Temali: Jurnal Pembangunan Sosial
eISSN: 2615-5028, Vol 8, No 1, 2025, pp. 29-40
http://dx.doi.org/10.15575/jt.v8i1.38690

Membangun Ketahanan Digital: Pengembangan Model Strategi Pertahanan Siber Berbasis Manajemen Risiko

Andi Sutomo
Universitas Pertahanan Republik Indonesia
andisutomo888@gmail.com

Suyono Thamrin
Universitas Pertahanan Republik Indonesia
suyono.thamrin@gmail.com

Pujo Widodo
Universitas Pertahanan Republik Indonesia
pujowidodo78@gmail.com

Yono Reksoprodjo
Universitas Pertahanan Republik Indonesia
yono@sintesagroup.com

Suggested Citation:

Sutomo, Andi; Thamrin, Suyono; Widodo, Pujo; Reksoprodjo, Yono. (2025). Membangun Ketahanan Digital: Pengembangan Model Strategi Pertahanan Siber Berbasis Manajemen Risiko. *Temali: Jurnal Pembangunan Sosial*, Volume 8, Nomor 1: 29–40. http://dx.doi.org/10.15575/jt.v8i1.38690.

Article's History:

Received December 2024; *Revised* January 2025; *Accepted* January 2025.

Abstract:

This research aims to develop a cyber defense strategy model based on risk management to enhance national resilience against increasingly complex cyber threats. The study uses a qualitative approach with data collection techniques through literature review and data analysis assisted by NVivo 12 Pro software to organize, code, and analyze the data thematically. The results show that the risk management-based cyber defense strategy model includes integrated stages of planning, organizing, implementation, and evaluation to address various cyber threats. This model also emphasizes the importance of cross-sector cooperation and the role of cyber diplomacy in maintaining national security stability. This research contributes a strategic framework based on risk management that can serve as a reference for the development of national cyber defense policies and enhancing Indonesia's position in global information security.

Keywords: cyber defense, risk management, information security, national strategy, NVivo.

Abstrak:

Penelitian ini bertujuan untuk mengembangkan model strategi pertahanan siber berbasis manajemen risiko guna meningkatkan ketahanan nasional terhadap ancaman siber yang semakin kompleks. Penelitian menggunakan pendekatan kualitatif dengan teknik pengumpulan data melalui studi pustaka dan analisis data berbantuan perangkat lunak NVivo 12 Pro untuk mengorganisasikan, mengkoding, dan menganalisis data secara tematik. Hasil penelitian menunjukkan bahwa model strategi pertahanan siber berbasis manajemen risiko mencakup tahapan

perencanaan, pengorganisasian, pelaksanaan, dan evaluasi secara terintegrasi untuk menghadapi berbagai ancaman siber. Model ini juga menyoroti pentingnya kerja sama lintas sektor dan peran diplomasi siber dalam menjaga stabilitas keamanan nasional. Penelitian ini memberikan kontribusi berupa kerangka kerja strategis berbasis manajemen risiko yang dapat menjadi acuan dalam pengembangan kebijakan pertahanan siber nasional dan peningkatan posisi Indonesia dalam keamanan informasi global.

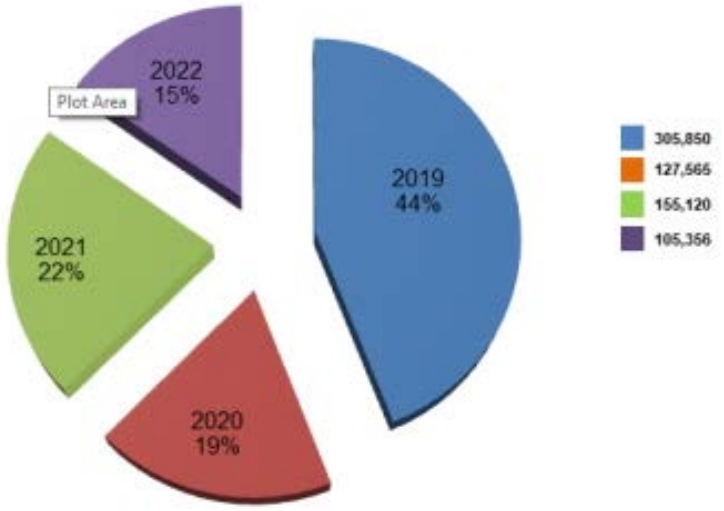
Kata Kunci: *pertahanan siber, manajemen risiko, keamanan informasi, strategi nasional, NVivo.*

PENDAHULUAN

Perkembangan pesat ilmu pengetahuan dan teknologi informasi dalam beberapa dekade terakhir telah merevolusi cara manusia menjalani kehidupan. Ketergantungan pada sistem digital yang terintegrasi di hampir semua sektor, termasuk pemerintahan, ekonomi, dan militer, telah meningkatkan efisiensi sekaligus memperbesar risiko keamanan (Aslan et al., 2023). Salah satu ancaman serius yang terus berkembang adalah serangan siber yang tidak hanya bersifat merugikan tetapi juga sangat kompleks dan canggih (Mahmudov, 2023). Indonesia, sebagai salah satu negara dengan transformasi digital yang berkembang pesat, menghadapi ancaman siber yang terus meningkat, terutama pada sektor strategis seperti pertahanan nasional.

Salah satu bukti nyata adalah tingginya intensitas serangan siber terhadap Kementerian Pertahanan Republik Indonesia (Kemhan RI). Berdasarkan data dari Pusat Pertahanan Siber Kemhan RI (Pushansiber), jumlah serangan siber yang menyasar instansi ini menunjukkan tren fluktuatif tetapi tetap signifikan. Pada tahun 2019, tercatat 305.850 serangan siber, kemudian menurun pada 2020 menjadi 127.565 serangan. Namun, angka ini kembali meningkat pada 2021 dengan total 155.120 serangan. Hingga April 2022, sudah tercatat 105.356 serangan. Data ini menunjukkan bahwa ancaman siber bersifat dinamis, tergantung pada kondisi geopolitik, motivasi penyerang, dan kerentanan sistem. Gambar 1 di bawah ini menggambarkan rata-rata serangan siber yang dihadapi Kemhan RI dari tahun 2019 hingga 2022 (Pushansiber Kemhan RI, 2022).

Gambar 1. Rata-rata serangan siber terhadap Kemhan RI per tahun



Sumber: Pushansiber Kemhan RI, 2022.

Serangan ini menunjukkan bahwa keberlanjutan operasional dan perlindungan terhadap infrastruktur digital vital, khususnya di sektor pertahanan, menjadi prioritas yang mendesak. Jika tidak diatasi secara serius, hal ini berpotensi mengancam kedaulatan negara (Lehto, 2022).

