Neptunus: Jurnal Ilmu Komputer Dan Teknologi Informasi
Vol.2, No.4 November 2024
e-ISSN: 3031-898X; p-ISSN: 3031-8998, Hal 116-132
DOI: https://doi.org/10.61132/neptunus.v2i4.428
Available online at: https://journal.arteii.or.id/index.php/Neptunus

Studi Literatur: Strategi Pengamanan Siber dalam Menghadapi *Cyber Crime*

Wahyuni Susilowati[1*], Agussalim[2]
UPN "Veteran" Jawa Timur, Indonesia

Alamat: Jl. Rungkut Madya, Gn. Anyar, Kec. Gn. Anyar, Surabaya, Jawa Timur
*Korespondensi penulis: wahyunisusilowati.16@gmail.com**

Abstract. *In the current digital era, cybersecurity of data and information systems. The threat of attacks, or , is a form of threat that continues to grow along with advances in technology. This research aims to learn about cybersecurity strategies in dealing with . The method used in this research is a literature review. This journal was prepared based on an analysis of research results from various journals accessed through secondary data sources, namely the Google Scholar database, and e-resources from Springer, Cambridge, and Taylor and Francis. The research results show that implementing technology such as encryption, multifactor authentication, and user training, are some of the effective steps that have been proven to reduce risk. However, challenges in implementing this strategy remain, both from a technical and non-technical perspective, which require special attention from researchers and practitioners in the field of cyber security*.

Keywords*: Cyber Crime, Cyber Security, Strategy*

Abstrak. Di era digital saat ini, salah satu aspek penting dalam menjaga integritas dan keamana data serta informasi merupakan tugas dari keamanan. Seiring dengan berkembangnya kemajuan teknologi, ancaman juga semakin meningkat. Tujuan yang diharapkan atas penelitian ini untuk mempelajari tentang strategi pengamanan siber dalam menghadapi . Metode yang digunakan dalam penelitian ini adalah tinjauan literatur. Jurnal ini dibuat berdasarkan analisis hasil penelitian yang berasal dari berbagai jurnal yang diakses melalui sumber data sekunder yaitu database google ccholar, e-resource dari springer, cambridge maupun taylor and francis. Hasil penelitian menunjukkan bahwa implementasi teknologi seperti enkripsi, otentikasi multifaktor, serta pelatihan pengguna, merupakan beberapa langkah efektif yang telah terbukti mampu mengurangi risiko. Namun, tantangan dalam implementasi strategi ini tetap ada, baik dari segi teknis maupun non-teknis, yang memerlukan perhatian khusus dari peneliti dan praktisi di bidang keamanan siber

Kata kunci: *Cyber Crime*, Pengamanan Siber, Strategi

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi yang pesat di era digital telah memberikan banyak manfaat, namun juga menciptakan celah yang mampu dipergunakan pihak-pihak yang tidak memiliki tanggung jawab. Di era digital saat ini, keamanan siber telah menjadi aspek penting dalam menjaga integritas dan keamanan data serta sistem informasi. Ancaman serangan termasuk salah satu bentuk ancaman yang terus berkembang seiring dengan kemajuan teknologi. mencakup berbagai bentuk kejahatan yang dilakukan melalui perangkat komputer atau jaringan internet, seperti pencurian data pribadi, penipuan, peretasan, hingga serangan siber skala besar terhadap infrastruktur kritis.

Indonesia, sebagai negara yang semakin terintegrasi dalam ekonomi digital global, juga rentan terhadap serangan siber. Berdasarkan data yang disampaikan oleh Badan Siber

Received: September 19, 2024; Revised: Oktober 03, 2024; Accepted: Oktober 17, 2024; Online Available: Oktober 19, 2024

dan Sandi Negara (BSSN) menunjukkan bahwa kasus serangan siber di Indonesia menunjukkan peningkatan yang signifikan setiap tahunnya. Kejahatan siber dapat berdampak luas, mulai dari kerugian finansial, kerusakan reputasi perusahaan, hingga ancaman terhadap keamanan nasional. Serangan siber tidak hanya mengungkap kelemahan dalam infrastruktur digital nasional, tetapi juga menyoroti kebutuhan mendesak untuk strategi keamanan siber yang lebih efektif dan bertanggung jawab. Keamanan siber merupakan upaya untuk melindungi komputer, jaringan, aplikasi perangkat lunak, sistem penting, dan data dari ancaman digital yang mungkin terjadi

Seiring dengan meningkatnya ancaman , kebutuhan akan strategi pengamanan siber yang lebih kuat dan komprehensif menjadi sangat penting. Upaya pengamanan siber tidak hanya harus mencakup teknologi, tetapi juga kebijakan, regulasi, serta kesadaran individu dan organisasi dalam menjaga keamanan informasi mereka. Pengembangan teknologi pengamanan, seperti firewall, enkripsi, sistem deteksi intrusi, serta metode autentikasi yang lebih aman, harus diimbangi dengan strategi manajemen risiko yang efektif.

