysis. *Journal of Infrastructure Security*, *15*(3), 245–260.

Chen, L., & Williams, R. (2023). The Evolution of Spear Phishing: Advanced Techniques Targeting Critical Infrastructure Personnel. *Journal of Cybersecurity and Privacy*, *5*(2), 118–135.

Critical Infrastructure Disruptions: Global Economic Impact Assessment 2022–2023. (t.t.). EIU Publications.

Harris, S., & Patel, A. (2015). Critical in frastructure and national security. Dalam *Springer*. Springer.

Harsono, P. (2021). *Perlindungan Infrastruktur Kritis dalam Era Digital*. Penerbit Keamanan Nasional.

Haryanto, D. (2020). *Kolaborasi Pentahelix dalam Meningkatkan Keamanan Siber di Indonesia*. Penerbit Ilmu Teknologi.

Hathaway, M. J., & Crootof, R. (2017). Cybersecurity and National Security: Understanding the Importance of Infrastructure Protection. *Journal of National Security Law*, *6*(1), 45–63.

Huang, S., Chen, S., & Lin, C. (2020). Impact of Cybersecurity Attacks on Healthcare Systems. *Journal of Healthcare Management*, *65*(3), 12–20.

IBM Security. (2023). X-Force Threat Intelligence Index 2023. Dalam *IBM Corporation*. IBM Corporation.

Johnson, C. A., Flage, R., & Guikema, S. D. (2021). Feasibility study of PRA for critical infrastructure risk analysis. *Reliability Engineering & System Safety*, *212*, 107643.

Kumar, R., & Agrawal, R. (2019). Cybersecurity Risks in Financial Institutions. *International Journal of Financial Services Management*, *21*(4), 245–256.

Lindqvist. (2021). Effects of Critical Infrastructure Failure: A Cross-Cultural Survey Analysis. *International Journal of Disaster Risk Reduction*, *62*, 102393.

Luhmann, N. (1995). *Social systems*. Stanford University Press.

Martinez, C., Wilson, T., & Lee, J. (2024). Multivector Attacks on Critical Infrastructure: Analysis and Detection Methods. *Critical Infrastructure Protection Review*, *14*(1), 33–49.

Martinez, L., & Kumar, S. (2024). SCADA Systems Security: Vulnerabilities and Mitigation Strategies. *Industrial Control Systems Security Review*, *12*(1), 45–62.

Miller, A. (2020). Effects of Cyber Attacks on Critical Infrastructure on Economy. *Journal of Cybersecurity Economics*, *2*(1), 45–68.

Nguyen, T. (2023). Anxiety of Infrastructure: A New Framework for Understanding Social Reactions to Critical Service. *Disruptions Quarterly of Sociology*, *64*(3), 512–531.

Pagani, A., Mosquera, G., Alturki, A., Johnson, S., Jarvis, S., Wilson, A., Guo, W., & Varga, L. (2019). Resilience or robustness: identifying topological vulnerabilities in rail networks. *Royal Society open science*, *6*(2), 181301.

Park, J., & Roberts, M. (2023). Social Engineering Attacks on Critical Infrastructure: Patterns and Prevention. *Cybersecurity Journal*, *15*(4), 178–193.

Pfleeger, C. (2017). *Security in computing*. Prentice Hall.

Rahmawati, S. (2022). *Edukasi Keamanan Siber bagi Masyarakat: Upaya Meningkatkan Kesadaran di Era Digital*. Penerbit Ilmu Komunikasi.

Rashid, F., & Tsering, J. (2018). Ransomware Impact on Healthcare Systems: A Case Study of WannaCry. *Health Informatics Journal*, *24*(4), 361–380.

Roberts, A., & Park, J. (2021). Collaborative Approaches to Critical Infrastructure Protection. *Security Studies Review*, *25*(2), 89–104.

Roberts, P. (2023). Instabilitas politik sebagai konsekuensi dan penyebab serangan infrastruktur kritis. *Journal of Political Risk*, *11*(2), 78–93.

Sari, R., & Gunawan, E. (2023). *Infrastruktur Teknologi dan Keamanan Siber: Tantangan dan Solusi*. Penerbit Teknologi.

Smith, J. (2016). Cyber Attacks on Energy Infrastructure: A Case Study of the Ukrainian Power Grid. *Journal of Energy Security*, *30*(2), 40–46.

Smith, R., Jones, S., & Lewis, T. (2019). The Psychological Impact of Cyberattacks on Society. *Journal of Social Psychology*, *15*(4), 233–247.

Smith, S. (2016). Healthcare infrastructure and the digital era. Dalam *Oxford University Press*. Oxford University Press.

Sullivan, M. (2019). The role of infrastructure in public health emergencies. *International*.

Thompson, R., Wilson, K., & Brown, S. (2023). Healthcare Infrastructure Cybersecurity: Lessons from the Irish Hospital Attack. *International Journal of Healthcare Security*, *9*(3), 112–127.

Van Oorschot, P., & Zhang, S. (2021). Social Engineering in Cybersecurity: The Evolution of a Concept. *Computers & Security*, *108*, 102359.

Watson, M., & Brown. (2022). Case Study: The Cyber Attack on the Florida Water Treatment Facility. *Journal of Critical Infrastructure Protection*, *36*, 100425.

Widodo, S. (2021). *Regulasi Keamanan Siber: Kebijakan dan Implementasinya di Indonesia*. Penerbit Kebijakan Nasional.

Williams, A., & Cooper. (2022). Effects of Critical Infrastructure Attacks on Economic Security: Stock Market Performance and Investment Patterns. *Economic Security Review*, *15*(4), 204–219.

Williams, P., & Zetter, K. (2020). Ransomware and its impact on critical infrastructure. *Journal of Cybersecurity Research*, *9*(1), 102–114.

Yin, Z., & Xie, J. (2021). Artificial Intelligence and Cybersecurity: Trends and Challenges. *IEEE Transactions on Cybernetics*, *51*(5), 1147–1157.

Zetter, K. (2014). The cyber threat to critical infrastructure. *The New York Times*.

Zhang, X., Li, L., & Chen, Y. (2018). Cybersecurity Challenges in Transportation Systems. *Journal of Transportation Technology*, *14*(1), 34–45.

Zohar, Y., & Magen, J. (2020). The Economic Impact of Cyber Attacks on Critical Infrastructure. *Global Cybersecurity Review*, *3*(1), 55–72.