Selain serangan langsung terhadap sistem pertahanan, ancaman siber juga mencakup aktivitas seperti spionase, sabotase, vandalisme digital, dan serangan pada elemen vital lainnya seperti jaringan listrik dan infrastruktur telekomunikasi (Lindsay, 2021). Dalam konteks global, kemampuan Indonesia dalam mempertahankan lalu lintas informasi dari ancaman-ancaman ini masih dianggap lemah (Krisnata et al., 2020). Kasus-kasus *hacking,* spionase, dan sabotase menunjukkan rendahnya dominasi serta kontrol atas

lalu lintas informasi strategis (Jacks & Adler, 2015). Kelemahan ini menggarisbawahi kebutuhan mendesak untuk membangun sistem pertahanan siber nasional yang kuat, komprehensif, dan adaptif terhadap ancaman yang terus berkembang (Mahadwartha, & Ismiyanti, 2022).

Kajian literatur menunjukkan bahwa strategi adalah elemen kunci dalam memastikan keberhasilan suatu organisasi, terutama dalam menghadapi tantangan yang kompleks (Robinson, 2021). Strategi merupakan elemen kunci dalam keberhasilan organisasi, terutama dalam menghadapi tantangan yang kompleks (Rai et al., 2019). Sun-Tzu (2002) dalam *The Art of War* menekankan pentingnya pemahaman mendalam tentang musuh dan diri sendiri dalam merancang strategi yang efektif. Hunger (2010) mendefinisikan strategi sebagai model atau rencana yang menggabungkan tujuan utama, kebijakan, dan tindakan untuk mencapai hasil yang diinginkan. Dalam konteks pertahanan siber, Rai et al. (2019) menyebutkan bahwa strategi pertahanan siber melibatkan langkah-langkah untuk melindungi ruang siber demi mencapai tujuan strategis suatu negara.

Penelitian sebelumnya telah memberikan kontribusi signifikan dalam memahami berbagai aspek pertahanan siber. Sun et al. (2023) menyurvei pendekatan penambangan intelijen ancaman siber untuk pertahanan siber yang proaktif. Penelitian mereka menyoroti pentingnya analisis prediktif dalam mengantisipasi ancaman sebelum terjadi, meskipun implementasinya masih menghadapi tantangan teknis. Zhang dan Thing (2021) merefleksikan tiga dekade teknik penipuan dalam pertahanan siber aktif, yang meskipun efektif, membutuhkan strategi yang lebih holistik untuk menghadapi ancaman yang terus berkembang.

Husák et al. (2021) meneliti metode prediktif dalam pertahanan siber, menunjukkan bahwa penggunaan algoritma prediktif dapat meningkatkan deteksi dini terhadap ancaman. Namun, penelitian ini lebih fokus pada aspek teknis dan kurang memperhatikan integrasi manajemen risiko sebagai bagian dari strategi yang lebih luas. Yurekten dan Demirci (2021) membahas manfaat pertahanan siber berbasis Software-Defined Networking (SDN), tetapi implementasi teknologi ini membutuhkan kerangka kerja yang lebih jelas untuk manajemen risiko. Lee dan Kim (2021) mengeksplorasi penggunaan *blockchain* sebagai alat pertahanan siber, menunjukkan potensi *blockchain* dalam meningkatkan keamanan, tetapi juga mencatat tantangan dalam skalabilitas dan adopsi teknologi ini.

Broeders (2021) membahas konsep pertahanan siber aktif oleh sektor swasta, yang meskipun dapat meningkatkan keamanan, memerlukan koordinasi yang lebih baik dengan pemerintah untuk menghindari konflik hukum dan diplomasi. Penelitian lain oleh Al-Dosari et al. (2024) berfokus pada penerapan kecerdasan buatan dalam pertahanan siber di sektor perbankan. Mereka menemukan bahwa AI dapat meningkatkan efisiensi pertahanan siber, tetapi menghadapi tantangan dalam hal keandalan data dan risiko bias algoritmik.

Dari kajian literatur ini, terlihat bahwa sebagian besar penelitian sebelumnya menekankan pada pengembangan teknologi pertahanan siber, seperti *blockchain,* kecerdasan buatan, dan metode prediktif. Namun, penelitian-penelitian ini kurang memperhatikan integrasi strategi berbasis manajemen risiko yang mencakup aspek perencanaan, pengorganisasian, pelaksanaan, dan evaluasi secara menyeluruh. Selain itu, penelitian yang membahas diplomasi siber dan peran Indonesia dalam geopolitik pertahanan siber juga masih sangat terbatas.

Penelitian ini mengisi gap yang ada dengan mengintegrasikan pendekatan manajemen risiko ke dalam strategi pertahanan siber, yang belum banyak dibahas secara komprehensif dalam literatur sebelumnya. Selain itu, penelitian ini memberikan kontribusi unik dengan mempertimbangkan dinamika ancaman siber dalam konteks geopolitik serta kebutuhan diplomasi siber Indonesia. Model strategi yang dikembangkan tidak hanya menawarkan pendekatan teknis tetapi juga mencakup aspek perencanaan strategis dan manajemen risiko untuk meningkatkan ketahanan nasional.

Oleh karena itu, penelitian ini bertujuan untuk mengembangkan model strategi pertahanan siber berbasis manajemen risiko guna meningkatkan ketahanan nasional terhadap ancaman siber. Model ini dirancang untuk memenuhi ekspektasi global sekaligus memperkuat posisi Indonesia dalam diplomasi dan keamanan informasi global.

Penelitian ini berargumen bahwa strategi pertahanan siber berbasis manajemen risiko adalah pendekatan yang paling efektif untuk menghadapi kompleksitas ancaman siber. Pendekatan ini melibatkan perencanaan, pengorganisasian, pelaksanaan, dan evaluasi yang terstruktur, sehingga memungkinkan identifikasi dan mitigasi risiko secara proaktif. Dengan strategi ini, Indonesia dapat memperkuat keamanan nasional, melindungi infrastruktur informasi vital, dan meningkatkan daya saing di arena geopolitik serta teknologi global.

METODE

Penelitian ini berfokus pada analisis strategi pertahanan siber berbasis manajemen risiko dengan mengambil kasus pada sektor pertahanan nasional Indonesia, khususnya pada Kementerian Pertahanan Republik Indonesia (Kemhan RI). Objek penelitian dipilih berdasarkan tingginya frekuensi serangan siber yang dilaporkan oleh Pushansiber Kemhan RI (2022) dalam beberapa tahun terakhir, yang menunjukkan kerentanan signifikan terhadap infrastruktur digital strategis. Penelitian ini juga mengkaji fenomena ancaman siber secara luas dalam konteks geopolitik dan teknologi global.