Dalam konteks ini, strategi keamanan siber yang efektif memerlukan pendekatan terpadu yang mencakup kolaborasi antara personel, proses, dan teknologi dalam organisasi. Program keamanan siber yang berhasil melibatkan edukasi karyawan tentang praktik keamanan yang optimal serta menggunakan teknologi pertahanan siber otomatis untuk melindungi infrastruktur TI yang ada. Pengamanan siber juga memerlukan kerjasama lintas sektor, baik antara pemerintah, perusahaan swasta, maupun masyarakat. Kolaborasi ini diperlukan untuk memastikan penerapan standar keamanan yang tinggi, respon cepat terhadap insiden siber, serta pengembangan kapasitas sumber daya manusia yang memiliki keahlian di bidang keamanan siber

2. KAJIAN TEORITIS

Konsep Strategi

a. Definisi dan Konsep Dasar

Strategi keamanan siber merupakan kumpulan langkah-langkah maupun tindakan yang digunakan dalam rangka melindungi sistem komputer, jaringan, maupun data dari ancaman siber serta melindungi dari akses yang tidak hendaki. Konsep dasar strategi pengamanan siber dikenal sebagai CIA Triad, yang mencakup tiga aspek utama yaitu:

1) *Confidentiality* (Kerahasiaan)

Mengamankan informasi sensitif dari akses yang tidak berwenang. Penerapannya bisa dengan membatasi akses data, seperti menggunakan two factor authentication (2FA) dan mengontrol akses database

2) *Integrity* (Integritas)

Menjaga keaslian dan kebenaran data. Implementasinya berkaitan dengan menjaga data agar tidak terjadi manipulasi atau kebocoran, seperti menggunakan enkripsi dan tanda tangan digital

3) *Availability* (Ketersediaan)

Memastikan sistem dan layanan tetap dapat diakses oleh pengguna yang berwenang. Penerapannya bisa dengan menjaga performa website atau aplikasi agar selalu tersedia bagi pengunjung

b. Jenis-Jenis Strategi Pengamanan Siber

Strategi pengamanan siber dapat dikelompokkan berdasarkan area implementasinya, seperti:

1) *Network Security*: Melindungi jaringan internal dari ancaman siber dengan menggunakan antivirus, firewall, dan two factor authentication
2) *Cloud Security*: Melindungi data yang tersimpan di cloud dengan enkripsi, pengelolaan akses yang ketat, dan pemantauan terus-menerus
3) *Application Security*: Melindungi aplikasi dari ancaman siber dengan menggunakan autentikasi, password yang kuat, dan sidik jari atau pengenalan wajah

c. Ancaman Keamanan Siber

Ancaman keamanan siber dapat berupa:

1) *Cyber Crime*: Manipulasi data, transaksi ilegal, dan pengrusakan sistem komputer.
2) *Cyber Attack*: Serangan siber yang bertujuan untuk mengakses, memodifikasi, atau merusak informasi sensitif.
3) *Cyber Terrorism*: Kegiatan yang bertujuan mengganggu stabilitas sosial, politik, dan ekonomi suatu negara melalui pemanfaatan teknologi internet.

d. Strategi Penguatan Cyber Security

Untuk mewujudkan keamanan nasional di era Society 5.0, strategi penguatan *cyber security* yang harus dilakukan adalah:

1) *Capacity Building*: Meningkatkan kemampuan dan sumber daya manusia dalam bidang cyber security.
2) Pembentukan Undang-Undang Khusus: Membuat undang-undang khusus tentang tindak pidana siber.
3) Kerjasama Stakeholder: Meningkatkan kerjasama antara pemangku kepentingan baik dalam negeri maupun internasional dengan bidang pengamanan siber

e. Pendekatan Strategi Keamanan Siber

Pendekatan strategi keamanan siber yang efektif melibatkan:

1) *Zero Trust:* Menghapus kepercayaan otomatis dan secara terus-menerus memverifikasi setiap interaksi digital
2) Pendekatan Proaktif: Mengadopsi pendekatan proaktif dalam mencegah serangan siber dengan penerapan kontrol keamanan yang ketat dan pemantauan intelijen keamanan
3) Kerjasama Internasional: Meningkatkan kerjasama internasional dalam bidang cyber security untuk mengidentifikasi ancaman baru dan mengembangkan solusi yang efektif
4) Peran Pemerintah dan Masyarakat

Peran pemerintah dan masyarakat sangat penting dalam menyosialisasikan mengenai bahaya serangan siber dan meningkatkan kesadaran akan pentingnya keamanan siber

Konsep Cyber Security

Keamanan siber merupakan kumpulan alat, kebijakan, prinsip perlindungan, rekomendasi, strategi pengendalian risiko, tindakan, pelatihan, aplikasi unggulan, jaminan, serta informasi terkait teknologi yang berfungsi untuk melindungi dunia online, organisasi, dan pengguna (Indah, 2022). Warisan organisasi dan individu yang terlibat dalam keamanan siber mencakup berbagai fungsi yang berkaitan dengan komputasi, individu, infrastruktur, program, layanan, sistem telekomunikasi, serta semua data yang masuk dan keluar melalui internet. Cybersecurity juga dapat didefinisikan sebagai serangkaian kegiatan yang bertujuan menjaga serta mengurangi risiko terhadap privasi,integritas, dan

ketersediaan informasi. Proses ini harus melindungi sistem informasi dari berbagai serangan, baik fisik maupun digital

Keamanan siber adalah upaya untuk melindungi informasi dari serangan siber. Ada beberapa elemen utama dalam keamanan siber, yaitu:

a. Kebijakan keamanan dokumen: Standar informasi yang dituangkan dalam dokumen untuk memandu semua proses perlindungan informasi.
b. Infrastruktur informasi: Media yang mendukung operasional informasi, mencakup perangkat keras dan lunak seperti router, switch, server, sistem operasi, basis data, dan situs web.
c. Pertahanan perimeter: Mekanisme yang berfungsi melindungi komponen infrastruktur informasi, seperti IDS, IPS, dan firewall
d. Sistem pemantauan jaringan: Perangkat yang digunakan untuk memantau kondisi, memeriksa peralatan, dan menilai kelayakan infrastruktur informasi.
e. Sistem informasi dan manajemen acara: merupakan alat dengan fungsi mengamati segala peristiwa dan kejadian terkait keamanan dalam jaringan.
f. Penilaian keamanan jaringan: Komponen yang berfungsi untuk mengendalikan dan mengukur tingkat keamanan informasi.
g. Ketersediaan sumber daya manusia dan keamanan: Berkaitan dengan tersedianya tenaga ahli dan jaminan keamanan pada sistem informasi.

