International Journal of Integrated Science and Technology (IJIST)
Vol.3, No.1, 2025: 1241-1252

Development of Cyber Security System to Protect Domestic Defense Industry Infrastructure

Agra Nurtrihadi[1], Jupriyanto[2], Dangan Waluyo[3]
Universitas Pertahanan

Corresponding Author: Agra Nurtrihadi; agra.nurtrihadi@gmail.com

A R T I C L E I N F O

Keywords: Cybersecurity, Infrastructure, Defense Industry

Received : 12, November
Revised : 20, December
Accepted: 18, January

A B S T R A C T

Indonesia can join global alliances focusing on cybersecurity to accelerate the adoption of new technologies and share intelligence on global threats. The aim of this study is to explore how an effective cybersecurity system can be developed to protect the domestic defense industry's infrastructure from evolving cyber threats and to identify the main challenges faced in implementing cybersecurity technologies within the defense industry's infrastructure. The findings of this study indicate that through integrated efforts involving strong regulations, responsive policies, and strategic collaboration, the cybersecurity system of the defense industry can become more resilient. This not only protects defense interests but also strengthens national sovereignty and stability in an increasingly challenging digital era.

INTRODUCTION

In the increasingly advanced digital era, cybersecurity has become one of the main focuses in various sectors, including the domestic defense industry. Defense industry infrastructure plays a strategic role in maintaining the stability and sovereignty of the country. According to Aji (2023) the increasingly complex digital ecosystem and the increase in organized cyber attacks have put this infrastructure under serious threat. The development of a robust and adaptive cybersecurity system is an urgent need to protect the domestic defense industry infrastructure from potential risks that can weaken the country's resilience. The cybersecurity system in the context of the defense industry must be designed holistically, covering aspects of technology, human resources, and policy (Faizal et al., 2023) .

In terms of technology, system development must be oriented towards the implementation of advanced security solutions such as *Artificial Intelligence (AI), Machine Learning (ML), and Blockchain. AI and ML* can be used to detect and respond to cyber threats in real-time, enabling risk mitigation before attacks reach critical infrastructure. According to Nugroho et al. (2021) Blockchain technology can be utilized to improve data and transaction integrity, ensuring that sensitive information cannot be manipulated by unauthorized parties. The development of a cybersecurity system requires the integration of software and hardware that meets international standards. The implementation of firewalls, intrusion detection systems (IDS), and data encryption are fundamental steps that must be implemented (Sigiro et al., 2023) .

It is not enough to rely on technology alone, this development must also include periodic cyber attack simulations (penetration testing) to identify system vulnerabilities. The results of this test then become the basis for improving and strengthening the existing security system. From a human resources perspective, the development of a cybersecurity system requires competent experts. According to Rizki (2022) professionals in the field of cybersecurity must continue to be trained to deal with increasingly dynamic and complex threats. The government and educational institutions can work together to provide training and certification programs to improve the quality of the workforce in this sector. It is important to build a culture of cybersecurity awareness across all levels of the organization, so that every individual has a responsibility to protect the information and systems they use.

Regular educational campaigns can also help improve employee understanding of cyber threats and preventive measures. Policy aspects are also an important element in developing a cybersecurity system. According to Luthfah (2023) clear and firm regulations regarding data protection and cybersecurity must be implemented, including the imposition of severe sanctions against cybercriminals. The government must have an integrated national strategy, including coordination between various related institutions such as the military, intelligence agencies, and the private sector. In addition, policies must encourage investment in research and development of cybersecurity technology, so that Indonesia is not only a user, but also a producer of innovative cybersecurity technology (Makbull Rizki, 2022) .

International cooperation is also an integral part of the development of cybersecurity systems. Given the cross-border nature of cyber threats, collaboration with other countries in sharing information, technology, and best practices can strengthen national cyber defense. Indonesia can join a global alliance that focuses on cybersecurity to accelerate the adoption of new technologies and share intelligence on global threats. According to Sigiro et al., (2023) this cooperation must remain in line with national interests, ensuring that no strategic information is misused. Equally important, the development of cybersecurity systems must consider protecting the supply chain in the defense industry. Many modern cyber attacks target vendors or partners with weaker security gaps.