Penelitian ini menggunakan pendekatan kualitatif yang memungkinkan eksplorasi mendalam terhadap permasalahan yang kompleks dan dinamis (Dirgantara et al., 2024; Lune & Berg, 2017; Maxwell, 2008). Data dalam penelitian ini dikumpulkan melalui studi pustaka, yang mencakup analisis dokumen, laporan tahunan, jurnal akademik, serta literatur yang relevan dengan topik penelitian. Studi pustaka dilakukan untuk memperoleh pemahaman yang komprehensif mengenai strategi pertahanan siber dan manajemen risiko dalam konteks nasional dan global.

Proses penelitian dilakukan melalui beberapa tahap. Pertama, identifikasi permasalahan dilakukan dengan mengkaji berbagai literatur dan laporan terkait ancaman siber dan pertahanan nasional. Kedua, pengumpulan data melalui studi pustaka dilakukan dengan menyeleksi sumber-sumber yang relevan dan berkualitas, baik dari jurnal ilmiah, laporan instansi pemerintah, maupun referensi akademik lainnya. Data yang terkumpul kemudian diorganisasikan dan dikategorikan berdasarkan tema atau topik yang relevan dengan tujuan penelitian.

Teknik analisis data dilakukan dengan menggunakan perangkat lunak NVivo 12 Pro untuk mendukung proses pengolahan data secara efisien. Data yang diperoleh dianalisis melalui tahapan reduksi data, penyajian data, dan penarikan kesimpulan (Miles & Huberman, 2013). NVivo membantu dalam melakukan koding, analisis tematik, dan triangulasi data dari berbagai sumber literatur. Proses ini memungkinkan pengujian keabsahan data melalui perbandingan hasil kajian pustaka serta membantu menyusun model strategi pertahanan siber berbasis manajemen risiko yang komprehensif.

HASIL DAN PEMBAHASAN

Tantangan Ketahanan Siber Nasional

Indonesia menghadapi tantangan serius dalam keamanan sibernya, yang memerlukan perhatian mendalam untuk memastikan keamanan dan stabilitas digital. Menurut laporan Global Cybersecurity Index (2017) yang diterbitkan oleh The ITU Telecommunication Development Sector (ITU-D), Indonesia mendapatkan nilai 0.424, menempatkan negara ini pada posisi ke-69 dari 164 negara dengan status *Maturing* (menuju kesiapan) (Bruggemann et al., 2022). Meskipun laporan tersebut menunjukkan kemajuan dibandingkan dengan beberapa negara berkembang lainnya, situasi keamanan siber Indonesia masih berada dalam tahap berbahaya dan kritis. Beberapa komponen, seperti sektor Computer Emergency Response Team (CERT), standar organisasi, strategi keamanan siber, matriks keamanan siber, praktik terbaik *(good practice),* program edukasi, industri dalam negeri, perjanjian bilateral, perjanjian multilateral, serta kerja sama antara pemerintah dan swasta, masih mendapat penilaian merah (Rizki, 2022). Hal ini menunjukkan perlunya reformasi menyeluruh untuk membangun ketahanan siber yang tangguh.

Ancaman keamanan siber terus berkembang dengan tingkat kecanggihan yang semakin tinggi. Serangan seperti *ransomware, phishing,* dan *malware* telah menjadi ancaman umum yang dihadapi organisasi di seluruh dunia, termasuk Indonesia (Bardin, 2025). Data sensitif sering menjadi target utama, baik di sektor pemerintahan maupun swasta. Kemampuan organisasi untuk mengelola risiko keamanan siber secara efektif menjadi sangat penting untuk melindungi data sensitif mereka. Dalam konteks ini, menurut Kalangi et al. (2022) banyak organisasi, termasuk industri perbankan, masih lemah dalam menerapkan Good Corporate Governance (GCG) dan manajemen risiko. Padahal, manajemen risiko adalah elemen fundamental dalam memastikan keamanan dan keandalan data.

Sebagai contoh, serangan *ransomware* WannaCry pada 2017 menunjukkan bagaimana serangan siber dapat melumpuhkan layanan publik dan mengancam infrastruktur kritis (Mohurle & Patil, 2017). Serangan ini menargetkan berbagai negara, termasuk Indonesia, menyebabkan kerugian finansial yang besar dan memengaruhi ribuan organisasi (Kao & Hsiao, 2018). Serangan ini menggarisbawahi kebutuhan mendesak untuk membangun pertahanan siber yang mampu mendeteksi, mencegah, dan merespons ancaman secara cepat dan efektif.

Serangan *ransomware* seperti WannaCry bukanlah satu-satunya ancaman siber yang signifikan di Indonesia. Berdasarkan data dari Kaspersky, jumlah kejahatan siber di Indonesia terus meningkat, dengan serangan *ransomware* menjadi salah satu modus yang paling sering digunakan. Pada tahun 2023, Indonesia mencatat 97.226 serangan ransomware. Metode ini dianggap efisien oleh pelaku karena dapat dieksekusi secara otomatis hanya dengan mengeksploitasi celah keamanan dan kebocoran kredensial. Bahkan, rata-rata 411.000 *malware* baru terdeteksi setiap harinya, menandakan semakin canggihnya teknologi yang digunakan para pelaku kejahatan siber (CNN Indonesia, 2024b).

Kejahatan siber juga semakin kompleks dengan berbagai jenis serangan yang menargetkan infrastruktur strategis. Data Kaspersky menunjukkan bahwa serangan phishing finansial mencapai 97.465 kasus, serangan insiden lokal sebanyak 16,4 juta, dan serangan Remote Desktop Protocol (RDP) sebanyak 11,7 juta pada 2023. Lanskap ancaman yang terus berkembang ini diperburuk oleh kurangnya alat pemantauan dan keterampilan staf keamanan siber di Indonesia, yang menjadikan 52% dari sistem keamanan siber nasional lebih sulit menangani ancaman dibandingkan tiga tahun sebelumnya (CNN Indonesia, 2024b).

Dampak nyata dari serangan siber ini terlihat pada insiden serangan *ransomware* terhadap Pusat Data Nasional (PDN) pada Juni 2024. Serangan ini menyebabkan gangguan besar pada layanan publik di sektor pendidikan, keamanan, keimigrasian, hingga kepegawaian. Tidak hanya itu, data dari lembaga strategis seperti Badan Intelijen Strategis (BAIS), Kementerian Perhubungan, dan INAFIS Polri dilaporkan bocor dan diperjualbelikan di *dark web* dengan nilai yang mencapai ratusan miliar rupiah. Insiden-insiden ini menunjukkan kerentanan signifikan terhadap keamanan data nasional, terutama di lembaga-lembaga vital (Javier, 2024).