Di Indonesia, untuk menjaga keamanan siber, diperlukan kebijakan yang mengatur berbagai aspek terkait keamanan siber dalam regulasi, mencakup pedoman dokumen, persyaratan infrastruktur yang sesuai standar global, serta pertahanan perimeter yang memadai. Perangkat pemantauan jaringan, sistem manajemen informasi, dan peristiwa berperan penting dalam melacak insiden keselamatan. Penilaian keamanan komunitas juga bertindak sebagai kontrol dan pengukuran keamanan.

Dengan ancaman seperti pencurian data, peretasan situs web, dan pelanggaran data pribadi, perlindungan siber sangat penting untuk melindungi komunitas internet dan mempertahankan keamanan data secara global**.**

Konsep

Kejahatan siber atau adalah aktivitas yang sangat merugikan banyak pengguna internet. melibatkan upaya untuk mengakses perangkat komputer orang lain secara ilegal dengan tujuan menemukan, mencuri, merusak, atau meretas data privasi, yang dapat menimbulkan kerugian bagi pengguna internet. Pelaku kejahatan siber dapat menargetkan

perusahaan besar, pengguna internet, sistem digital, bisnis pemerintah, dan banyak target lainnya. didefinisikan sebagai tindakan yang bertentangan dengan hukum yang memanfaatkan jaringan komputer sebagai alat atau sasaran, demi keuntungan pribadi maupun merugikan orang lain. Kejahatan komputer yang sering dikaitkan dengan peretas (hacker) umumnya memiliki konotasi negatif.

Kejahatan siber ini menjadi ancaman serius dalam kehidupan modern, dan pemerintah sering kesulitan menangani kejahatan yang dilakukan melalui teknologi komputer. Dampaknya sangat merugikan masyarakat, terutama karena kurangnya pemahaman tentang ancaman online serta lemahnya perlindungan terhadap data pribadi. Untuk menghadapi masalah , penting dilakukan pencegahan yang lebih baik. melibatkan pelanggaran privasi yang dilakukan baik secara langsung di tempat komputer tersebut berada atau melalui jaringan komunikasi jarak jauh.

Kejahatan ini memakan banyak korban, terutama dalam aspek finansial, dan seringkali korban hanya bisa menyesali apa yang sudah terjadi. Untuk mencegah hal ini terjadi, berikut prosedur yang bisa dilakukan antara lain:

a. **Edukasi pengguna**: Memberikan pemahaman baru tentang dan internet.
b. **Menggunakan perspektif peretas**: Melihat dari sudut pandang peretas untuk mengamankan sistem.
c. **Sistem tambalan**: Memperbaiki kelemahan-kelemahan yang ada dalam sistem.
d. **Aturan dan kebijakan**: Menetapkan prosedur dan regulasi yang melindungi sistem dari akses tidak sah.
e. **IDS dan IPS**: Memanfaatkan Intrusion Detection System serta Intrusion Prevention System untuk mendeteksi serta mencegah serangan.
f. **Firewall dan antivirus**: Menggunakan aplikasi firewall dan antivirus untuk menjaga keamanan sistem.

3. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah pendekatan tinjauan pustaka. Tinjauan pustaka didefinisikan sebagai metode penelitian dengan maksud menggali data serta meringkas temuan berdasarkan penelitian terdahulu, dan menganalisis berbagai pandangan ahli yang tercantum dalam karya tulis. Proses tinjauan pustaka terdiri dari empat tahapan utama. Tahap yang pertama merupakan perencanaan review yang mana peneliti merencanakan pengumpulan informasi dan materi dari berbagai sumber dan literatur lainnya untuk dilakukan kegiatan review. Di tahap kedua, peneliti meninjau

dengan melakukan pemeriksaan serta melakukan evaluasi sumber informasi yang sesuai guna memberikan kepastian terkait kesesuaian hasil review dengan topik yang dibahas. Di tahap ketiga yaitu menganalisis hasil review dengan berbagai sumber informasi dengan mengikuti pedoman yang dianjurkan. Dan di tahap terakhir, penyusunan ulasan yang didasarkan pada hasil review dan temuan dari beberapa artikel yang telah ditinjau.

Data sekunder merupakan data yang digunakan dalam penelitian ini. Data sekunder dapat didefinisikan sebagai data yang tidak didapatkan secara langsung dari partisipan. Data ini dikumpulkan dari artikel maupun jurnal sebagai sumber informasi. Google Scholar, E-resource Cambridge, Springer, dan Taylor & Francis dengan kata kunci "Cyber security" dan "" merupakan beberapa rumah jurnal yang digunakan untuk mengkoleksi artikel dalam hal pembahasan topik penelitian

4. HASIL DAN PEMBAHASAN

Pembahasan dan Analisis

Dalam bagian ini, peneliti menjalankan eksplorasi literatur ilmiah untuk menganalisis pentingnya cyber security dalam menghadapi .

