Jurnal Review Pendidikan dan Pengajaran
http://journal.universitaspahlawan.ac.id/index.php/jrpp
Volume 8 Nomor 1, 2025
P-2655-710X e-ISSN 2655-6022

Submitted : 27/02/2025
Reviewed : 02/03/2025
Accepted : 02/03/2025
Published : 08/03/2025

Ria Wulandari[1]
Priyanto Suharto[2]
Afrizal Hendra[3]

STRATEGI KEMENTERIAN PERTAHANAN DALAM PENGAMANAN SISTEM INFORMASI BERBASIS SATELIT GUNA MENGHADAPI CYBERTHREAT

Abstrak
Ancaman siber (cyberthreat) semakin kompleks. Penggunaan teknologi satelit dalam sistem informasi pertahanan memiliki peran yang sangat strategis. Penelitian ini bertujuan untuk menganalisis strategi yang diterapkan oleh Kementerian Pertahanan dalam menghadapi ancaman siber terhadap sistem informasi satelit. Metode yang digunakan dalam penelitian ini adalah deskriptif kualitatif dengan pendekatan studi pustaka. Data dikumpulkan melalui kajian literatur dari berbagai sumber terkait kebijakan pengamanan siber, teknologi enkripsi, serta langkah-langkah mitigasi yang diambil oleh Kementerian Pertahanan. Berdasarkan temuan penelitian, disarankan agar Kementerian Pertahanan terus memperkuat kerangka kerja keamanan siber yang komprehensif, termasuk pengembangan kebijakan yang adaptif, investasi dalam teknologi keamanan terbaru, serta peningkatan kapasitas sumber daya manusia. Selain itu, penting untuk membangun ekosistem keamanan siber nasional yang melibatkan seluruh pemangku kepentingan, baik pemerintah, swasta, maupun akademisi. Dengan demikian, Indonesia dapat lebih siap menghadapi ancaman siber yang semakin canggih dan melindungi kepentingan nasional di era digital.
Kata Kunci: Cyberthreat; Kementerian Pertahanan Republik Indonesia, Satelit, Strategi Pertahanan

Abstract
Cyberthreats are increasingly complex. The use of satellite technology in defense information systems has a very strategic role. This research aims to analyze the strategies implemented by the Ministry of Defense in dealing with cyber threats to satellite information systems. The method used in this research is descriptive qualitative with a literature study approach. Data was collected through literature review from various sources related to cybersecurity policies, encryption technology, and mitigation measures taken by the Ministry of Defense. Based on the research findings, it is recommended that the Ministry of Defense continue to strengthen a comprehensive cybersecurity framework, including the development of adaptive policies, investment in the latest security technologies, and human resource capacity building. In addition, it is important to build a national cybersecurity ecosystem that involves all stakeholders, including the government, private sector and academia. Thus, Indonesia can be better prepared to face increasingly sophisticated cyberthreats and protect national interests in the digital era.
Keywords: Cyberthreat; Republic Indonesia Defense Ministry, Satellite, Defense Strategy

PENDAHULUAN

Pada tanggal 1 November 2023, situs website Kemhan RI diretas oleh hacker, yang mengindikasikan adanya ancaman serius terhadap keamanan siber di Indonesia (BSSN, 2023). Hacker tersebut menggunakan perangkat malware, lebih spesifiknya adalah jenis malware stealer, yang berhasil mengakses dan mencuri data-data penting (Kompas.com, 2023). Data pribadi pegawai di Kemhan RI, termasuk informasi sensitif lainnya, bocor akibat peretasan ini

[1,2,3] Universitas Pertahanan
Email: riawulandhari@gmail.com, priyantosuharto@gmail.com, ijal_91@yahoo.com

(Kompas.com, 2023). Selain itu, hacker juga mengunggah data curian tersebut ke situs BreachForums, yang memperburuk situasi karena data yang dicuri bisa disalahgunakan oleh pihak yang tidak bertanggung jawab (Kompas.com, 2023). Hal ini menambah risiko kejahatan siber yang lebih besar, mulai dari pemerasan hingga potensi ancaman terhadap kedaulatan negara (Akram, 2023). Ancaman yang ditimbulkan oleh kebocoran data ini dapat dimanfaatkan untuk melakukan manipulasi publik, spionase, serta disinformation, yang semakin merusak kepercayaan terhadap sistem pertahanan Indonesia (Buku Putih, 2015).

