Strategi Pertahanan Siber dalam Melindungi Infrastruktur Kritis Nasional *(Analisa Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 Tentang Pertahanan Siber)*

Mochammad Yunianto[1], Lukman Yudho Prakoso[2], Yudha Rusniwan[3]
[1,2,3]Sekolah Staff dan Komando TNI, Indonesia
E-mail: moch.yunianto@gmail.com

Article Info
Article History
Received: 2024-09-07
Revised: 2024-10-27
Published: 2024-11-10

Keywords:
Strategy;
Defense;
Cyber;
Infrastructure;
Critical;
National.

Abstract
Along with the development of science and digitalization of information technology, the threat of cyber attacks will continue to increase and this threat is predicted to cause tension between countries that can threaten world peace. Cyber defense is very important to do because of the increasing number of strategic infrastructure and public services that depend on the digital world. So the method in writing this journal article uses a qualitative method with a descriptive analysis method, data sources obtained through regulatory analysis and library research from specific to general. In this study, the author has analyzed government regulations and official literature relevant to the research subject which is carried out by inventorying positive laws related to Indonesia's cyber defense strategy to protect national critical infrastructure. Given that the cyber defense strategy in protecting national critical infrastructure is very important to be carried out through policies or regulations, technology and human resources in accordance with the Regulation of the Minister of Defense Number 82 of 2014 concerning Cyber Defense.

Artikel Info
Sejarah Artikel
Diterima: 2024-09-07
Direvisi: 2024-10-27
Dipublikasi: 2024-11-10

Kata kunci:
Strategi;
Pertahanan;
Siber;
Infrastruktur;
Kritis;
Nasional.

Abstrak
Seiring berkembangnya ilmu pengetahuan dan digitalisasi teknologi informasi, ancaman serangan siber akan terus bertambah dan ancaman ini diramalkan dapat menimbukan ketegangan antar negara yang dapat mengancam perdamaian dunia. Adapun pertahanan siber sangat penting untuk dilakukan karena semakin banyaknya infrastruktur strategis dan layanan publik yang bergantung pada dunia digital. Sehingga metode dalam menulis artikel jurnal ini menggunakan metode kualitatif dengan jenis metode deskriptif analisis, sumber data yang didapat melalui analisa regulasi dan *library research* dari khusus ke umum. Dalam penelitian ini penulis telah menganalisa regulasi dari pemerintah dan literatur resmi yang relevan dengan subjek penelitian yang dilakukan dengan menginventarisasi hukum positif yang berkaitan dengan strategi pertahanan siber indonesia guna melindungi infrastruktur kritis nasional. Mengingat strategi pertahanan siber dalam melindungi infrastruktur kritis nasional sangat penting untuk dilakukan dengan melalui kebijakan atau regulasi, teknologi dan sumber daya manusia yang sesuai dengan Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pertahanan Siber.

I. PENDAHULUAN

Dunia global mempunyai peran penting dalam perkembangan ilmu pengetahuan sehingga digitalisasi teknologi informasi yang pesat telah membawa berbagai implikasi pada kehidupan antar negara (Arifina, 2022). Dalam Undang-Undang Nomor 3 Tahun 2002 mengenai Pertahanan Negara menyatakan bahwa ancaman di dalam sistem pertahanan negara terdiri dari ancaman militer dan ancaman non-militer, sehingga ancaman siber merupakan bagian dari ancaman tersebut. Ancaman perang siber menunjukkan prespektif bahwa dunia maya saat ini menjadi tempat baru untuk melakukan perang yang dapat menyebabkan konflik antara negara (Darumaya et al., 2023). Perang siber juga dapat mengguncang dunia global sehingga dipastikan menimbulkan ketegangan antar negara yang berdampak pada terancamnya keamanan nasional serta perdamaian dunia (Agung, 2021; Vimy et al, 2022). Resiko serangan siber akan terus meningkat seiring berkembang-nya teknologi informasi, sehingga angka serangan siber yang terjadi di Indonesia semakin tinggi, hal ini jelas menjadi ancaman yang sangat serius bagi pertahanan dan keamanan negara (Hasan, 2022). Dengan adanya berbagai kejadian tersebut maka diperlukan penelitian yang bersifat *continue* dalam mengatasi berbagai strategi, taktik dan teknik pertahanan siber.