Tabel 1. Identitas Jurnal

Jurnal	Identitas Jurnal	
	Judul	Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber dan Sandi Negara
	Jurnal	Jurnal Dinamika Global
	Volume dan Halaman	Vol. 7 No. 2, hal 291-312
	Tahun	2022
	Penulis	Yusuf Ginanjar
	Link	https://doi.org/10.36859/jdg.v7i02.1187
	Judul	The Impact of in Modern Generation Based on Systematic Literature Review Analysis
	Jurnal	Journal of Techno-Social
	Volume dan Halaman	Vo. 15 No. 2
	Tahun	2023
	Penulis	Kong Ming Chai, Ang Zi Xuan, Muhaymin Hakim Abdullah
	Link	https://doi.org/10.30880/jts.2023.15.02.009
	Judul	Explainable AI For Cybersecurity Automation, Intelligence, and Trustworthiness In Digital Twin: Methods, Taxonomy, Challenges and Prospects
	Jurnal	Korean Institute of Communications and Information Sciences
	Volume dan Halaman	Vol. 10 No. 4, hal 935-958
	Tahun	2024

	Penulis	Iqbal H Sarker, et all
	Link	https://doi.org/10.1016/j.icte.2024.05.007
	Judul	Cyber Strategy in Practice
	Jurnal	The Rusi Journal
	Volume dan Halaman	Vo. 169 No. 3
	Tahun	2024
	Penulis	Tom Johansmeyer, Gareth Mott, Jason R C Nurse
	Link	https://doi.org/10.1080/03071847.2024.2377544
	Judul	The Role of the Cybersecurity Strategy of the Republic of Poland in Ensuring Cybersecurity
	Jurnal	Polish Political Science Yearbook
	Volume dan Halaman	Vol. 52 No. 3 & hal 61-69
	Tahun	2023
	Penulis	Miroslaw Karpiuk, Anna Makuch, Urszula Soler
	Link	https://doi.org/10.15804/ppsy202383
	Judul	Perceptions and Dilemmas Around Cyber-Security In A Spanish Research Center After A Cyber-Attack
	Jurnal	International Journal of Information Security
	Volume dan Halaman	Vol. 23 No. 3 & hal 1477-1512
	Tahun	2024
	Penulis	Adan Joaquin Navajas, Gelabert Eulalia, et all
	Link	https://doi.org/10.1007/s10207-024-00847-7
	Judul	Risks to Cybersecurity From Data Localization, Organized By Techniques, Tactics and Procedures
	Jurnal	Journal of Cyber Policy
	Volume dan Halaman	Vol. - & hal 1-32
	Tahun	2024
	Penulis	Swire Peter, Mayo DeBrae Kennedy, et all
	Link	https://doi.org/10.1080/23738871.2024.2384724
	Judul	An Assessment Of Cybersecurity Performance In The Saudi Universities: A Total Quality Management Approach
	Jurnal	Cogent Education
	Volume dan Halaman	Vol. 10 No.2, hal 1-16
	Tahun	2023
	Penulis	Alhumud Tahani Abdullah, et all
	Link	https://doi.org/10.1080/2331186X.2023.2265227
	Judul	The Infodemic as a Threat to Cybersecurity
	Jurnal	The International Journal of Intelligence, Security, and Public Affairs
	Volume dan Halaman	Vol. 23 No. 3, hal 180-196
	Tahun	2021
	Penulis	Tiffany Smith

	Link	https://doi.org/10.1080/23800992.2021.1969140
.	Judul	Analysis of Encrypted Network Traffic for Enhancing Cyber-security in Dynamic Environments
	Jurnal	Applied Artificial Intelligence
	Volume dan Halaman	Vol. 38 No.1
	Tahun	2024
	Penulis	Faeiz Alserhani
	Link	https://doi.org/10.1080/08839514.2024.2381882

Sumber : diolah peneliti (2024)

Langkah yang bisa dilakukan stelah menetapkan serta memilih jurnal yang akan menjadi subjek penelitian adalah melakukan tinjauan jurnal dengan review sebagai berikut:

Tabel 2. Hasil Review

Jurnal	**Review**	
	Judul	Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber dan Sandi Negara
	Permasalahan	Beberapa poin penting yang menjadi fokus permasalahan dalam artikel ini adalah tingginya ancaman di Indonesia, adanya keterbatasan sumber daya manusia, kebijakan dan regulasi yang belum optimal, kurangnya kolaborasi dan koordinasi antara berbagai pihak dalam menghadapi dan adanya perkembangan teknologi yang cepat
	Tujuan	Tujuan penelitian ini adalah untuk menganalisis dan memahami strategi Indonesia dalam membangun keamanan siber untuk menghadapi ancaman melalui Badan Siber dan Sandi Negara (BSSN). Penelitian ini bertujuan untuk menganalisis strategi yang diterapkan oleh BSSN dalam menghadapi dan menangani ancaman di Indonesia, mengidentifikasi tantangan yang dihadapi dalam implementasi strategi keamanan siber dan memberikan rekomendasi untuk meningkatkan efektivitas strategi keamanan siber yang ada
	Metode	Dalam penelitian ini beragam metode dan teknik digunakan, studi Pustaka untuk mengumpulkan berbagai sumber, termasuk laporan tahunan, kajian dari instansi pemerintah, dokumen perjanjian internasional, serta berita online yang berkaitan dengan keamanan siber. Metode deskriptif yang digunakan untuk menggambarkan dan menganalisis fenomena yang berkaitan demgan keamanan siber dan dan analisis kualitatif yang digunakan untuk memahami makna, konsep, dan karakteristik dari strategi keamanan siber yang diterapkan oleh BSSN dalam menghadapi ancaman
	Hasil Penelitian	Hasil penelitian ini memberikan gambaran yang jelas tentang kondisi keamanan siber di Indonesia dan langkah-langkah yang perlu diambil untuk meningkatkan efektivitas strategi yang ada dalam menghadapi ancaman
	Judul	The Impact of in Modern Generation Based on Systematic Literature Review Analysis