Menurut laporan SAFEnet, insiden keamanan digital di Indonesia juga meningkat tajam pada awal 2024. Dalam periode Januari hingga Maret 2024, tercatat 61 serangan siber, hampir dua kali lipat dibandingkan periode yang sama tahun sebelumnya. Motif politik menjadi salah satu penyebab utama, terutama terkait Pemilu 2024 dan kritik terhadap pasangan calon presiden-wakil presiden. Contoh serangan ini adalah teror digital yang dialami Guru Besar Psikologi UGM Yogyakarta, Prof. Koentjoro Soeparno, dan rekan-rekannya setelah mereka terlibat dalam aksi Kampus Menggugat (CNN Indonesia, 2024a).

Situasi ini menunjukkan bahwa Indonesia berada dalam posisi yang rawan terhadap serangan siber. Berdasarkan riset Comparitech pada 2021, Indonesia menempati peringkat ke-18 dari 75 negara paling rentan terhadap ancaman siber. Posisi ini mengindikasikan adanya kebutuhan mendesak untuk meningkatkan ketahanan siber nasional, baik melalui pengembangan infrastruktur keamanan, pelatihan tenaga ahli, maupun kolaborasi lintas sektor (Javier, 2024).

Serangan siber yang telah dijelaskan berbahaya bagi keamanan nasional Indonesia. Hal ini karena Indonesia memiliki infrastruktur vital yang mencakup sektor keuangan, kelistrikan, telekomunikasi, dan pemerintahan, seperti Kementerian Pertahanan. Infrastruktur ini merupakan tulang punggung operasi negara yang harus dilindungi dari ancaman siber. Dalam dokumen Global Cybersecurity Index, perlindungan terhadap infrastruktur kritis di Indonesia masih menjadi tantangan besar, terutama dalam hal standar keamanan dan respons terhadap insiden siber (Iftikhar, 2024). Sebagai contoh, sektor kelistrikan merupakan salah satu infrastruktur yang sangat rentan terhadap serangan siber. Sebuah serangan terhadap jaringan listrik tidak hanya dapat menyebabkan gangguan layanan, tetapi juga memengaruhi stabilitas sosial dan ekonomi secara luas (Cui et al., 2021). Upaya perlindungan terhadap infrastruktur kunci ini harus menjadi bagian integral dari strategi pertahanan siber Indonesia. Hal ini memerlukan kolaborasi lintas sektor antara pemerintah, perusahaan swasta, dan komunitas teknologi untuk memastikan bahwa semua elemen infrastruktur kritis dilindungi secara memadai (Ding et al., 2022).

Ketahanan siber tidak hanya bergantung pada teknologi, tetapi juga pada sumber daya manusia yang terampil dan terlatih. Saat ini, Indonesia menghadapi kekurangan tenaga ahli di bidang keamanan siber. Pendidikan dan pelatihan menjadi faktor kunci untuk mengatasi masalah ini (Arianto & Anggraini, 2019). Menurut Rizki (2022), diperlukan peningkatan signifikan dalam pendidikan dan pelatihan keamanan siber, termasuk pelatihan bagi ahli keamanan siber dan kampanye kesadaran siber untuk masyarakat luas. Program pelatihan yang dirancang dengan baik dapat memberikan keterampilan yang diperlukan untuk mendeteksi, mencegah, dan merespons ancaman siber secara efektif. Selain itu, pelatihan kesadaran siber untuk masyarakat juga penting untuk mengurangi risiko serangan berbasis *social engineering,* seperti *phishing* (Bécue et al., 2021). Kampanye nasional yang fokus pada edukasi siber dapat membantu meningkatkan kesadaran masyarakat tentang pentingnya keamanan data pribadi dan cara melindunginya.

Regulasi dan kerangka kerja keamanan siber memainkan peran penting dalam menciptakan lingkungan yang aman secara digital. Namun, banyak regulasi di Indonesia yang masih dalam tahap pengembangan dan belum sepenuhnya diterapkan. Selain itu, kurangnya koordinasi antara berbagai lembaga pemerintah dan sektor swasta memperburuk situasi (Novita et al., 2024). Indonesia perlu mengembangkan kerangka kerja keamanan siber yang komprehensif, yang mencakup regulasi yang jelas, pedoman implementasi, dan mekanisme pengawasan yang efektif. Kerja sama internasional juga menjadi aspek penting dalam strategi keamanan siber, mengingat sifat ancaman siber yang tidak mengenal batas geografis, Indonesia perlu memperkuat hubungan dengan negara lain melalui perjanjian bilateral dan multilateral. Hal ini akan memungkinkan berbagi informasi, praktik terbaik, dan teknologi dalam upaya bersama untuk mengatasi ancaman siber global (Steingartner & Galinec, 2021).

Upaya ini mencerminkan kebutuhan akan pendekatan strategis yang mencakup penguatan teknologi, pendidikan, regulasi, dan kolaborasi lintas sektor. Dengan langkah-langkah yang terintegrasi, Indonesia dapat membangun ketahanan siber yang tangguh untuk melindungi kedaulatan digitalnya serta menciptakan lingkungan yang lebih aman bagi seluruh masyarakat dan sektor strategis.

Strategi Pertahanan Siber Berbasis Manajemen Risiko

Strategi pertahanan siber berbasis manajemen risiko menjadi kebutuhan mendesak dalam menghadapi ancaman kejahatan siber yang semakin kompleks. Bahri (2023) menjelaskan bahwa serangan siber adalah tindakan yang dilakukan oleh pihak-pihak dengan tujuan negatif, seperti peretas atau bahkan negara, untuk mengganggu sistem infrastruktur yang terkomputerisasi. Serangan ini tidak lagi bersifat individual, melainkan melibatkan negara atau aktor non-negara.

Peningkatan ancaman kejahatan siber, baik oleh negara maupun aktor non-negara, berdampak pada munculnya *cyber warfare* atau gangguan siber lainnya. Ketergantungan negara terhadap jaringan komunikasi menciptakan tantangan dan risiko tersendiri. Oleh karena itu, analisis manajemen risiko diperlukan untuk menghadapi ancaman ini, dengan tujuan menjaga pertahanan dan kedaulatan Negara Kesatuan Republik Indonesia (NKRI). Manajemen risiko adalah serangkaian prosedur dan metodologi yang digunakan untuk mengidentifikasi, mengukur, memantau, dan mengendalikan risiko yang timbul dalam suatu organisasi (Gurtu & Johny, 2021).