Salah satu dampak negatif dari perkembangan siber adalah suatu kejahatan dalam bentuk pelanggaran hukum, jika eksalasinya semakin meningkat maka dapat mengancam kedaulatan

negara, keutuhan wilayah dan keselamatan bangsa. Mengingat jaringan komputer dalam perang siber digunakan untuk membangun strategis penyerangan pada sistem informasi yang dimiliki oleh musuh (Arifina, 2022). Sebagai upaya dalam menanggulangi masalah serangan di dunia maya, maka dibutuhkan sebuah lembaga yang berfungsi sebagai benteng pertahanan siber. Indonesia sendiri telah melakukan perang siber dengan negara lain sejak tahun 1998, seperti contoh kerusuhan rasial yang disebabkan oleh para *hacker* China dengan Taiwan, kerusuhan di dunia maya antara Indonesia dengan Portugal mengenai Timor-Timur dan perang siber antara Indonesia dengan Malaysia. Menurut Laporan *Wolrd Economic Forum* pada tahun 2014 menyatakan bahwa ancaman siber menjadi tantangan terbesar keempat di skala internasional setelah perubahan iklim, kondisi pengangguran dan kemiskinan (Agung, 2021).

Di Indonesia, pertahanan militer berbasis siber sangat penting untuk dilakukan, hal tersebut disebabkan oleh semakin banyaknya infrastruktur strategis dan layanan umum yang bergantung pada sistem informasi, teknologi dan jaringan internet. Akibatnya situasi seperti ini rentan terhadap gangguan, bahaya dan serangan yang dilakukan oleh berbagai pihak (Soewardi, 2013). Terlebih lagi ancaman serangan siber ini telah meningkat dengan cepat dan memengaruhi dinamika lingkungan strategis (Darumaya et al., 2023). Dalam konteks infrastruktur informasi kritis di Indonesia dapat berupa aset, sistem dan jaringan. Di mana infrastruktur ini akan menggabungkan jaringan internet dan telekomunikasi agar masyarakat Indonesia dapat menggunakannya. Sehingga aspek keamanan sangat penting pada infrastruktur informasi kritis, mengingat jika terjadi kendala pada infrastruktur kritis tersebut maka akan berpengaruh buruk pada strategi lainnya, seperti pertahanan dan keamanan, ekonomi, energi dan lainnya. Dengan demikian untuk meningkatkan efektivitas keandalan, ketersediaan dan integritas jaringan informasi baik di tataran nasional maupun internasional, aspek keamanan menjadi suatu hal yang mutlak untuk dilakukan (Siagian et al. 2018). Adapun Indonesia saat ini telah mengarahkan tujuannya ke arah pertempuran siber. Untuk menyikapi perang siber tersebut, maka Kementerian Pertahanan Republik Indonesia telah merumuskan regulasi dalam menghadapinya, yang disusun dalam konsep Sistem Pertahanan Siber seperti Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 mengenai Pertahanan Siber, karena permasalahan tersebut maka strategi pertahanan siber sangat penting untuk dilakukan dalam melindungi infrastruktur kritis nasional.