A comprehensive approach is needed that includes evaluating the security of business partners, monitoring the devices used, and proactively managing risks. In the long term, the successful development of a cybersecurity system in the defense industry will have a significant positive impact (Soesanto et al., 2023). This will increase national resilience to cyber threats that can paralyze critical systems, such as arms control, military logistics, and strategic communications. This development will also strengthen Indonesia's position on the global stage as a country with a reliable cybersecurity ecosystem. This success can open up new opportunities in the technology industry, such as the development of locally made cybersecurity software that has the potential to become a leading export product.

However, challenges remain in this development process. One of them is budget constraints, considering that advanced cybersecurity technology requires significant investment. Lack of coordination between various related parties is often an obstacle in building an integrated cybersecurity ecosystem. To overcome these challenges, the government needs to make cybersecurity a national priority, allocate adequate resources, and ensure synergy between stakeholders (Hajar, 2023) .

METHODS

Qualitative research methods are used in the development of cybersecurity systems to protect domestic defense industry infrastructure because they are able to dig up in-depth understanding of the needs, challenges, and opportunities in this field. Qualitative research aims to analyze phenomena holistically, focusing on the experiences, perceptions, and views of cybersecurity experts and practitioners. This method involves data collection through in-depth interviews, focus group discussions, and strategic document analysis. Key informants typically include information technology experts, security software developers, and stakeholders in the defense sector.

The data obtained was analyzed using a thematic approach, which allows the identification of key patterns and issues related to cyber threats, infrastructure vulnerabilities, and risk mitigation strategies. This study also emphasizes the importance of local context, such as regulations, domestic technological capabilities, and geopolitical conditions, to ensure that the solutions developed are relevant and effective. With a qualitative approach, this

study can produce strategic and innovative recommendations to create an adaptive cybersecurity system that is able to face the complexity of global threats, while supporting national resilience in a sustainable manner.

RESULTS AND DISCUSSIONS

In the digital era that is all connected, cyber threats have become one of the main challenges for national security, especially for sectors that have strategic interests such as the defense industry. According to (Svintsytsky, 2022) cyber threats that continue to grow in terms of frequency, complexity, and scale, require the development of a cybersecurity system that is not only resilient but also adaptive. This system must be able to anticipate, prevent, detect, and respond to various cyber threats quickly and effectively to protect the domestic defense industry infrastructure which is one of the main pillars of state sovereignty. The development of an effective cybersecurity system begins with conducting a comprehensive risk analysis.

This step aims to identify and understand potential threats that can disrupt the operation of defense infrastructure, such as ransomware attacks, data theft, sabotage, and Distributed Denial of Service (DDoS) attacks. Risk analysis also involves mapping vulnerabilities in the network, software, and hardware used. (Khlaponin et al., 2022) . With a comprehensive understanding of these threats and vulnerabilities, mitigation measures can be designed in a targeted manner. One of the key elements in developing an effective cybersecurity system is the application of advanced technologies capable of dealing with increasingly complex cyber threats. Artificial Intelligence (AI) and Machine Learning (ML) are two technologies that can play an important role in strengthening cybersecurity systems.

AI can be used to analyze big data and detect anomalous patterns that indicate potential cyberattacks. ML allows systems to learn and adapt to new threats automatically, thereby increasing system responsiveness and reliability. Another relevant technology is Blockchain, which can be used to maintain data integrity and prevent manipulation of sensitive information (Shulha et al., 2022) . In addition to technology, the development of a cybersecurity system must include the implementation of a zero trust-based strategy. Zero trust is a security approach that does not trust any entity, either from inside or outside the network, without verification. This approach ensures that every user or device must go through a strict authentication process before gaining access to the system. Zero trust also includes network segmentation to minimize the risk of spreading attacks if one part of the system is successfully penetrated (Tashtoush et al., 2022) .