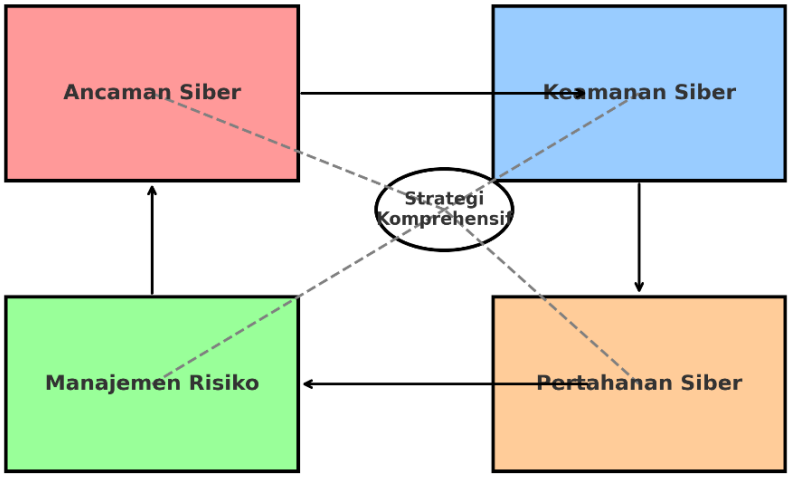
Risiko kejahatan siber memiliki potensi besar terhadap kehilangan data sistem informasi, kegiatan militer, dan gangguan lain yang memanfaatkan jaringan komputer serta internet (Broeders, 2021). Dalam menghadapi ancaman ini, pemerintah melalui Kementerian Pertahanan telah mempersiapkan diri dengan sumber daya manusia yang kompeten dalam teknologi, sistem infrastruktur yang andal, serta dukungan perundang-undangan yang memadai (Kementerian Pertahanan RI, 2024). Langkah dilakukan untuk melaksanakan operasi *cyber warfare* yang efektif (Sari, 2024).

Pertahanan siber merupakan mekanisme perlindungan terhadap jaringan komputer yang mencakup tindakan reaksi dan perlindungan terhadap infrastruktur penting (Kementerian Pertahanan RI, 2019). Selain itu, jaminan terhadap informasi yang dimiliki oleh suatu organisasi atau entitas pemerintahan juga menjadi prioritas. Konsep pertahanan siber menekankan tindakan pencegahan, pendeteksian, dan penanggulangan serangan siber secara tepat sehingga tidak ada infrastruktur atau informasi yang rusak (Bahri, 2023). Oleh karena itu, strategi pertahanan siber harus selalu memperhatikan manajemen risiko.

Keterkaitan antara objek penelitian, yaitu infrastruktur informasi vital di sektor pertahanan, dan subjek penelitian, seperti ahli keamanan siber, manajer industri pertahanan, dan akademisi, menjadi esensial dalam memahami dinamika strategi pertahanan siber. Pendekatan ini menghasilkan model pertahanan yang komprehensif dan relevan dengan kebutuhan nasional.

Badan Siber dan Sandi Negara (BSSN) memiliki peran utama dalam melaksanakan tugas pertahanan siber. Namun, BSSN tidak bergerak sendiri. Sesuai dengan konsep perang semesta, berbagai instansi dan lembaga saling bersinergi dalam memperkuat pertahanan nasional (Sari, 2024). Sebagai komponen utama dari infrastruktur siber nasional, BSSN bertanggung jawab merumuskan kebijakan, standar keamanan siber, dan strategi pertahanan siber. Meski demikian, konsep pertahanan siber di Indonesia belum sepopuler di negara lain seperti Amerika Serikat, Australia, atau Singapura.

Gambar 2. Model pengembangan strategi pertahanan siber berbasis manajemen risiko



Sumber: Hasil Penelitian, 2024.

Gambar 2 di atas merupakan representasi model pengembangan strategi pertahanan siber berbasis manajemen risiko menggunakan aplikasi NVivo. Model ini menunjukkan empat elemen utama yang saling berkaitan, yaitu ancaman siber, keamanan siber, pertahanan siber, dan manajemen risiko. Elemen-elemen ini menjadi fondasi dalam merancang strategi komprehensif untuk melindungi infrastruktur informasi vital nasional dari berbagai ancaman siber.

Pertama, ancaman siber. Ancaman siber mencakup berbagai risiko seperti serangan *malware, phishing, ransomware*, hingga serangan yang bersifat destruktif terhadap infrastruktur kritis. Menurut Agrafiotis et al. (2018), pelanggaran data dan serangan siber adalah peristiwa risiko utama yang mengancam organisasi di seluruh dunia. Identifikasi ancaman ini menjadi langkah awal dalam menyusun strategi pertahanan yang efektif, sebagaimana direkomendasikan oleh prinsip manajemen risiko.

Kedua, keamanan siber. Keamanan siber bertujuan untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi dalam sistem digital. Davis (2021) menekankan pentingnya pengelolaan keamanan informasi untuk menjaga keandalan teknologi yang semakin vital bagi operasi organisasi. Dalam konteks nasional, keamanan siber harus berfokus pada pencegahan, pendeteksian, dan mitigasi ancaman siber secara terintegrasi.

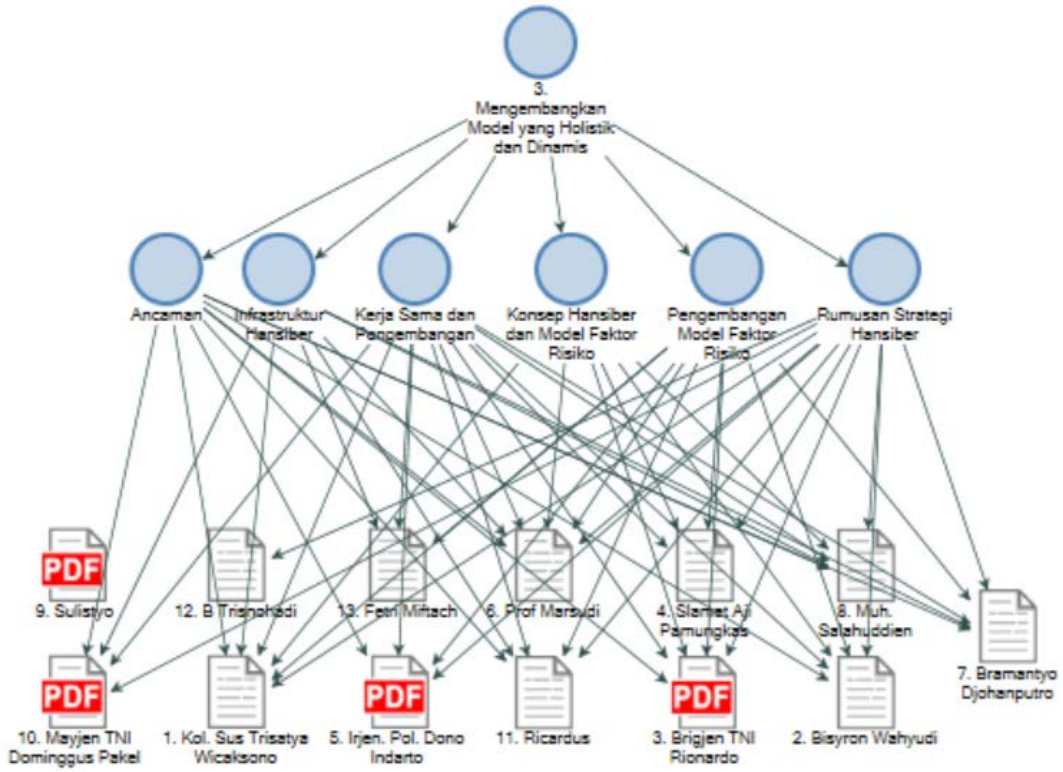
Ketiga, pertahanan siber. Pertahanan siber mencakup perlindungan aktif terhadap infrastruktur digital, termasuk reaksi terhadap insiden siber. Hal ini melibatkan strategi mitigasi risiko yang melibatkan kebijakan, prosedur, dan teknologi. Sesuai dengan pandangan Cebula et al. (2010), pendekatan berbasis manajemen risiko dapat mengurangi dampak insiden dengan memperkuat sistem pertahanan pada berbagai tingkat operasional.