II. METODE PENELITIAN

Adapun metode dalam menulis artikel jurnal ini yaitu menggunakan metode kualitatif (Muhammad Rizal, 2021) dengan jenis metode deskriptif analisis, sumber data yang didapat melalui analisa regulasi dan *library research* dari khusus ke umum (Raco, 2010). Alasan dalam menggunakan metode kualitatif adalah metode kualitatif menggunakan cara berfikir induktif yang jauh lebih cepat dalam menemukan permasalahan data sehingga dari metode tersebut dapat menemukan keterhubungan dalam mempengaruhi data satu sama lain sehingga memberikan struktur analisis yang eksplisit (Muhammad Rizal, 2021). Adapun penelitian ini merupakan penelitian hukum normatif yang artinya penelitian yang dilakukan dan ditujukan pada peraturan perundang-undangan tertulis dan berbagai literatur yang berkaitan dengan permasalahan penelitian ini. Penelitian ini dilakukan dengan menginventarisasi hukum positif yang berkaitan dengan strategi pertahanan siber dalam melindungi infrastruktur kritis nasional (Analisa Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 Tentang Pertahanan Siber).

III. HASIL DAN PEMBAHASAN

Cyber war atau yang biasa dikenal dengan sebutan perang *siber* (Serangan Siber) adalah segala bentuk perbuatan, perkataan, pemikiran baik yang dilakukan dengan sengaja maupun tidak sengaja oleh pihak manapun, dengan motif dan tujuan apapun, yang dilakukan di lokasi mana pun, yang disasarkan pada sistem elektronik atau muatannya (informasi) maupun peralatan yang sangat bergantung pada teknologi dan jaringan dalam skala apapun terhadap obyek vital maupun non vital dalam lingkup militer dan nonmiliter, yang bertujuan untuk mengancam kedaulatan negara, keutuhan wilayah dan keselamatan bangsa. Adapun yang dimaksud dengan pertahanan siber (*siber defense*) adalah suatu upaya untuk menanggulangi serangan siber yang menyebabkan terjadinya gangguan terhadap penyelenggaraan pertahanan negara. Sedangkan yang dimaksud dengan infrastruktur kritis adalah aset, sistem, maupun jaringan, berbentuk fisik maupun virtual yang sangat vital, dimana gangguan terhadapnya berpotensi

mengancam keamanan, kestabilan perekonomian nasional, keselamatan dan kesehatan masyarakat atau gabungan diantaranya (Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber, 2014). Selain itu *cyber war* atau perang siber bisa diartikan sebagai bentuk konflik yang dilakukan dengan menggunakan teknologi informasi dan komunikasi untuk menyerang, merusak atau mengganggu sistem komputer dan jaringan. Hal ini merupakan bentuk pertarungan modern yang melibatkan aksi-aksi seperti peretasan, penyebaran malware dan serangan siber lainnya.

Tujuan dari adanya *cyber war* antara lain digunakan sebagai alat pengumpulan intelijen, dalam hal ini digunakan sebagai alat yang berfungsi untuk memperoleh data sensitif atau rahasia dari negara atau organisasi yang menjadi target. Selain itu *cyber war* juga bertujuan untuk merusak atau menghancurkan infrastruktur penting seperti sistem komunikasi, sistem energi, atau jaringan transportasi, mengganggu operasi bisnis atau pemerintah yang bertujuan untuk menciptakan ketidakstabilan atau kekacauan. Serta *cyber war* juga berfungsi sebagai media dalam menyebarkan informasi palsu atau propaganda untuk memanipulasi opini publik dan mempengaruhi hasil politik maupun sosial.

Bentuk-bentuk dari adanya ancaman dan serangan siber yaitu ancaman dan serangan tersebut dapat dilakukan oleh pelaku yang mewakili pemerintah (*State Actor*) atau non pemerintah (*Non State Actor*), sehingga pelaku bisa bersifat perorangan, kelompok, golongan, organisasi atau bahkan sebuah negara. Secara umum unsur-unsur yang dapat diidentifikasi memiliki potensi sebagai sumber ancaman terdiri atas sumber internal dan eksternal, kegiatan intelijen, kekecewaan, investigasi, organisasi ekstremis, grup kejahatan terorganisir, persaingan, permusuhan dan konflik serta teknologi. Bentuk ancaman siber yang sering terjadi saat ini menurut Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber dapat berupa:

1. *Serangan Advanced Persistent Threats* (APT), *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS), serangan yang dilakukan dengan melakukan *overloading* kapasitas sistem dan mencegah pengguna yang sah untuk mengakses dan menggunakan sistem atau sumber daya yang ditargetkan. Serangan ini bertujuan untuk mengganggu operasional sistem, dengan cara menghadapkan sistem pada permintaan akses dan proses yang jauh lebih besar dari yang bisa ditangani sistem. Sehingga sistem menjadi terlalu sibuk dan *crash*, akibatnya menjadi tidak dapat melayani atau tidak dapat beroperasi. Permasalahan ini merupakan ancaman yang berbahaya bagi organisasi yang mengandalkan hampir sepenuhnya pada kemampuan internet guna menjalankan roda kegiatannya.
2. Serangan *Defacement*, serangan yang dilakukan dengan cara melakukan penggantian atau modifikasi terhadap halaman web korban sehingga isi dari halaman web korban berubah sesuai dengan motif penyerang.
3. Serangan *Phishing*, serangan dilakukan dengan cara memberikan alamat website palsu dengan tampilan persis sama dengan website aslinya. Tujuan dari serangan *phishing* ini adalah untuk mendapatkan informasi penting dan sensitif seperti username, password dan lain-lain.
4. Serangan Malware, yaitu suatu program atau kode berbahaya yang dapat digunakan untuk mengganggu operasi normal dari sebuah sistem komputer. Biasanya program malware telah dirancang untuk mendapatkan keuntungan finansial atau keuntungan lain yang direncanakan. Adapun jumlah serangan malware terus berkembang, sehingga saat ini telah menjadi pandemi yang sangat nyata. Malware telah terjadi dimana-mana dan mempengaruhi semua orang yang terlibat dalam setiap sektor kegiatan.
5. Penyusupan siber, serangan yang dapat menyerang sistem melalui identifikasi pengguna yang sah dan parameter koneksi seperti password, melalui eksploitasi kerentanan yang ada pada sistem.

Dengan adanya tindakan *cyber war* tersebut maka menurut Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber terkait dengan strategi pertahanan siber untuk melindungi infrastruktur kritis nasional sangat urgen untuk dilaksanakan melalui:

1. Pembuatan Kebijakan atau Regulasi

   Urgensinya dalam pembuatan kebijakan atau regulasi dalam menangani kejahatan siber sangat penting karena sangat berkaitan dengan perlindungan keamanan, penegakan hukum dan stabilitas sosial. Mengingat regulasi dapat membantu melindungi data pribadi individu dari pencurian, penyalahgunaan dan pelanggaran privasi. Dengan

adanya aturan yang ketat, organisasi harus mematuhi standar keamanan untuk dapat melindungi data pengguna. Regulasi juga menetapkan standar untuk melindungi informasi sensitif, seperti data keuangan, medis dan intelijen yang dapat digunakan oleh penjahat siber untuk melakukan tindakan merugikan. Selain itu pembuatan regulasi dimaksudkan untuk menyediakan kerangka hukum yang jelas dalam mendefinisikan kejahatan siber, proses penegakan hukum dan hukuman yang sesuai bagi pelaku, hal ini tentunya dapat mempermudah pihak berwenang untuk menangani kasus-kasus siber secara efektif. Pembuatan kebijakan khususnya regulasi seringkali mencakup kerjasama internasional yang diperlukan untuk menangani kejahatan siber yang melibatkan pelaku lintas batas yang tentunya hal tersebut dapat membantu mengkoordinir tindakan hukum diberbagai Negara.

Adapaun pembuatan regulasi harus menerapkan standar keamanan yang harus dipatuhi oleh semua anggota didalamnya, hal ini bertujuan untuk membantu mencegah kejahatan siber dengan memastikan bahwa mereka menggunakan Langkah-langkah perlindungan yang memadai. Selain itu adanya kebijakan yang dibuat oleh pemerintah juga dapat membantu organisasi dalam meng-identifikasi dan mengelola risiko siber dengan menetapkan prosedur dan kebijakan yang harus diikuti untuk mengurangi kemungkinan serangan dan kerusakan. Pembuatan kebijakan dan regulasi meliputi pembuatan panduan tentang bagaimana menangani insiden siber, termasuk pelaporan dan mitigasi, sehingga organisasi dapat merespons dengan cepat dan efektif.