The development of a cybersecurity system does not only focus on technology but also on human resources. Effective cybersecurity requires a competent and trained workforce. Training and certification for cybersecurity professionals are essential. According to (Kryshtanovych et al., 2023) a culture of cybersecurity awareness must be instilled throughout the organization, so that each individual understands their role in protecting the system from threats. Regular education and training campaigns can help improve employee understanding of the importance of cybersecurity and the steps they can take to

prevent attacks. Policies and regulations also play an important role in supporting the development of a cybersecurity system. The government must design a comprehensive and integrated national policy to ensure the security of the defense industry infrastructure (Macas et al., 2024) .

The policy includes minimum security standards, guidelines for risk mitigation, and mechanisms for reporting cyber incidents. Regulations should also support cooperation between the public and private sectors in technology development and sharing information related to cyber threats. International cooperation is also an important element in developing an effective cybersecurity system (Ferreira et al., 2023) . Cyber threats are cross-border, so collaboration with other countries can strengthen national defense. Sharing intelligence information on global threats, sharing best practices, and participating in international cybersecurity alliances can help Indonesia improve its defense capacity. However, this cooperation must be carried out carefully to ensure that national interests are maintained and strategic data is not misused.

To improve the effectiveness of the cybersecurity system, cyberattack simulations or penetration testing need to be carried out periodically. This simulation aims to identify weaknesses in the system before exploitation by irresponsible parties. The results of the simulation can be used to update security policies and strengthen the overall system defense. According to (Khatun et al., 2023) it is important to have a reliable disaster recovery mechanism to ensure that the system can return to function quickly after an attack. Another aspect that needs to be considered is protection of the supply chain. Many modern cyberattacks exploit weaknesses in vendors or partners connected to key infrastructure. Security evaluation of business partners and vendors should be part of the overall cybersecurity strategy.

The development of an effective cybersecurity system also requires adequate investment. The government and private sector must allocate sufficient budget for technology procurement, workforce training, research, and development. Although it requires large costs, this investment is very important to maintain the sovereignty and stability of the country (Kirshner, 2023) . The application of cybersecurity technology to domestic defense industry infrastructure is faced with various complex and dynamic challenges. As a very strategic sector that is vulnerable to cyber attacks, the defense industry requires a robust and adaptive security system. However, this effort is not free from various obstacles, both technical, financial, regulatory, and human resources. These challenges must be addressed comprehensively so that the security of defense infrastructure can be guaranteed.

One of the main challenges is the rapid and unpredictable development of cyber threats. Cybercriminals continue to develop new attack techniques and methods, such as Advanced Persistent Threats (APT), ransomware, phishing, and exploitation of zero-day vulnerabilities. According to (Karpiuk, 2021) Security technology that is considered cutting-edge today can quickly become obsolete when new threats emerge. The defense industry needs to continue investing in technology updates and the development of adaptive security systems that can detect and respond to threats in real-time. However, these

investments often require large costs, which is a challenge for developing countries with limited budgets. The limited human resources with expertise in cybersecurity are also a significant obstacle.

The defense industry requires professionals who not only understand the technical aspects of cybersecurity but also have knowledge of the specific needs of the defense sector. Unfortunately, the number of experts in this field is still limited, while the need continues to increase. This shortage is exacerbated by the high level of competition with the private sector which often offers greater incentives to attract the best talent (Aloseel et al., 2021) . As a result, the defense industry often struggles to retain quality experts in the long term. Another challenge is the vulnerability of the supply chain. The defense industry often works with vendors, partners, and third parties to procure technology, hardware, and software. If one party in the supply chain has a weakness in its security system, then the entire defense infrastructure can be targeted for attack. For example, software or hardware infected with malware can be used to infiltrate key systems. Rigorous security evaluations and audits of all partners are required, which often require a lot of time and resources (Kuzior et al., 2023).

Interoperability issues are also a significant challenge. Defense infrastructure often consists of multiple systems built by different vendors, with varying technology standards. This incompatibility can create security gaps that are vulnerable to exploitation. Integration between new technologies and legacy systems is often a complicated and risky process. Legacy systems often have limited security updates, making them more vulnerable to cybercriminals (Lee et al., 2022) . In terms of regulation, the main challenge lies in the lack of a comprehensive legal and policy framework related to cybersecurity in the defense sector. Although several countries, including Indonesia, have basic regulations regarding cybersecurity, specific policies to protect defense infrastructure often lack detail.