Keempat, manajemen risiko. Manajemen risiko berfungsi sebagai kerangka kerja utama dalam model ini. Pendekatan ini mengidentifikasi, mengevaluasi, dan mengendalikan risiko yang dapat mengancam infrastruktur informasi vital. Menurut ISO 31000, penerapan manajemen risiko memungkinkan organisasi untuk memprioritaskan tindakan mitigasi berdasarkan tingkat risiko yang teridentifikasi (Bécue et al., 2021). Dalam hal ini, peran NVivo sebagai alat analisis data membantu merancang strategi yang berbasis bukti dan terukur.

Model ini menggarisbawahi pentingnya kolaborasi antara elemen-elemen tersebut dalam membangun strategi pertahanan siber yang efektif. Dengan menggunakan NVivo, analisis data yang dilakukan dapat menghasilkan wawasan yang mendalam untuk merancang strategi yang holistik. Pendekatan ini mendukung upaya mitigasi risiko, perlindungan infrastruktur vital, dan penciptaan kebijakan keamanan siber yang berkelanjutan. Kombinasi elemen ancaman, keamanan, pertahanan, dan manajemen risiko memberikan dasar yang kuat bagi pengembangan strategi pertahanan siber nasional.

Selanjutnya, setelah pembuatan model, data diolah melalui tahapan reduksi, koding, dan triangulasi. Proses ini menghasilkan visualisasi data, seperti yang ditampilkan pada Gambar 3. Visualisasi ini menunjukkan bahwa pengembangan model strategi pertahanan siber berbasis manajemen risiko harus melibatkan berbagai pihak. Selain itu, aspek-aspek yang perlu diperhatikan meliputi ancaman, infrastruktur, kerja sama, konsep pertahanan siber, serta pengembangan model strategi yang diinginkan.

Gambar 3. Visualisasi model strategi pertahanan siber berbasis manajemen risiko melalui Nvivo



Sumber: Hasil Penelitian, 2024.

Gambar 3 tersebut menggambarkan model pengembangan strategi pertahanan siber berbasis manajemen risiko yang terstruktur secara hierarkis. Pada bagian puncak, terdapat tujuan utama, yaitu *Mengembangkan Model yang Holistik dan Dinamis*. Tujuan ini mencerminkan pentingnya membangun strategi pertahanan siber yang komprehensif dan fleksibel untuk menghadapi tantangan yang terus berkembang.

Model ini terbagi menjadi beberapa komponen utama, yaitu *Ancaman, Infrastruktur Pertahanan, Kerja Sama dan Pengembangan, Konsep Hansiber dan Model Faktor Risiko, Pengembangan Model Faktor Risiko,* dan *Rumusan Strategi Hansiber*. Setiap komponen memiliki peran penting dalam mendukung pengembangan model yang diinginkan. Komponen-komponen ini saling berhubungan, menciptakan integrasi antara berbagai elemen strategis untuk menciptakan sistem pertahanan siber yang kuat.

Di bagian bawah, terdapat dokumen yang menjadi landasan dan referensi dalam pengembangan model ini. Setiap dokumen terhubung dengan komponen-komponen utama, menunjukkan bahwa pengembangan model ini didasarkan pada data empiris, kajian literatur, serta wawasan dari para ahli di bidang keamanan siber, pertahanan, dan manajemen risiko. Misalnya, dokumen seperti PDF dan catatan dari individu tertentu memberikan kontribusi terhadap elemen-elemen seperti ancaman dan konsep faktor risiko.

Interkoneksi dalam gambar 3 menggambarkan sinergi antara berbagai elemen, baik dari aspek teknis seperti ancaman dan infrastruktur, maupun aspek kolaboratif seperti kerja sama dan pengembangan. Hal ini menunjukkan bahwa pengembangan strategi pertahanan siber tidak hanya berfokus pada elemen teknis, tetapi juga membutuhkan pendekatan multidisiplin yang melibatkan kebijakan, regulasi, teknologi, dan manusia.

Keseluruhan diagram ini menekankan pentingnya pendekatan holistik dalam strategi pertahanan siber. Dengan melibatkan berbagai komponen dan sumber data, model ini dapat menciptakan sistem pertahanan siber yang mampu menghadapi ancaman siber yang terus berkembang dan menjaga keandalan infrastruktur informasi vital nasional. Pendekatan berbasis data dan partisipasi aktif dari berbagai pihak menjadi kunci utama keberhasilan dalam pengembangan strategi ini.

Strategi Pertahanan Siber untuk Melindungi Infrastruktur Informasi Vital Nasional

Pengembangan model strategi pertahanan siber berbasis manajemen risiko menjadi penting dalam menjaga keamanan dan keandalan infrastruktur informasi vital nasional. Risiko dunia maya didefinisikan sebagai risiko operasional terhadap aset informasi dan teknologi yang dapat memengaruhi kerahasiaan, ketersediaan, dan/atau integritas informasi atau sistem informasi (Cebula et al., 2014). Peristiwa risiko siber yang sering terjadi meliputi pelanggaran data dan serangan siber (Agrafiotis et al., 2018).

Blakley (2002) menyatakan bahwa keamanan informasi sangat penting, terutama dengan meningkatnya ketergantungan pada teknologi informasi. Dalam konteks pertahanan siber, fokus utama adalah melindungi informasi vital yang erat kaitannya dengan pertahanan nasional. Oleh karena itu, peningkatan keamanan siber dan keberlanjutan operasional sistem-sistem ini menjadi prioritas utama dalam pengelolaan risiko dan pengembangan kebijakan keamanan informasi.