Mengingat bahwa kejahatan siber dapat menyebabkan kerugian ekonomi yang signifikan bagi perusahaan dan individu. Maka kebijakan yang dibuat oleh pemerintah dapat membantu mengurangi dampak kerugian dengan menetapkan Langkah-langkah pen-cegahan dan respons yang efektif. Sehingga dengan adanya regulasi, publik merasa lebih aman dalam menggunakan layanan digital dan berinteraksi secara online. Dengan kerangka hukum yang jelas pada pembuatan kebijakan maupun regulasi, maka pencegahan dalam dunia siber (*cyber war*) akan dapat direspons dengan cepat guna menjaga keamanan dan stabilitas di dunia digital.

2. Teknologi

Secara keseluruhan pada bidang teknologi, teknologi memberikan alat dan metodologi yang diperlukan untuk mengidentifikasi, mencegah dan menangani kejahatan siber secara efektif. Tanpa teknologi, akan sangat sulit untuk melindungi sistem informasi dari ancaman yang semakin canggih dan beragam di era digital saat ini. Teknologi memainkan peran yang sangat penting dalam menangani kejahatan siber, hal ini seperti contoh teknologi dapat memungkinkan pemantauan jaringan dan sistem secara real – time. Alat seperti sistem deteksi intrusi (IDS) dan sistem pencegahan intrusi (IPS) dapat mengidentifi-kasi dan merespons ancaman dengan cepat. Dengan bantuan teknologi analitik, data besar yang dihasilkan dari aktivitas jaringan dapat dianalisis untuk mendeteksi pola atau anomali yang mungkin menunjukkan serangan siber. Sementara itu teknologi *firewall* dan perang-kat lunak antivirus membantu melindungi sistem dari serangan dengan memblokir akses yang tidak sah dan mendeteksi serta menghapus malware. Selain itu teknologi berupa enkripsi digunakan untuk melindungi data yang sedang dikirim atau disimpan dari akses yang tidak sah, memastikan bahwa informasi sensitif tetap aman.

Dengan adanya teknologi juga memungkinkan automasi dalam merespons insiden siber, seperti memutuskan sambungan dari jaringan untuk mencegah penyebaran malware atau melakukan pemulihan data otomatis. Dengan adanya teknologi *threat intelligence* membantu dalam mengumpulkan dan menganalisis informasi tentang ancaman siber yang ada di luar organisasi. Mengingat teknologi menyediakan platform untuk manajemen insiden yang memungkinkan tim keamanan siber berkoordinasi secara efektif dan menangani insiden dengan cara yang terstruktur, maka dengan adanya teknologi juga memungkinkan pertukaran informasi dan kolaborasi antara negara, organisasi dan lembaga penegak hukum dalam menghadapi ancaman siber yang bersifat lintas batas.

3. Sumber Daya Manusia

Sumber Daya Manusia (SDM) sangat penting dalam menangani kejahatan siber karena beberapa alasan. Meskipun teknologi memainkan peran besar dalam perlindungan dan respons terhadap ancaman siber, keahlian dan keterampilan manusia tetap esensial