Pada era digital saat ini, teknologi berbasis satelit telah menjadi elemen penting dalam mendukung berbagai aspek pertahanan negara. Sistem informasi berbasis satelit digunakan untuk komunikasi militer, pengintaian, navigasi, hingga pemantauan pergerakan pasukan dan aset strategis. Menurut Wakil Menteri Pertahanan Tahun 2021 M. Herindra, peran penting satelit bukan hanya untuk komunikasi, tetapi sangat vital penggunaannya dalam sistem pertahanan untuk mengintegrasikan fungsi pertahanan negara (Kemhan, 2021). Seiring dengan meningkatnya ketergantungan pada teknologi ini, ancaman siber (cyberthreat) terhadap infrastruktur satelit juga semakin kompleks dan berbahaya. Serangan siber dapat menyebabkan gangguan serius pada sistem komunikasi dan pencurian data rahasia, bahkan mengancam keselamatan nasional melalui sabotase teknologi satelit. Kementerian Pertahanan dihadapkan pada tantangan besar untuk melindungi sistem informasi berbasis satelit dari berbagai jenis ancaman siber, termasuk peretasan, malware, dan serangan denial of service (DoS). Pengamanan yang efektif memerlukan pendekatan yang mencakup aspek teknologi, kebijakan, serta pengembangan sumber daya manusia.

Sistem informasi berbasis satelit menjadi salah satu prioritas utama Kementerian Pertahanan. Penyusunan strategi yang efektif untuk melindungi infrastruktur vital ini memerlukan pemahaman yang mendalam tentang ancaman yang ada, kekuatan dan kelemahan yang dimiliki oleh sistem, serta peluang dan tantangan yang mungkin muncul. Oleh karena itu, pendekatan yang komprehensif dan sistematis ini menggunakan analisis SWOT (Strengths, Weaknesses, Opportunities, Threats) yang dapat membantu Kementerian Pertahanan merumuskan strategi yang lebih matang dalam menghadapi ancaman siber. Selain itu, ancaman yang bersifat lintas batas ini menuntut kolaborasi dengan berbagai pihak, baik di tingkat nasional maupun internasional, guna memastikan keamanan yang berkelanjutan. Tulisan ini bertujuan untuk membahas strategi-strategi utama yang dapat diambil oleh Kementerian Pertahanan dalam melindungi sistem informasi berbasis satelit guna menghadapi ancaman siber. Fokus utama adalah penguatan infrastruktur keamanan, pengembangan kemampuan deteksi dan respons, kolaborasi antar lembaga, peningkatan kualitas sumber daya manusia, serta pemanfaatan teknologi mutakhir seperti kecerdasan buatan dan big data. Strategi-strategi ini diharapkan dapat meningkatkan ketahanan nasional dalam menghadapi serangan siber yang semakin canggih. Untuk merumuskan strategi yang tepat dalam pengamanan sistem informasi berbasis satelit, terdapat beberapa pertanyaan mendasar yang perlu dijawab seperti bagaimana strategi Kementerian Pertahanan dalam melindungi sistem informasi berbasis satelit dari ancaman siber?

METODE

Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan studi pustaka yang komprehensif. Analisis teks dilakukan terhadap berbagai sumber utama, termasuk buku, artikel ilmiah, jurnal akademik, serta laporan dari media massa. Periode kajian penelitian mencakup tahun 2022 hingga 2024, dengan fokus utama pada pemahaman proses, makna, dan konteks terkait ancaman siber serta strategi pertahanan yang diterapkan oleh Indonesia. Data dalam penelitian ini dikumpulkan melalui kajian literatur dari berbagai sumber kredibel yang membahas aspek kebijakan pengamanan siber, teknologi enkripsi, serta langkah-langkah mitigasi yang diterapkan oleh Kementerian Pertahanan. Selain itu, penelitian ini juga menelaah regulasi yang mengatur keamanan siber di Indonesia serta studi kasus terkait insiden serangan siber yang pernah terjadi. Pendekatan ini memungkinkan analisis mendalam terhadap efektivitas strategi yang telah diterapkan, sekaligus mengidentifikasi tantangan serta peluang dalam penguatan sistem keamanan siber nasional.