The implementation of regulations is often hampered by slow bureaucracy and lack of coordination between institutions. In fact, cybersecurity requires a fast and coordinated response, especially when dealing with emergency incidents. Funding is also a major obstacle in the application of cybersecurity technology in the defense sector (Al Humaid Alneyadi & Normalini, 2023) . Advanced technologies, such as Artificial Intelligence (AI), Machine Learning (ML), and Blockchain, which can increase the effectiveness of security systems, require large investments in procurement, development, and maintenance. Developing countries often face limited defense budgets, so funding priorities are allocated more to other operational needs than to the development of cybersecurity technology.

The threat of insider attacks is also a challenge that is often overlooked. Employees or personnel who have access to defense systems can be a threat if they intentionally or unintentionally leak confidential information or facilitate cyber attacks (Fernandez De Arroyabe et al., 2023) . These insider attacks are difficult to detect and require strict supervision and policies to prevent them. For example, implementing the principle of least privilege, which provides minimal access to personnel according to their job requirements, can help reduce this risk.

On the other hand, the lack of awareness of the importance of cybersecurity among stakeholders is often a major obstacle. Some organizations still view cybersecurity as a purely technical issue, without realizing its strategic impact on operations and state sovereignty. This low awareness often leads to inadequate resource allocation for the development and maintenance of security systems. (Khoironi, 2020) .

International cooperation also faces its own challenges. Although cyber threats are cross-border and require global collaboration, not all countries are willing to share strategic information related to cyber threats. This is often influenced by concerns about data leakage or mistrust between countries. In fact, effective cooperation can help accelerate the response to global threats and strengthen the overall cybersecurity system (Farid et al., 2023) . Regulation, policy, and inter-agency cooperation play a very important role in developing a cybersecurity system for the defense industry. As a strategic sector, the defense industry is often the main target of cyber attacks aimed at weakening national stability and security. In this context, comprehensive regulations, adaptive policies, and solid cooperation between related institutions are the main pillars for creating an effective and threat-resistant cybersecurity system (Vania et al., 2023) .

Regulation serves as a legal basis that governs every aspect of cybersecurity in the defense sector. Clear and detailed regulations provide guidance for all relevant parties, including government, industry, and cooperation partners, in developing and implementing security systems. For example, regulations can include cyber incident reporting obligations, minimum security standards for hardware and software, and periodic security evaluation and audit mechanisms (Mukhlis et al., 2024) . Regulations must also accommodate the development of new technologies and threats. Without adequate regulations, the development of cybersecurity systems tends to run without a clear direction and has the potential to create gaps that can be exploited by irresponsible parties. Policies, on the other hand, provide an operational framework for implementing regulations. Well-designed policies must be able to adapt to the specific needs of the defense sector, including sensitive data management and critical infrastructure protection (Hariyadi & Nastiti, 2021) .

One example of a relevant policy is the development of a national framework for cybersecurity that includes risk mitigation strategies, technical capacity building, and budget allocation for research and development of security technology. The policy should also include education and training for human resources in the defense sector, so that personnel involved have adequate competence in dealing with increasingly complex cyber threats. (Soewardi, 2013) . In addition to regulations and policies, inter-agency cooperation is a key element in building a resilient cybersecurity system. In the context of the defense industry, this cooperation includes collaboration between ministries, defense institutions, intelligence agencies, and the relevant private sector. This collaboration is needed to ensure a rapid and accurate exchange of information on cyber threats, so that the response given can be more effective. For example, intelligence agencies can provide information on potential threats, while

technical institutions are responsible for developing appropriate technological solutions (Munawar, 2020) .