untuk memastikan efektivitas dan keberhasilan strategi keamanan siber. SDM yang terlatih dapat melakukan analisis mendalam tentang risiko dan ancaman siber. Mereka dapat mengidentifikasi potensi celah keamanan yang mungkin tidak terdeteksi oleh sistem otomatis, mengingat bahwa keahlian manusia diperlukan untuk menilai efektivitas kontrol keamanan dan untuk membuat penyesuaian jika diperlukan. Berdasarkan hasil evaluasi dan pengalaman praktis, SDM yang berpengalaman dapat mengembangkan kebijakan dan prosedur keamanan siber yang sesuai dengan kebutuhan organisasi dan regulasi yang berlaku, seperti contoh dalam menerapkan dan menegakkan kebijakan keamanan memerlukan keterampilan manajerial dan teknis untuk memastikan semua langkah diikuti dan dipatuhi oleh semua anggota organisasi. Ketika terjadi serangan siber, tim keamanan siber yang terlatih diperlukan untuk merespons insiden secara efektif, termasuk mengidentifikasi, mengisolasi dan memitigasi ancaman. Selain itu SDM dengan keahlian forensik digital dapat melakukan investigasi untuk memahami bagaimana serangan terjadi, mengidentifikasi pelaku dan mencegah serangan di masa depan.

TNI mempunyai kewajiban dalam tugasnya untuk menerapkan arsitektur pengamanan informasi tingkat tinggi terhadap segala sesuatu hal yang berkaitan dengan pertahanan negara khususnya di bidang siber. Hal ini tentunya TNI dapat membuat, mengimplementasikan dan mengoperasikan secara efektif arsitektur yang mencakup seluruh tahap siklus pertahanan siber agar mampu mengatasi ancaman terhadap faktor orang, logikal dan teknologi dari penyerang yang memiliki sumber daya yang besar dan akses yang luas dari berbagai aspek antara lain keuangan, teknologi intelijen dan politik.

Personel TNI yang berintegritas tinggi dan profesional dalam membangun dan mengimplementasikan pengamanan informasi serta mengoperasikannya secara efektif, dapat melakukan pengawasan yang aman melalui pengawasan logikal dan fisik yang berintegritas tinggi serta mampu mendeteksi setiap proses yang tidak terotorisasi. Selain itu dalam kegiatan penyelenggaraan siber, TNI juga harus mampu menganalisa kelemahan dari lawan, menganalisa manajemen pengamanan dalam menjaga kerahasiaan informasi, melakukan pengalihan serangan agar sistem utama terhindar dari ancaman dan dapat mempelajari teknik serangan yang dilakukan serta memberikan peringatan *real time* berlapis agar dapat menjamin ketersediaan, kerahasiaan dan integritas dari peringatan yang diberikan. Dengan adanya Menganalisa serangan dengan dukungan implementasi yang efektif dari arsitektur pengamanan tingkat tinggi yang telah ditetapkan, maka serangan balik merupakan suatu pilihan yang harus dipertimbangkan secara matang baik dari sisi hukum dan diplomasi, mengingat hal tersebut merupakan salah satu strategi pertahanan siber dalam melindungi infrastruktur kritis nasional.

IV. SIMPULAN DAN SARAN

A. Simpulan

Berdasarkan dari pembahasan yang telah diuraikan pada penelitian ini, dapat disimpulkan bahwa upaya yang dilakukan oleh pemerintah Indonesia dalam menanggulangi ancaman siber telah disusun dalam konsep strategi pertahanan siber yang tercantum pada Peraturan Menteri Nomor 82 Tahun 2014 mengenai pedoman pertahanan siber, hal ini dikarenakan Peraturan menteri tersebut dapat dijadikan sebagai acuan untuk melindungi infrastruktur kritis nasional. Adapun Tentara Nasional Indonesia juga mempunyai tanggung jawab dalam menjaga keamanan nasional di bidang siber. Ancaman siber menjadi tantangan terbesar bagi keamanan nasional di era digital saat ini. Untuk melakukan pertahanan siber yang efektif, kebijakan atau regulasi harus disusun, infrastruktur teknologi harus diperkuat dan pengembangan sumber daya manusia (SDM) juga harus handal dalam berkemampuan di bidang siber, serta kolaborasi atau kerja sama antara lembaga pemerintahan maupun non pemerintahan harus dibangun. Kesadaran dan kesiapan siber di pemerintahan dan seluruh komponen masyarakat harus ditingkatkan. Sehingga, strategi pertahanan siber yang komprehensif ini dapat melindungi infrastruktur nasional dan menjamin keamanan nasional.