Selain itu, penulis juga menggunakan teori masa depan perang total oleh Priyanto. Dunia maya dan ruang angkasa sebagai arena konflik baru (Priyanto, 2024c). Dunia maya dan ruang angkasa menjadi arena yang sangat penting untuk kompetisi dan konflik internasional. Serangan

siber dapat merusak keamanan nasional tanpa perang fisik, dan militerisasi ruang angkasa dapat menyebabkan perlombaan ruang angkasa baru di antara kekuatan-kekuatan global (Priyanto, 2024a). Operasi siber dan penggunaan senjata tanpa awak akan menjadi sangat penting dalam mencegah eskalasi dan melindungi penduduk sipil. Pengembangan perjanjian dan norma baru untuk mengatur teknologi ini diperlukan untuk mengurangi risiko konflik yang tidak terkendali (Priyanto, 2024b)

HASIL DAN PEMBAHASAN

Situs Kementerian Pertahanan Indonesia pernah mengalami serangan siber. Salah satu insiden terjadi pada 2020, di mana hacker berhasil menembus sistem informasi Kementerian Pertahanan. Serangan ini menunjukkan adanya kerentanan dalam sistem pengamanan siber yang dimiliki oleh institusi vital seperti Kemenhan. Upaya peretasan tersebut menjadi sorotan karena mengancam keamanan informasi negara, terutama yang berkaitan dengan pertahanan nasional (Saptohutomo, 2023). Satelit memainkan peran yang sangat penting dalam keamanan siber, terutama dalam mendukung infrastruktur kritis dan komunikasi militer. Satelit bukan hanya untuk komunikasi, tetapi sangat vital penggunaaannya dalam sistem pertahanan untuk mengintegrasikan fungsi pertahanan negara. Pemanfaatan Satelit untuk mendukung pertahanan negara, diharapkan dapat membawa dampak positif bagi peningkatan kinerja Kemhan dan TNI di bidang pertahanan khususnya serta kemajuan bangsa dan negara pada umumnya (Kemhan RI, 2021). Teknologi satelit memungkinkan komunikasi yang aman dan andal di tingkat global, membantu koordinasi dan pemantauan sistem pertahanan negara. Namun, satelit juga menjadi target utama ancaman siber, seperti peretasan dan gangguan sinyal, yang dapat mempengaruhi stabilitas sistem komunikasi, pengintaian, dan navigasi. Keamanan satelit sangat bergantung pada perlindungan terhadap serangan yang bisa merusak data sensitif atau mengganggu operasi penting, sehingga pengamanan sistem satelit harus sejalan dengan perkembangan teknologi keamanan siber yang terus berkembang. Banyak sistem infrastruktur kritis seperti jaringan listrik, komunikasi, dan keuangan bergantung pada satelit untuk beroperasi, (Manulis, 2021). Jika satelit ini diretas atau dihambat, dapat menyebabkan gangguan besar pada layanan-layanan penting ini, bahkan menyebabkan kelumpuhan nasional.

Kementerian Pertahanan Republik Indonesia telah mengakui pentingnya infrastruktur teknologi berbasis satelit dalam mendeteksi dan merespons ancaman siber. Penggunaan sistem pertahanan siber yang canggih memungkinkan deteksi dini terhadap potensi serangan yang dapat merusak infrastruktur kritis dan data negara. Satelit menyediakan konektivitas ke daerah-daerah terpencil yang sulit dijangkau oleh infrastruktur darat. Ini membuat mereka menjadi target menarik bagi para pelaku kejahatan siber yang ingin mengakses sistem yang kurang terlindungi. Satelit juga digunakan untuk mengumpulkan berbagai jenis data, termasuk data intelijen. Data ini dapat digunakan untuk melacak aktivitas musuh, mengidentifikasi ancaman potensial, dan memantau infrastruktur kritis. Namun, data yang sensitif ini juga menjadi target utama bagi para hacker. Pemerintah dan militer menggunakan satelit untuk berkomunikasi secara aman. Jika komunikasi satelit ini diretas, dapat membahayakan operasi militer dan keamanan nasional. Sistem navigasi global seperti GPS bergantung pada jaringan satelit. Jika sistem ini diretas atau dihambat, dapat menyebabkan gangguan pada transportasi, logistik, dan layanan darurat.