International cooperation is also important. Cyber threats are often cross-border, requiring coordination with other countries to address them. In this regard, the defense industry can take advantage of global cooperation platforms such as the NATO Cyber Defense Center or similar frameworks that allow the exchange of knowledge and technology between countries. However, international cooperation often faces challenges, especially related to issues of trust and data confidentiality (Khotimah et al., 2022) . A clear policy is needed regarding the boundaries and conditions of cooperation, so that collaboration can take place without compromising national security. Cooperation between the government and private sectors also plays an important role. Many advanced security technologies used in the defense sector are developed by private companies. Partnerships between the government and the private sector should focus on research and development of cybersecurity technologies that are specific to defense needs.

Technology companies can work with defense agencies to create early detection systems that can identify cyber threats in real time. On the other hand, the government must provide incentives for private companies to actively participate in this effort, for example by providing research funds or tax exemptions. Regulations, policies, and inter-agency cooperation must also be supported by strengthening awareness of the importance of cybersecurity among stakeholders (Putri et al., 2022) . This awareness must be built through ongoing education programs, campaigns, and training. For example, military personnel serving in the field of cyber defense must be given a deep understanding of applicable regulations and how to implement them in their daily duties. Without adequate awareness, regulations and policies that have been formulated are often not implemented optimally.

However, the development of regulations, policies, and inter-agency cooperation is not without challenges. One of the main obstacles is slow bureaucracy, which often hinders the implementation of policies quickly and effectively. In addition, the lack of coordination between institutions often results in overlapping responsibilities and unsynchronized policies (Elan Maulani et al., 2023) . To overcome these obstacles, a more integrated coordination mechanism is needed, for example through the establishment of a special agency responsible for cybersecurity in the defense sector. In the long term, effective regulations, policies, and inter-agency cooperation will create a cybersecurity ecosystem that is stronger and more responsive to threats. This not only protects the defense industry infrastructure but also strengthens the country's sovereignty as a whole. With strong regulations, adaptive policies, and solid cooperation, the defense industry will be better prepared to face the challenges of the digital era, where cyber threats are one of the biggest risks to national stability and security (Sahrudin & Ulum, 2023) .

CONCLUSIONS AND RECOMMENDATIONS

Regulation, policy, and inter-agency cooperation are fundamental elements in developing a cybersecurity system to protect the domestic defense industry infrastructure. Regulation provides a clear legal framework, policy creates an adaptive operational strategy, while inter-agency cooperation ensures the synergy needed to address increasingly complex and cross-border cyber threats. The importance of this cooperation is not only involving domestic institutions, but also the private sector and international cooperation to support technological innovation and rapid response to threats.

Strengthening awareness of cybersecurity, integrating inter-agency coordination mechanisms, and reducing bureaucratic obstacles are the main challenges that need to be overcome. With integrated efforts through strong regulations, responsive policies, and strategic collaboration, the defense industry cybersecurity system can become more resilient. This not only protects defense interests, but also strengthens the sovereignty and stability of the country in the challenging digital era **.**

REFERENCES

Aji, M. P. (2023). Sistem Keamanan Siber Dan Kedaulatan Data Di Indonesia Dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System And Data Sovereignty In Indonesia In Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2). Https://Doi.Org/10.22212/Jp.V13i2.3299

Al Humaid Alneyadi, M. R. M., & Normalini, M. K. (2023). Factors Influencing User's Intention To Adopt Ai-Based Cybersecurity Systems In The Uae. *Interdisciplinary Journal Of Information, Knowledge, And Management*, *18*. Https://Doi.Org/10.28945/5166

Aloseel, A., He, H., Shaw, C., & Khan, M. A. (2021). Analytical Review Of Cybersecurity For Embedded Systems. In *Ieee Access* (Vol. 9). Https://Doi.Org/10.1109/Access.2020.3045972

Elan Maulani, I., Rayhan Sunandar Putra, D., & Komarudin, K. (2023). Sistem Deteksi Intrusi Cerdas: Studi Perbandingan Algoritma Pembelajaran Mesin Untuk Keamanan Siber. *Jurnal Sosial Teknologi*, *3*(11). Https://Doi.Org/10.59188/Jurnalsostech.V3i11.987

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis Risiko Teknologi Informasi Pada Bank Syariah : Identifikasi Ancaman Dan Tantangan Terkini. *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam*, *5*(2). Https://Doi.Org/10.47435/Asy-Syarikah.V5i2.2022

Farid, I., Reksoprodjo, A. H., & Suhirwan. (2023). Pemanfaatan Artificial Intelligence Dalam Pertahanan Siber. *Nusantara: Jurnal Ilmu Pengetahuan Sosial* , *10*(2).