	Permasalahan	Penelitian ini membahas tentang beberapa isu kunci terhadap dampak pada generasi modern, diantaranya meningkatnya seiring meluasnya teknologi dan penggunaan internet yang menyebabkan semakin banyak banyak individu atau kelompok yang menjadi target serangan
	Tujuan	Tujuan yang diuraikan dalam penelitian ini adalah untuk menganalisis dampak terhadap generasi modern. Secara khusus penelitian ini bertujuan untuk mengidentifikasi berbagai dampak , meningkatkan kesadaran di antara individu dan organisasi tentang resiko
	Metode	Dalam penelitian ini menggunakan metode studi pustaka dengan meninjau secara sistematis terhadap jurnal yang ada dengan tema dampak
	Hasil Penelitian	Tinjauan literatur menyoroti bahwa kejahatan dunia maya memiliki dampak negatif yang luas terhadap stabilitas keuangan, kesejahteraan emosional, dan kepercayaan sosial, sehingga menekankan perlunya kesadaran dan tindakan pencegahan yang mendesak untuk memerangi masalah-masalah ini dalam lanskap digital modern
	Judul	Explainable AI For Cybersecurity Automation, Intelligence, and Trustworthiness in Digital Twin: Methods, Taxonomy, Challenges and Prospects
	Permasalahan	Dalam artikel ini mengidentifikasi beberapa tantangan dan masalah utama yang terkait dengan integrasi model keamanan siber. Berikut adalah beberapa isu utama yang dibahas yaitu adanya kerentanan keamanan yang dapat membahayakan kerahasiaan, integritas dan ketersediaan data, adanya tantangan dalam memperoleh data yang memadai dan mengembangkan algorima pemodelan yang efektif untuk keamanan siber berbasis AI, dan pentingnya membuat model AI yang dapat ditafsirkan dan dipercaya
	Tujuan	Penelitian ini bertujuan untuk meningkatkan ketahanan dan keamanan infrastruktur kembaran digital melalui penerapan teknik AI dan XAI yang canggih
	Metode	Metode yang digunakan dalam penelitian ini adalah kualitatif dengan meninjau terkait AI, XAI dan keamanan siber khususnya dalam konteks kembaran digital dan studi kasus dengan menyajikan beberapa kasus penggunaan di dunia nyata untuk menggambarkan bagaimana AI, XAI dapat diterapkan secara efektif dalam keamanan siber dalam kembaran digital
	Hasil Penelitian	Hasil penelitian menunjukkan bahwa meskipun terdapat tantangan yang harus diatasi, integrasi AI/XAI dalam keamanan siber untuk digital twins menawarkan jalan yang menjanjikan untuk meningkatkan langkah-langkah keamanan dan ketahanan terhadap ancaman siber.
	Judul	Cyber Strategy in Practice
	Permasalahan	Isu utama yang dibahas dalam penelitian ini terkait strategi keamanan siber nasional khususnya dalam konteks konflik yang sedang berlangsung di Ukraina. Isu isu utama tersebut meliputi: mengintegrasikan keamanan siber ke dalam strategi keamanan nasional yang lebih luas merupakan hal yang penting

	Tujuan	Tujuan dari penelitian ini adalah untuk menganalisis dan mengkritisi strategi keamanan siber nasional (NCSS) AS, Rusia, dan Ukraina dalam konflik yang sedang berlangsung di Ukraina.
	Metode	Metode yang digunakan dalam penelitian ini adalah pendekatan kualitatif dimana dengan mengkombinasikan analisis dokumen, analisis komparatif, analisis wacana dan evaluasi kontekstual dengan menyediakan kerangka kerja yang komprehensif untuk memahami kompleksitas strategi keamanan siber nasional
	Hasil Penelitian	Secara keseluruhan, hasil penelitian ini memberikan wawasan berharga mengenai efektivitas dan tantangan strategi keamanan siber nasional saat ini, dan menekankan perlunya adaptasi dan penyempurnaan berkelanjutan dalam menanggapi lanskap ancaman siber yang dinamis.
	Judul	The Role of the Cybersecurity Strategy of the Republic of Poland in Ensuring Cybersecurity
	Permasalahan	Jurnal ini membahas beberapa tantangan terkait keamanan siber di Polandia dengan menyoroti masalah utama, diantaranya kurangnya langkah-langkah keamanan siber yang memadai sehingga menyebabkan kerentanan yang melemahkan operasi sektor publik dan swasta
	Tujuan	Tujuan penelitian yang disajikan dalam artikel ini adalah menunjukkan pentingnya strategi keamanan siber nasional republic Polandia dalam memastikan penggunaan dunia maya yang aman
	Metode	Metode yang digunakan dalam penelitian ini adalah metode penelitian kualitatif yang dilakukan dengan cara menganalisis peraturan hukum yang berlaku yang mana mengatur aspek strategis keamanan siber. Metode ini melibatkan pemeriksaan undang-undang, peraturan, dan kerangka hukum yang ada unntuk memahami implikasi dan efektivitas dalam menangani masalah keamanan siber
	Hasil Penelitian	Hasil penelitian menunjukkan bahwa meskipun Strategi Keamanan Siber Polandia merupakan alat penting untuk meningkatkan keamanan siber, strategi ini harus terus dievaluasi dan diadaptasi untuk mengatasi tantangan yang muncul dan memastikan lingkungan digital yang aman bagi semua pemangku kepentingan.
	Judul	Perceptions and Dilemmas Around Cyber-Security in a Spanish Research Center after A Cyber- Attack
	Permasalahan	Artikel ini membahas beberapa masalah yang terkait dengan keamanan siber di sebuah pusat penelitian di Spanyol setelah serangan siber yang signifikan.
	Tujuan	Tujuan penelitian yang disajikan dalam artikel ini adalah untuk menilai dampak serangan siber terhadap persepsi karyawan terhadap keamanan siber di sebuah pusat penelitian di Spanyol.
	Metode	Metode yang digunakan dalam penelitian yang disajikan dalam artikel ini adalah pendekatan metode campuran. Metodologi ini menggabungkan teknik penelitian kuantitatif dan kualitatif untuk memberikan pemahaman yang komprehensif tentang dampak serangan siber terhadap persepsi keamanan siber.