Dalam rangka penyelenggaraan pertahanan siber, Kementerian Pertahanan berpedoman pada Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber. Demi melindungi infrastruktur kritis seperti sistem informasi berbasis satelit, dibutuhkan regulasi yang jelas dan efektif terkait keamanan siber. Penyusunan regulasi ini merupakan ranah yang sangat strategis bagi Kementerian Pertahanan, mengingat ancaman siber yang semakin kompleks dan berpotensi merusak ketahanan negara. Regulasi tersebut perlu mencakup pengaturan teknis, operasional, serta kerangka hukum yang memungkinkan respons cepat terhadap ancaman, sambil memastikan perlindungan terhadap data sensitif dan keberlanjutan operasi pertahanan.

Selain itu, regulasi ini harus mampu mengakomodasi perkembangan teknologi yang pesat dan memperhitungkan kerentanan sistem siber yang terus berkembang. Kementerian Pertahanan, sebagai lembaga yang memiliki tanggung jawab terhadap keamanan nasional, perlu bekerja sama dengan sektor terkait, termasuk lembaga-lembaga pemerintah lainnya dan mitra internasional, untuk memastikan bahwa regulasi yang disusun dapat memberikan perlindungan

maksimal terhadap ancaman siber. Hal ini mencakup juga pengaturan tentang standar keamanan siber, prosedur respons insiden, serta pembentukan kapasitas sumber daya manusia yang terampil dalam menghadapi tantangan dunia maya. Dengan demikian, regulasi yang kuat dan adaptif sangat diperlukan untuk memastikan keberlanjutan dan keandalan sistem pertahanan yang berbasis teknologi satelit.

Undang-Undang RI Nomor 3 Tahun 2002 tentang Pertahanan Negara menyebutkan bahwa pertahanan negara bertujuan untuk menjaga dan melindungi kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia (NKRI) dan keselamatan segenap bangsa dari segala bentuk ancaman, baik ancaman militer maupun non-militer. Ancaman non- militer khususnya di ruang siber telah menyebabkan kemampuan negara dalam bidang soft dan smart power pertahanan harus ditingkatkan melalui strategi penangkalan, penindakan dan pemulihan pertahanan siber (cyber defense) dalam rangka mendukung penerapan strategi nasional keamanan siber yang dimotori oleh Kementerian Komunikasi dan Digital.

Kementerian Komunikasi dan Digital, selaku leading sektor Pemerintah Republik Indonesia dalam bidang Telekomunikasi dan Informatika seharusnya menerapkan agenda kebijakan keamanan siber dalam membangun Secure Cyber Environment yang telah ada di Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber. Adapun yang harus diimplementasikan adalah strategi kebijakan Capacity Building, Policy and Legal Framework, Organizational Structure, Technical and Operational Measures, dan International Cooperation. Selanjutnya peran Kementerian Komunikasi dan Digital sebagai pengelola keamanan siber nasional dan kebijakan yang diterapkan dalam peran tersebut akan menjadi acuan utama bagi perumusan pedoman pertahanan siber ini. Berikut ini hasil analisis SWOT yang dapat diterapkan pada pengamanan sistem informasi berbasis satelit:

Tabel 1. SWOT Analisis: Pengamanan Sistem Informasi Berbasis Satelit

Faktor	Penjelasan
Strengths (Kekuatan)	**Infrastruktur Teknologi yang Maju**: Satelit dan sistem komunikasi yang digunakan sangat canggih dan memiliki kemampuan pertahanan yang tinggi. **Sumber Daya Manusia Terlatih**: Adanya tim teknis yang kompeten dan terlatih dalam menghadapi ancaman siber. Mereka yang direkrut adalah seorang profesional Cybersecurity Engineers yang memiliki certified Information System Security Professional (CISSP), CompTIA Security+, dan Certified Ethical Hacker (CEH). **Kerjasama Internasional**: Kerjasama dengan negara dan lembaga internasional dalam hal pertahanan siber dan berbagi teknologi.
Weaknesses (Kelemahan)	**Ketergantungan yang Tinggi pada Satelit**: Ketergantungan pada sistem satelit yang menjadi titik rawan dan berpotensi diserang. **Keterbatasan Infrastruktur Keamanan**: Kurangnya pengamanan yang cukup terhadap infrastruktur satelit, seperti kurangnya deteksi serangan dan mitigasi risiko. **Kesenjangan dalam Keterampilan Siber**: Tidak semua bagian atau instansi memiliki pemahaman yang cukup tentang ancaman siber, dan masih ada celah dalam pelatihan keamanan di level yang lebih luas.
Opportunities (Peluang)	**Perkembangan Teknologi Keamanan Siber**: Adanya peluang untuk memanfaatkan teknologi keamanan siber terbaru yang lebih canggih untuk melindungi sistem satelit. **Kolaborasi Global**: Meningkatnya kolaborasi global dalam menghadapi ancaman siber yang memungkinkan berbagi informasi dan teknologi keamanan yang lebih baik. **Inovasi dalam Keamanan Satelit**: Peluang untuk mengembangkan solusi baru dalam mengamankan satelit, seperti penggunaan kriptografi dan teknologi blockchain untuk autentikasi dan enkripsi data.
Threats (Ancaman)	**Serangan Siber yang Semakin Canggih**: Serangan siber yang lebih kompleks seperti peretasan, malware, dan serangan denial-of-service (DoS) yang bisa merusak sistem komunikasi satelit. **Ancaman dari Negara dan Aktor Non-Negara**: Serangan dari negara asing atau kelompok non-negara yang memiliki kemampuan canggih untuk meretas atau mengganggu satelit. **Serangan terhadap Rantai Pasokan Satelit**: Ancaman terhadap pemasok dan kontraktor yang bekerja dalam pembangunan dan pemeliharaan satelit, yang dapat menjadi titik lemah

Faktor	Penjelasan
	dalam sistem.

SIMPULAN

Berdasarkan hasil analisis SWOT di atas menunjukkan bahwa Kementerian Pertahanan memiliki potensi yang besar untuk mengamankan sistem informasi berbasis satelit. Namun, tantangan yang dihadapi juga sangat kompleks. Dengan menerapkan strategi yang tepat, Kementerian Pertahanan dapat meningkatkan kemampuannya dalam menghadapi ancaman siber dan melindungi aset-aset strategis negara. Maka, strategi yang perlu di terapkan adalah pelunya peningkatan kesadaran keamanan siber secara berkala, memperkuat sistem pertahanan siber dengan menggunakan teknologi terbaru dan melakukan pemutakhiran secara berkala, melakukan kerjasama dengan negara-negara lain dalam berbagi informasi intelijen, serta menyiapkan rencana respons insiden untuk mengatasi serangan siber yang terjadi.

DAFTAR PUSTAKA

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. SAGE Publications.

Tamsir, N., Aini, N., Asri, R., Moedjahedy, J. H., Muhyidin, Y., Pradnyana, I. W. W., ... & Saputro, I. A. (2023). Keamanan Sistem Informasi. Indiepress Books.

Priyanto. (2024). Buku ajar: Indonesia total war strategy: Strategi, taktik, dan implementasi (pp. 134–136). CV Aksara Global Akademia.

Priyanto. (2024a). Defense management: Integrating strategy, innovation, and leadership in the modern era. CV Aksara Global Akademia

Priyanto. (2024b). Network centric warfare (NCW): Dalam perspektif manajemen pertahanan (pp. 67–69). Garut, Jawa Barat: CV Aksara Global Akademia.

Priyanto. (2024c). Total war strategy: Revolutionizing warfare through comprehensive tactics and global leadership (pp. 124–127). CV Aksara Global Akademia.

Sugiyono. (2009). Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Alfabeta.

Tippe, Syarifudin. (2016). Ilmu Pertahanan, Sejarah, Konsep, Teori, dan Implementasi. Salemba Humanika.

Azzqy, A.A. (2024). Two Decades of Asymmetrical Threats to Non-traditional Security in Asia Pacific and Challenges for Indonesia (2003-2023). Budi Luhur Journal of Strategic & Global Studies.