Fernandez De Arroyabe, I., Arranz, C. F. A., Arroyabe, M. F., & Fernandez De Arroyabe, J. C. (2023). Cybersecurity Capabilities And Cyber-Attacks As Drivers Of Investment In Cybersecurity Systems: A Uk Survey For 2018 And

2019. *Computers And Security*, *124*. Https://Doi.Org/10.1016/J.Cose.2022.102954

Ferreira, L., Silva, D. C., & Itzazelaia, M. U. (2023). Recommender Systems In Cybersecurity. *Knowledge And Information Systems*, *65*(12). Https://Doi.Org/10.1007/S10115-023-01906-6

Hajar, S. (2023). Digital Entrepreneurship Discourse In The National Economy. *Innovative: Journal Of Social Science Research*, *3*(1).

Hariyadi, D., & Nastiti, F. E. (2021). Analisis Keamanan Sistem Informasi Menggunakan Sudomy Dan Owasp Zap Di Universitas Duta Bangsa Surakarta. *Jurnal Komtika (Komputasi Dan Informatika)*, *5*(1). Https://Doi.Org/10.31603/Komtika.V5i1.5134

Karpiuk, M. (2021). The Local Government's Position In The Polish Cybersecurity System. *Lex Localis*, *19*(3). Https://Doi.Org/10.4335/19.3.609-620(2021)

Khatun, M., Wagner, F., Jung, R., & Glaß, M. (2023). An Application Of Dematel And Fuzzy Dematel To Evaluate The Interaction Of Safety Management System And Cybersecurity Management System In Automated Vehicles. In *Engineering Applications Of Artificial Intelligence* (Vol. 124). Https://Doi.Org/10.1016/J.Engappai.2023.106566

Khlaponin, Y., Kozubtsova, L., Kozubtsov, I., & Shtonda, R. (2022). Functions Of The Information Security And Cybersecurity System Of Critical Information Infrastructure. *Cybersecurity: Education, Science, Technique*, *3*(15). Https://Doi.Org/10.28925/2663-4023.2022.15.1241341

Khoironi, S. C. (2020). Pengaruh Analisis Kebutuhan Pelatihan Budaya Keamanan Siber Sebagai Upaya Pengembangan Kompetensi Bagi Aparatur Sipil Negara Di Era Digital. *Jurnal Studi Komunikasi Dan Media*, *24*(1). Https://Doi.Org/10.31445/Jskm.2020.2945

Khotimah, H., Bimantoro, F., & Kabanga, R. S. (2022). Implementasi Security Information And Event Management (Siem) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat. *Jurnal Begawe Teknologi Informasi (Jbegati)*, *3*(2). Https://Doi.Org/10.29303/Jbegati.V3i2.752

Kirshner, M. (2023). Model-Based Systems Engineering Cybersecurity For Space Systems. *Aerospace*, *10*(2). Https://Doi.Org/10.3390/Aerospace10020116

Kryshtanovych, M., Lyubomudrova, N., Bondar, H., Motornyy, V., & Kuchmenko, V. (2023). An Intelligent Multi-Stage Model For Countering The Impact Of Disinformation On The Cybersecurity System. *Ingenierie Des Systemes D'information*, *28*(1). Https://Doi.Org/10.18280/Isi.280105

Kuzior, A., Yarovenko, H., Brożek, P., Sidelnyk, N., Boyko, A., & Vasilyeva, T. (2023). Company Cybersecurity System: Assessment, Risks And Expectations. *Production Engineering Archives*, *29*(4). Https://Doi.Org/10.30657/Pea.2023.29.43

Lee, D., Kim, D., Lee, C., Ahn, M. K., & Lee, W. (2022). Icstasy: An Integrated Cybersecurity Training System For Military Personnel. *Ieee Access*, *10*. Https://Doi.Org/10.1109/Access.2022.3182383