	Hasil Penelitian	Secara keseluruhan, hasil penelitian ini memberikan wawasan berharga mengenai kompleksitas persepsi keamanan siber dalam konteks penelitian dan menyoroti perlunya pendekatan seimbang yang membahas keamanan dan sifat inovatif dari kegiatan penelitian.
	Judul	Risks to cybersecurity from data localization, organized by techniques, tactics, and procedures.
	Permasalahan	Artikel ini membahas beberapa masalah yang terkait dengan undang-undang lokalitas data dan dampaknya pada keamanan siber.
	Tujuan	Tujuan dari penelitian yang disajikan dalam artikel "Risiko terhadap keamanan siber dari lokalitas data" adalah untuk menganalisis dan menyoroti risiko keamanan siber yang terkait dengan undang-undang lokalitas data.
	Metode	Secara keseluruhan, metodologi ini menggabungkan analisis kualitatif dan kuantitatif, memanfaatkan kerangka kerja yang mapan dan bukti empiris untuk menilai dampak lokalisasi data pada praktik keamanan siber.
	Hasil Penelitian	Secara keseluruhan, hasil penelitian menunjukkan bahwa meskipun lokalitas data sering dipromosikan sebagai cara untuk meningkatkan perlindungan data, hal ini dapat menciptakan risiko yang signifikan terhadap praktik keamanan siber dan efektivitas strategi pertahanan siber secara keseluruhan.
	Judul	An assessment of cybersecurity performance in the Saudi universities: A Total Quality Management approach
	Permasalahan	Artikel ini mengidentifikasi beberapa masalah utama terkait keamanan siber di beberapa universitas Saudi, antara lain terdapat kurangnya kesadaran keamanan siber di kalangan pelajar, yang disebabkan oleh berbagai faktor seperti kurangnya pelatihan dan pendidikan mengenai praktik keamanan siber, banyak universitas tidak memiliki kebijakan dan prosedur keamanan siber yang terdefinisi dengan baik. Kurangnya struktur ini dapat menyebabkan kerentanan dan respons yang tidak efektif terhadap ancaman siber.
	Tujuan	Tujuan penelitian yang diuraikan dalam artikel ini antara lain mengevaluasi kinerja keamanan siber universitas Saudi berdasarkan teori motivasi perlindungan, mengintegrasikan keamanan siber ke dalam manajemen mutu total, dan memberikan rekomendasi untuk peningkatan kinerja keamanan siber
	Metode	Metode yang digunakan dalam artikel ini adalah analisis kuantitatif yang didapatkan dari kuesioner serta analisis kualitatif yang diperoleh dari wawancara
	Hasil Penelitian	Hasil ini menggarisbawahi perlunya universitas-universitas Saudi untuk meningkatkan praktik keamanan siber mereka, meningkatkan kesadaran dan pelatihan, dan mengintegrasikan keamanan siber dengan lebih baik ke dalam tujuan strategis keseluruhan dan proses manajemen mutu mereka.
	Judul	The Infodemic as a Threat to Cybersecurity
	Permasalahan	Dalam artikel ini mengidentifikasi beberapa masalah utama yang

		terkait miss informasi dan keamanan siber. Masalah utama tersebut diantaranya adanya eksploitasi oleh penjahat siber, adanya penyebaran informasi yang tidak akurat, terdapat kesenjangan akuntabilitas yang signifikan di dunia maya
	Tujuan	Tujuan yang diharapkan dalam artikel ini adalah memahami hubungan antara infodemi dan keamanan siber, menjelaskan bagaimana serangan ini merusak keamanan, martabat dan kesetaraan manusia di dunia maya, mengidentifikasi tantangan akibat infodemic dan mengeksplorasi solusi potensial untuk memerangi ancaman yang ditimbulkan oleh infodemi
	Metode	Metode yang digunakan dalam artikel ini menggabungkan analisis kualitatif, studi kasus dan tinjauan literatur untuk memberikan pemahaman komprehensif tentang masalah yang dihadapi dan untuk menginformasikan solusi potensial
	Hasil Penelitian	Secara keseluruhan, hasil penelitian ini menggarisbawahi kebutuhan mendesak akan pendekatan komprehensif terhadap keamanan siber yang mempertimbangkan tantangan unik yang ditimbulkan oleh infodemik, dengan fokus pada perlindungan hak asasi manusia dan meningkatkan ketahanan terhadap ancaman siber.
.	Judul	Analysis of Encrypted Network Traffic for Enhancing Cyber-security in Dynamic Environments
	Permasalahan	Dalam artikel ini membahas beberapa isu utama terkait analisis lalu lintas jaringan terenskripsi dan implikasinya terhadap keamanan siber
	Tujuan	Penelitian ini bertujuan untuk mengusulkan penerapan metodologi canggih untuk meningkatkan efektivitas IDS dalam menganalisis lalu lintas terenkripsi, menciptakan kerangka kerja yang kuat yang mampu mengintegrasikan berbagai teknik canggih untuk mengoptimalkan pemilihan pengguna dan saluran untuk mendeteksi intruksi di lingkungan dinamis dan memberikan pendekatan komprehensif yang dapat beradaptasi dengan lansekap ancaman siber yang berubah dengan cepat
	Metode	Metode yang digunakan dalam penelitian ini adalah kualitatif
	Hasil Penelitian	Hasil penelitian menunjukkan bahwa metodologi yang diusulkan efektif meningkatkan keamanan jaringan yang menangani lalu lintas terenkripsi, memberikan arah yang menjanjikan dalam keamanan siber