Garcia, A. C., Martinez, M. V., Deagustini, C. A., & Simari, G. I. (2023). A multi-agent system for addressing cybersecurity issues in social networks. In ENIGMA@ KR (pp. 43–54).

Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber dan Sandi Negara. Jurnal Dinamika Global.

Kurniawan, A. (2022). Strategi keamanan siber nasional Indonesia: Tinjauan dan tantangan. Jurnal Keamanan Nasional, 15(2), 45–60.

Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet, 12, 157.

Manulis, M., Bridges, C. P., Harrison, R., Sekar, V., & Davis, A. (2021). Cyber security in new space: Analysis of threats, key enabling technologies and challenges. International Journal of Information Security, 20, 287-311.

Ramadhianto, R., Toruan, T.S., Kertopati, S.N., & Almubaroq, H.Z. (2023). Analysis of presidential regulations concerning cyber security to bolster defense policy management. Defense and Security Studies.

Simanjuntak, R. P., & Sijabat, R. R. M. (2024). Meningkatkan Keamanan Siber dalam Lingkungan Internet of Things (IoT) dengan Menggunakan Sistem Deteksi Intrusi Berbasis Pembelajaran Mesin. Dike, 2(2), 62-68.

Suharto, Priyanto. (2025). Legal protection in Indonesia's cyber resilience: Strategy and implementation to support national defense. Pena Justisia: Media Komunikasi dan Kajian Hukum, 23(3), 1. https://doi.org/10.31941/pj.v23i3.5639.

ANTARA. (2024). TNI commander receives president's order to form cyber military force. ANTARA Indonesian News Agency..

ANTARA. (2025). TNI to continue cyber defense training for soldiers. ANTARA Indonesian

News Agency. https://en.antaranews.com/news/343530/tni-to-continue-cyber- defense-training-for-soldiers .

BBC Indonesia. (2021). Sekitar 1,3 juta data pengguna eHAC di Indonesia berisiko disalahgunakan, seperti untuk penipuan hingga yang paling parah adalah manipulasi data, menurut pakar siber. https://www.bbc.com/indonesia/indonesia-58406164.

BBC News Indonesia. (2023). BSI diduga kena serangan siber, pengamat sebut sistem pertahanan bank 'tidak kuat'. https://www.bbc.com/indonesia/articles/cn01gdr7eero.

Badan Siber dan Sandi Negara (BSSN). (2023). Satu Dekade Kemitraan Komprehensif, RI dan Belanda Tingkatkan Kerja Sama di Bidang Keamanan Siber. https://www.bssn.go.id/satu-dekade-kemitraan-komprehensif-ri-dan-belanda- tingkatkan-kerja-sama-di-bidang-keamanan-siber/

Kemhan RI. (2021). Wamenhan : Peran Satelit Penting untuk Pertahanan Negara. https://www.kemhan.go.id/2021/12/23/wamenhan-peran-satelit-penting-untuk-pertahanan-negara.html. Diakses pada 11 November 2024.

Kemhan RI. (2024). Plt. Sekjen Kemhan Mewakili Wamenhan Jadi Narasumber Rapat Koordinasi Nasional Grand Design Keantariksaan Menuju Indonesia Emas 2045.

Purnama, B. E. (2023). Indonesia dan Inggris Sepakati Kerja Sama Keamanan Siber. Media Indonesia. https://mediaindonesia.com/internasional/592650/indonesia-dan-inggris-sepakati-kerja-sama-keamanan-siber

Saptohutomo, A. P. (2024). Konsep Angkatan Siber TNI, Pemerintah Dinilai Bisa Contoh Negara Lain. Kompas.com. http://kmp.im/AGHUh5

Saptohutomo, Aryo Putranto. (2023). Peretas Diduga Bobol Situs Kemenhan Manfaatkan Data Pegawai yang Bocor. https://nasional.kompas.com/read/2023/11/03/16515731/peretas-diduga-bobol-situs-kemenhan-manfaatkan-data-pegawai-yang-bocor. Diakses pada November 2024.

Kementerian Pertahanan Republik Indonesia. (2014). Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber. Jakarta: Kementerian Pertahanan RI.

Kementerian Pertahanan Republik Indonesia. (2015). Buku putih pertahanan. Jakarta: Kemhan RI.