B. Saran

Pembahasan terkait penelitian ini masih sangat terbatas dan membutuhkan banyak masukan, saran untuk penulis selanjutnya adalah mengkaji lebih dalam dan secara komprehensif tentang Strategi Pertahanan Siber dalam Melindungi Infrastruktur Kritis Nasional.

DAFTAR RUJUKAN

Agung, M. R. (2021). Faktor Penyebab Pengembangan Siber di Indonesia pada Era Pemerintahan Jokowi Tahap I. Jurnal Noken: Ilmu-Ilmu Sosial, 6(2), 91-103.

Ardiyanti, H. (2014). Siber Security dan Tantangan Pengembangannya di Indonesia. Politica, 5(1).

Arifina, N. (2022). Pertahanan Siber Indonesia di Kementerian Pertahanan Republik Indonesia. Jurnal Peperangan Asimetris, 8(1), 22-33.

Arifina, N., Sidik, F., & Sutanto, R. (2022). Strategi Pertahanan Siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia. Nusantara: Jurnal Ilmu Pengetahuan Sosial, 9(6), 2218-2227.

Chotimah, H. C. (2015). Membangun Pertahanan dan Keamanan Nasional dari Ancaman Siber di Indonesia. Jurnal Diplomasi, 7(4), 103-123.

Darumaya, B. A., Maarif, S., Touran, T., & Swastanto, Y. (2023). Pemikiran Potensial Ancaman Perang Siber di Indonesia: Suatu Kajian Strategi Pertahanan. Jurnal Keamanan Nasional, Vol. IX, No. 2, pp. 299-324.

Hasan, K. E. S., (2022). Perlunya Tentara Nasional Indonesia Memiliki Angkatan Siber Guna Menghadapi Era Siber Warfare. Journal of Education, Humaniora and Social Sciences (JEHSS), 5(1), 264-274.

Lebo, D., & Anwar, S. (2020). Pemberdayaan Komunitas Siber Oleh Pemerintah Republik Indonesia Dari Perspektif Strategi Perang Semesta. Jurnal Strategi Pertahanan Semesta, 6(1), 101-127.

Mahendra, Y. C., & Pinatih, N. K. D. S. A. P. (2023). Strategi Penanganan Keamanan Siber (Siber Security) di Indonesia. Jurnal Review Pendidikan dan Pengajaran (JRPP), 6(4), 1941-1949.

Peraturan Menteri Pertahanan Nomor 57 Tahun 2014 tentang Pedoman Strategis Pertahanan Nirmiliter.

Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber

Permanasari, A. (2018). Terorisme Siber, Perang Siber & Hukum Humaniter: Tantangan Bagi Kerangka Hukum Indonesia Tentang Pertahanan Siber. Hukum Pidana dan Pembangunan Hukum, 1(1).

Siagian, L., Budiarto, A., & Simatupang. (2018). Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. Jurnal Prodi Perang Asimetris, 4(3).

Soewardi, B. A. (2013). Perlunya Pembangunan Sistem Pertahanan Siber (Siber Defense) yang Tangguh Bagi Indonesia. Media Informasi Ditjen Pothan Menhan, pp. 31-35.

Syafi'i, M. H., Supriyadi, A. A., Prihanto, Y. & Gultom, R. A. G. (2023). Kajian Ilmu Pertahanan dalam Strategi Pertahanan Negara Guna Menghadapi Ancaman Teknologi Digital di Indonesia. Journal on Education, 5(2), 4063-4076.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, pasal 30 ayat 1, 2, dan 5 tentang Pertahanan dan Keamanan Negara.

Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.

Undang-Undang Nomor 25 Tahun 2009 Tentang Pelayanan Publik.

Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara.

Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia.

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Undang-Undang RI Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Vimy, T., Wiranto, S., Rudiyanto, Widodo, P., & Suwarno, P. (2022). Ancaman Serangan Siber Pada Keamanan Nasional Indonesia. Jurnal Kewarganegaraan, 6(1), 2319-2327.