Investasi dalam teknologi keamanan, pengelolaan risiko, dan kebijakan yang komprehensif menjadi bagian integral dari perlindungan terhadap serangan siber. Hal ini bertujuan untuk menjaga keandalan infrastruktur informasi vital sektor pertahanan. Langkah-langkah ini diperlukan untuk memastikan ketersediaan dan kerahasiaan sistem yang digunakan dalam mendukung operasi pertahanan nasional.

Untuk mencegah memburuknya keamanan siber, pemerintah Indonesia telah mengeluarkan beberapa regulasi. Salah satunya adalah Peraturan Menteri Komunikasi dan Informatika No.26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. Peraturan ini kemudian direvisi melalui Peraturan Menteri Komunikasi dan Informatika No.16/PER/M.KOMINFO/10/2010 dan diperbarui dengan Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.KOMINFO/12/2010. Regulasi ini menjadi dasar dalam melaksanakan pengamanan siber nasional.

Dengan adanya regulasi tersebut, kesadaran akan pentingnya keamanan siber diharapkan meningkat. Organisasi di sektor pertahanan diyakini dapat mematuhi praktik-praktik keamanan yang baik. Regulasi ini juga mengatur prosedur penanganan insiden keamanan dan respons terhadap serangan siber, sehingga membantu meminimalkan dampak serangan dan mempercepat proses pemulihan (Iftikhar, 2024).

Model faktor risiko yang dikembangkan dalam penelitian ini melibatkan penilaian holistik terhadap berbagai ancaman siber, termasuk serangan siber yang kompleks dan kerentanannya. Faktor-faktor risiko ini dicirikan dan dikategorikan untuk memberikan pemahaman mendalam tentang kontribusi masing-masing faktor terhadap risiko keseluruhan.

KESIMPULAN

Penelitian ini menemukan bahwa pengembangan model strategi pertahanan siber berbasis manajemen risiko memiliki pendekatan yang lebih holistik dibandingkan penelitian sebelumnya. Temuan utama menunjukkan bahwa integrasi manajemen risiko dalam strategi pertahanan siber tidak hanya mencakup aspek teknis, seperti teknologi dan pengelolaan infrastruktur, tetapi juga melibatkan elemen perencanaan strategis, pengorganisasian, pelaksanaan, dan evaluasi secara menyeluruh. Model ini dirancang untuk memenuhi kebutuhan unik Indonesia dalam menghadapi ancaman siber, termasuk peran penting diplomasi siber dalam meningkatkan posisi geopolitik negara. Dengan menggunakan perangkat lunak NVivo untuk menganalisis data secara tematik dan triangulasi, penelitian ini menghasilkan pendekatan berbasis bukti yang belum banyak dibahas dalam literatur sebelumnya.

Penelitian ini memberikan kontribusi signifikan dalam bidang keamanan siber, terutama pada pengembangan konsep strategi berbasis manajemen risiko yang dapat diaplikasikan untuk sektor pertahanan nasional. Kontribusi utama adalah formulasi kerangka kerja yang terintegrasi untuk mengidentifikasi dan memitigasi risiko siber, yang dapat menjadi acuan dalam menyusun kebijakan nasional dan strategi keamanan siber. Selain itu, penelitian ini memperkaya teori tentang pentingnya kolaborasi lintas sektor dalam keamanan siber, yang mencakup kerja sama antara pemerintah, sektor swasta, dan komunitas teknologi. Dari sisi metodologi, penggunaan NVivo sebagai alat analisis memberikan pendekatan baru yang dapat diterapkan pada penelitian-penelitian terkait manajemen risiko di bidang lainnya.

Namun, penelitian ini memiliki keterbatasan yakni pada fokusnya yang masih bersifat teoretis dan berbasis kajian pustaka. Penelitian ini belum melakukan validasi empiris terhadap model yang diusulkan melalui studi lapangan atau eksperimen langsung. Selain itu, penggunaan data sekunder dari berbagai sumber dapat menghasilkan bias interpretasi. Untuk penelitian selanjutnya, disarankan untuk melakukan pengujian lapangan terhadap model yang dikembangkan, termasuk studi kasus pada sektor-sektor strategis,

seperti energi, telekomunikasi, dan keuangan. Penelitian lanjutan juga perlu mengeksplorasi penerapan teknologi mutakhir, seperti kecerdasan buatan dan *blockchain*, dalam mendukung strategi pertahanan siber berbasis manajemen risiko.

DAFTAR PUSTAKA

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), tyy006.

Al-Dosari, K., Fetais, N., & Kucukvar, M. (2024). Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. *Cybernetics and Systems*, *55*(2), 302–330.

Arianto, A. R., & Anggraini, dan G. (2019). Membangun Pertahanan Dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team On Internet Infrastructure (ID-SIRTII). *Jurnal Pertahanan & Bela Negara*, *9*(1), 13–30.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

Bahri, I. S. (2023). *Cyber Crime dalam Sorotan Hukum Pidana (Edisi 2023)*. Bahasa Rakyat.

Bardin, J. S. (2025). Cyber Warfare. In *Computer and Information Security Handbook* (pp. 1345–1380). Elsevier.

Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*, *54*(5), 3849–3886.

Bradshaw, T. K., & Blakely, E. J. (2002). *Planning Local Economic Development: Theory and Practice*. Sage Publications.

Broeders, D. (2021). Private active cyber defense and (international) cyber security—pushing the line? *Journal of Cybersecurity*, *7*(1), tyab010.

Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2022). Global cybersecurity index (GCI) and the role of its 5 pillars. *Social Indicators Research*, 1–19.

Cebula, J. J., Popeck, M. E., & Young, L. R. (2014). A taxonomy of operational cyber security risks version 2. *Software Engineering Institute, Carnegie Mellon Univ., Pittsburgh, PA, Tech. Rep. CMU/SEI-2014-TN-006*.

Cebula, J. J., & Young, L. R. (2010). A taxonomy of operational cyber security risks. *Software Engineering Institute, Carnegie Mellon University*.

CNN Indonesia. (2024a). SAFEnet: Serangan Siber Naik Dua Kali Lipat di Awal 2024. *CNN Indonesia*. https://www.cnnindonesia.com/teknologi/20240509092409-192-1095674/safenet-serangan-siber-naik-dua-kali-lipat-di-awal-2024

CNN Indonesia. (2024b). Serangan Siber Menggila, 411 Ribu Malware Baru Muncul Tiap Hari di RI. *CNN Indonesia*. https://www.cnnindonesia.com/teknologi/20240522130109-185-1100872/serangan-siber-menggila-411-ribu-malware-baru-muncul-tiap-hari-di-ri

Cui, L., Guo, L., Gao, L., Cai, B., Qu, Y., Zhou, Y., & Yu, S. (2021). A covert electricity-theft cyberattack against machine learning-based detection models. *IEEE Transactions on Industrial Informatics*, *18*(11), 7824–7833.