Sumber : diolah peneliti (2024)

Pembahasan

Pembahasan dari literature review yang sudah disampaikan diatas yang mencakup dari berbagai topik antara lain:

a. Strategi Indonesia Membentuk *Cyber Security* Dalam Menghadapi Ancaman *Cyber Crime* Melalui Badan Siber dan Sandi Negara

   Penelitian ini dilakukan dengan tujuan untuk mengkaji maupun memahami strategi Indonesia dalam membentuk keamanan siber dalam menghadapi ancaman . Hasil penelitian menunjukkan bahwa dengan adanya penyusunan perangkat hukum dan kebijakan yang jelas serta komprehensif diimbangi dengan adanya optimalisasi tugas serta fungdi BSSN dan CERT sangat diperlukan untuk meningkatkan respon terhadap insiden keamanan siber

b. *The Impact of in Modern Generation Based on Systematic Literature Review Analysis*

   Penelitian ini berfokus pada dampak yang ditimbulkan akibat terhadap generasi modern baik dalam segi keuangan, kesejahteraan emosional maupun terhadap kepercayaan sosial. Adapun hasil penelitian menunjukkan bahwa kejahatan dunia maya memiliki dampak negatif yang luas sehingga perlunya kesadaran dan tindakan pencegahan yang mendesak demi meminimalisir masalah ini

c. *Explainable AI For Cybersecurity Automation, Intelligence, and Trustworthiness in Digital Twin: Methods, Taxonomy, Challenges and Prospects*

   Penelitian ini dilakukan dengan tujuan untuk meningkatkan ketahanan dan keamanan infrastuktur digital twins melalui teknik AI atau XAI yang canggih. Hasil penelitian menunjukkan bahwa AI maupun XAI mampu diterapkan secara efektif dalam keamanan siber. Selain itu, AI dan XAI juga memiliki potensi signifikan untuk meningkatkan ketahanan keamanan siber di lingkungan digital twins

d. *Cyber Strategy in Practice*

   Penelitian ini berfokus untuk menganalisis dan mengkritisi strategi keamanan siber nasional (NCSS) dari negara Amerika Serikat, Rusia dan Ukraina dalam konflik yang sedang berlangsung. Hasil penelitian menunjukkan bahwa perlunya adaptasi serta penyempurnaan yang berkelanjutan dalam menanggapi lansekap ancaman siber yang dinamis.

e. *The Role of the Cybersecurity Strategy of the Republic of Poland in Ensuring Cybersecurity*

   Penelitian ini dilakukan karena adanya kerentanan keamanan siber diimbangi dengan para pelaku kejahatan siber yang semakin canggih. Dan hasil penelitian ini menunjukkan bahwa pentingnya strategi keamanan siber nasional yang berfungsi sebagai kerangka kerja penting untuk melindungi dunia maya. Selain itu, perlunya koordinasi serta kolaborasi yang efektif antara berbagai pemangku kepentingan demi

mendorong pendekatan komprehensif terhadap keamanan siber. Pentingnya program pendidikan, informasi, dan pelatihan juga menjadi salah satu faktor penting yang dibutuhkan dalam meningkatkan kesadaran warga negara dan organisasi.

f. *Perceptions and Dilemmas Around Cyber-Security in a Spanish Research Center after A Cyber- Attack*

   Penelitian ini berfokus pada dampak yang dihasilkan dari serangan siber di sebuah pusat penelitian di Spanyol. Adapun hasil penelitian bahwa terdapat dampak yang signifikan atas persepsi karyawan terhadap keamanan TIK. Adanya kesadaran dan perhatian terkait isu keamanan siber menunjukkan bahwa serangan siber tersebut menjadi peringatan bagi banyak karyawan. Adanya pesan yang jelas dan konsisten dari pihak manajemen tentang pentingnya keamanan siber juga membantu meningkatkan pemahaman dan kepatuhan karyawan

g. *Risks to cybersecurity from data localization, organized by techniques, tactics, and procedures.*

   Penelitian ini berfokus untuk menganalisis dan menyoroti resiko keamanan siber terkait penerapan undang-undang lokalisasi data. Hasil penelitian menunjukkan perlunya pemeriksaan yang cermat terhadap kebijakan lokalisasi data untuk menghindari bahaya keamanan siber yang signifikan yang dapat timbul dari persyaratan lokalisasi yang ketat.

h. *An assessment of cybersecurity performance in the Saudi universities: A Total Quality Management approach*

   Penelitian ini dilakukan karena adanya beberapa permasalahan diantaranya adalah kurangnya kesadaran pelajar terhadap praktik keamanan siber, diimbangi dengan banyaknya universitas yang tidak memiliki kebijakan serta prosedur keamanan siber yang dapat dijelaskan dengan baik. Hasil penelitian menunjukkan bahwa pentingnya meningkatkan praktik keamanan siber dalam lingkungan universitas, meningkatkan kesadaran serta mengadakan pelatihan demi mencapai tujuan strategis.