Luthfah, D. (2023). Penguatan Keamanan Siber Pada Sektor Jasa Keuangan Indonesia. *Jurnal Penelitian Dan Karya Ilmiah Lembaga Penelitian Universitas Trisakti*. Https://Doi.Org/10.25105/Pdk.V9i1.18643

Macas, M., Wu, C., & Fuertes, W. (2024). Adversarial Examples: A Survey Of Attacks And Defenses In Deep Learning-Enabled Cybersecurity Systems. In *Expert Systems With Applications* (Vol. 238). Https://Doi.Org/10.1016/J.Eswa.2023.122223

Makbull Rizki. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia Dalam Menghadapi Tantangan Perkembangan Teknologi Dan Informasi. *Politeia: Jurnal Ilmu Politik*, *14*(1). Https://Doi.Org/10.32734/Politeia.V14i1.6351

Mukhlis, M., Arsad, A., Mukhsin, Z., & Said, S. (2024). Transformasi Digital Dalam Ekonomi Modern. *Jurnal Penkomi: Kajian Pendidikan Dan Ekonomi*, *7*(1).

Munawar, Z. (2020). Mekanisme Keselamatan, Keamanan Dan Keberlanjutan Untuk Sistem Siber Fisik. *Tematik*, *7*(1). Https://Doi.Org/10.38204/Tematik.V7i1.371

Nugroho, I. I., Pratiwi, R., & Az Zahro, S. R. (2021). Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber Di Indonesia. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, *1*(2). Https://Doi.Org/10.15294/Ipmhi.V1i2.53698

Putri, A. W. O. K., Aditya, A. R. M., Musthofa, D. L., & Widodo, P. (2022). Serangan Hacking Tools Sebagai Ancaman Siber Dalam Sistem Pertahanan Negara (Studi Kasus: Predator). *Global Political Studies Journal*, *6*(1). Https://Doi.Org/10.34010/Gpsjournal.V6i1.6698

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

Sahrudin, S., & Ulum, M. B. (2023). Penerapan Keamanan Siber Pada Sistem Transportasi Laut. *Jurnal Ilmiah Universitas Batanghari Jambi*, *23*(3). Https://Doi.Org/10.33087/Jiubj.V23i3.3839

Shulha, O., Yanenkova, I., Kuzub, M., Muda, I., & Nazarenko, V. (2022). Banking Information Resource Cybersecurity System Modeling. *Journal Of Open Innovation: Technology, Market, And Complexity*, *8*(2). Https://Doi.Org/10.3390/Joitmc8020080

Sigiro, F. H., Runturambi, A. J. S., & Widiawan, B. (2023). Collaborative Sharing Intelijen Ancaman Pada Komunitas Csirt Dalam Memperkuat Keamanan Siber Nasional. *Syntax Literate ; Jurnal Ilmiah Indonesia*, *7*(9). Https://Doi.Org/10.36418/Syntax-Literate.V7i9.14245

Soesanto, E., Romadhon, A., Dwi Mardika, B., & Fahmi Setiawan, M. (2023). Analisis Dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman Dan Solusi Dalam Lingkungan Digital Untuk Mengamankan Objek Vital Dan File. *Sammajiva : Jurnal Penelitian Bisnisdan Manajemen*, *1*(2).

Soewardi, B. A. (2013). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) Yang Tangguh Bagi Indonesia. *Potensi Pertahanan*.

Svintsytsky, A. V. (2022). The System Of Cybersecurity Bodies In Ukraine. *Revista Cientifica General Jose Maria Cordova*, *20*(38). Https://Doi.Org/10.21830/19006586.903

Tashtoush, Y. M., Darweesh, D. A., Husari, G., Darwish, O. A., Darwish, Y., Issa,

L. B., & Ashqar, H. I. (2022). Agile Approaches For Cybersecurity Systems, Iot And Intelligent Transportation. *Ieee Access*, *10*. Https://Doi.Org/10.1109/Access.2021.3136861

Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber. *Jurnal Multidisiplin Indonesia*, *2*(3). Https://Doi.Org/10.58344/Jmi.V2i3.157