Davis, R. E. (2021). *Auditing Information and Cyber Security Governance: A Controls-based Approach*. CRC Press.

Ding, S., Gu, W., Lu, S., Yu, R., & Sheng, L. (2022). Cyber-attack against heating system in integrated energy systems: Model and propagation mechanism. *Applied Energy*, *311*, 118650.

Dirgantara, N. C., Maharani, Y., Nada, R. Q., & Hidayatullah, A. F. (2024). Ecological Justice for Timbulsloko: A Disaster Jurisprudence Approach. *TEMALI: Jurnal Pembangunan Sosial*, *7*(1), 57–64.

Gurtu, A., & Johny, J. (2021). Supply chain risk management: Literature review. *Risks*, *9*(1), 16.

Hunger, J. (2010). *Essentials of Strategic Management*. Pearson.

Husák, M., Bartoš, V., Sokol, P., & Gajdoš, A. (2021). Predictive methods in cyber defense: Current experience and research challenges. *Future Generation Computer Systems*, *115*, 517–530.

Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. *PeerJ Computer Science*, *10*, e1772.

Jacks, W., & Adler, J. (2015). A proposed typology of online hate crime. *Open Access Journal of Forensic Psychology*, *7*, 64–89.

Javier, F. (2024). Serangan Siber ke Pusat Data Nasional hingga Kebocoran Data Berbagai Lembaga, Bagaimana Kinerja Indonesia dalam Keamanan Siber? *Tempo.Co*. https://www.tempo.co/data/data/serangan-siber-ke-pusat-data-nasional-hingga-kebocoran-data-berbagai-lembaga-bagaimana-kinerja-indonesia-dalam-keamanan-siber--991201

Kalangi, D., & Tewu, M. L. (2022). Problem Loans in Banks and Implementation of Good Corporate Governance (GCG). *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, *5*(3), 24430–24443.

Kao, D.-Y., & Hsiao, S.-C. (2018). The dynamic analysis of WannaCry ransomware. *2018 20th International Conference on Advanced Communication Technology (ICACT)*, 159–166.

Kementerian Komunikasi dan Informatika RI. (2007). *Peraturan Menteri Komunikasi dan Informatika Nomor 26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet*. Kementerian Komunikasi dan Informatika RI.

Kementerian Komunikasi dan Informatika RI. (2010). *Peraturan Menteri Komunikasi dan Informatika Nomor 29/PER/M.KOMINFO/12/2010 tentang Perubahan Kedua atas Peraturan Menteri komunikasi dan Informatika Nomor: 26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol I*. Kementerian Komunikasi dan Informatika RI. https://jdih.kominfo.go.id/produk_hukum/view/id/271/t/peraturan+menteri+komunikasi+dan+informatika+nomor+29permkominfo122010+tanggal+30+desember+2010

Kementerian Pertahanan RI. (2019). Pusdatin Kemhan Harus Siap dan Mampu Tangkal Serangan Siber. *Kementerian Pertahanan RI*. https://www.kemhan.go.id/2019/05/17/pusdatin-kemhan-harus-siap-dan-mampu-tangkal-serangan-siber.html

Kementerian Pertahanan RI. (2024). *Pedoman Pertahanan Siber*. Kementerian Pertahanan RI.

Krisnata, R., Reksoprodjo, A. H. S., & Waluyo, S. D. (2020). Strategi Pengembangan Kapabilitas Siber Pertahanan Untuk Menghadapi Peperangan Siber (Studi Kasus Pada Pushansiber Kemhan Ri 2020-2021). *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *9*(6), 2094–2103. https://doi.org/10.31604/jips.v9i6.2022.2094-2103

Lee, S., & Kim, S. (2021). Blockchain as a cyber defense: opportunities, applications, and challenges. *Ieee Access*, *10*, 2602–2618.

Lehto, M. (2022). Cyber-attacks against critical infrastructure. In *Cyber security: Critical infrastructure protection* (pp. 3–42). Springer.

Lindsay, J. R. (2021). Cyber espionage. *The Oxford Handbook of Cyber Security*, 223.

Lune, H., & Berg, B. L. (2017). *Qualitative research methods for the social sciences*. Pearson.

Mahadwartha, P. A., & Ismiyanti, F. (2022). *Manajemen Risiko*.

Mahmudov, N. (2023). Cyber Warfare: understanding the elements, effects, and future trends of cyber-attacks and defences. *Сигурност и Отбрана*, *2*, 37–53.

Maxwell, J. A. (2008). Designing a qualitative study. *The SAGE Handbook of Applied Social Research Methods*, *2*, 214–253.

Miles, M. B., & Huberman, A. M. (2013). *Qualitative Data Analysis: An Expanded Sourcebook*. Sage Publications, Inc.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938–1940.

Novita, D., Mulyono, M., & Retnowati, A. (2024). Perkembangan Hukum Siber di Indonesia: Studi Literatur tentang Tantangan dan Solusi Keamanan Nasional. *Innovative: Journal Of Social Science Research*, *4*(6), 1179–1186.

Pushansiber Kemhan RI. (2022). *Serangan Siber Terhadap Kemhan RI Setiap Tahun*. Pushansiber Kemhan RI.

Rai, S., Singh, K., & Varma, A. K. (2019). Global Research Trend On Cyber Security: A Scientometric Analysis. *Library Philosophy And Practice (E-Journal)*, *3339*.

Rizki, M. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia Dalam Menghadapi Tantangan Perkembangan Teknologi Dan Informasi. *Politeia: Jurnal Ilmu Politik*, *14*(1), 54–62.

Robinson, S. (2021). *The Blind Strategist: John Boyd And The American Art Of War*. Exisle Publishing.

Sari, R. P. (2024). PDN diserang Hacker, Seberapa Lemah Keamanan Siber Indonesia? *Cloud Computing Indonesia*. https://www.cloudcomputing.id/berita/keamanan-siber-indonesia#google_vignette

Steingartner, W., & Galinec, D. (2021). Cyber threats and cyber deception in hybrid warfare. *Acta Polytechnica Hungarica*, *18*(3), 25–45.

Sun-Tzu. (2002). *Sun-Tzu Seni Perang* (R. A. B. Centre (ed.)). Lucky Publishers.

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: a survey and new perspectives. *IEEE Communications Surveys & Tutorials*, *25*(3), 1748–1774.

Yurekten, O., & Demirci, M. (2021). SDN-based cyber defense: A survey. *Future Generation Computer Systems*, *115*, 126–149.

Zhang, L., & Thing, V. L. L. (2021). Three decades of deception techniques in active cyber defense-retrospect and outlook. *Computers & Security*, *106*, 102288.