i. *The Infodemic as a Threat to Cybersecurity*

   Penelitian ini dilakukan dengan tujuan untuk memahami hubungan antara infodemi dan keamanan serta memahami bagaiman serangan siber mampu merusak keamanan. Hasil penelitian menunjukkan bahwa adanya peningkatan ancaman siber yang mana khususnya akan menyerang populasi tertentu dimana populasi tersebut memiliki keterbatasan liberasi digital. Sehingga perlunya mekanisme pelaporann yang lebih baik demi meningkatkan pemahaman tentang sifat dan dampak serangan siber

j. Analysis of Encrypted Network Traffic for Enhancing Cyber-security in Dynamic Environments

Penelitian ini berfokus pada penerapan metodologi canggih yang digunakan untuk meningkatkan efektivitasnya dalam mengurangi dampak serangan siber. Berdasarkan hasil penelitian menunjukkan bahwa metodologi yang dimaksud efektif meningkatkan keamanan jaringan serta mampu memberikan arah yang menjanjikan dalam keamanan siber

5. KESIMPULAN

Dari hasil studi literatur dapat disimpulkan bahwa cyber crime merupakan ancaman serius yang terus berkembang seiring dengan kemajuan teknologi. sendiri memiliki dampak negatif yang bisa mempengaruhi baik terhadap stabilitas keuangan, kesejahteraan emosional, serta kepercayaan sosial. Selain itu, juga dapat menyebabkan kerentanan yang nantinya akan melemahkan operas sektor publik dan swasta. Dalam menghadapi ancaman ini, diperlukan strategi pengamanan siber yang komprehensif dan adaptif. Adanya implementasi teknologi seperti enkripsi, integrasi AI maupun XAI dalam keamanan siber juga mampu meningkatkan langkah-langkah keamanan dan ketahanan terhadap ancaman siber. Selain itu, penyusunan perangkat hukum dan kebijakan yang jelas dan komprehensif sangat penting untuk mendukung keamanan siber. Hal ini mencakup penyusunan strategi keamanan siber nasional yang dapat mengarahkan tindakan dan kebijakan yang lebih efektif. Serta pentingnya edukasi dan peningkatan kesadaran masyarakat mengenai keamanan siber juga merupakah salah satu langkah penting. Masyarakat yang lebih sadar akan risiko dan cara melindungi diri dapat membantu mengurangi dampak dari ancaman . Pengembangan lebih lanjut dalam bidang keamanan siber, termasuk peningkatan pelatihan bagi tenaga ahli, penguatan kerjasama internasional, dan pengembangan teknologi yang lebih baik untuk mendeteksi dan merespons ancaman. Namun, tantangan dalam implementasi strategi ini tetap ada, baik dari segi teknis maupun non-teknis, yang memerlukan perhatian khusus dari peneliti dan praktisi di bidang keamanan siber

DAFTAR PUSTAKA

Alhumud, T. A. A., Omar, A., & Altohami, W. M. A. (2023). An assessment of cybersecurity performance in Saudi universities: A Total Quality Management approach. *Cogent Education, 10*(2). https://doi.org/10.1080/2331186X.2023.2265227

Alserhani, F. (2024). Analysis of encrypted network traffic for enhancing cybersecurity in dynamic environments. *Applied Artificial Intelligence, 38*(1). https://doi.org/10.1080/08839514.2024.2381882

Chai, K. M., Xuan, A. Z., & Abdullah, M. H. (2023). The impact of [title incomplete] in modern generation based on systematic literature review analysis. *Journal of Techno-Social, 15*(2). https://doi.org/10.30880/jts.2023.15.02.009

Ginanjar, Y. (2022). Strategi Indonesia membentuk cyber security dalam menghadapi ancaman cyber crime melalui Badan Siber dan Sandi Negara. *Jurnal Dinamika Global, 7*(02), 291–312. https://doi.org/10.36859/jdg.v7i02.1187

Indah, F., Sidabutar, A., & Annisa, N. (2022). Peran cyber security terhadap keamanan data penduduk negara Indonesia (Studi kasus: Hacker Bjorka). *Jurnal Bidang Penelitian Informatika, 1*(1), 1–8.

Johansmeyer, T., Mott, G., & Nurse, J. R. C. (2024). Cyber strategy in practice. *The RUSI Journal, 169*(3), 40–51. https://doi.org/10.1080/03071847.2024.2377544

Karpiuk, M., Makuch, A., & Soler, U. (2023). The role of the Cybersecurity Strategy of the Republic of Poland in ensuring cybersecurity. *Polish Political Science Yearbook, 52*(3), 61–69. https://doi.org/10.15804/ppsy202383

Navajas-Adán, J., Badia-Gelabert, E., Jiménez-Saurina, L., Marijuán-Martín, M. J., & Mayo-García, R. (2024). Perceptions and dilemmas around cybersecurity in a Spanish research center after a cyber-attack. *International Journal of Information Security, 23*(3), 2315–2331. https://doi.org/10.1007/s10207-024-00847-7

Sarker, I. H., Janicke, H., Mohsin, A., Gill, A., & Maglaras, L. (2024). Explainable AI for cybersecurity automation, intelligence, and trustworthiness in digital twin: Methods, taxonomy, challenges, and prospects. *ICT Express, 10*(4), 935–958. https://doi.org/10.1016/j.icte.2024.05.007

Smith, T. (2021). The infodemic as a threat to cybersecurity. *International Journal of Intelligence, Security, and Public Affairs, 23*(3), 180–196. https://doi.org/10.1080/23800992.2021.1969140

Swire, P., Kennedy-Mayo, D., Bagley, D., Krasser, S., Modak, A., & Bausewein, C. (2024). Risks to cybersecurity from data localization, organized by techniques, tactics, and procedures. *Journal of Cyber Policy*, 1–32. https://doi.org/10.1080/23738871.2024.2384724