International Conference Restructuring and
Transforming Law 2026
Volume 5, Issue 1, July 2026
e-ISSN :2963-931X
icrtlaw@ums.ac.id

Cyber Security Risk Management in Critical Infrastructure and Public Services

Anteng Nirwanto, S.A.P.,M.A.P

Public Administration, Law and Politic Science, Universitas Muhammadiyah Surakarta

an664@ums.ac.id

Najwa Filza

Public Administration, Law and Politic Science, Universitas Muhammadiyah Surakarta

C300250081@student.ums.ac.id

Kafka Anwijzi

Public Administration, Law and Politic Science, Universitas Muhammadiyah Surakarta
C300250114@student.ums.ac.id

Rona Kartika Cahya Wulan

Public Administration, Law and Politic Science, Universitas Muhammadiyah Surakarta
C300250049@student.ums.ac.id

ABSTRACT

The development of information and communication technology has driven digital transformation in various sectors, particularly critical infrastructure and public services. However, increased connectivity and dependence on digital systems have also been accompanied by increasingly complex cybersecurity threats. This study aims to analyze cybersecurity risk management in critical infrastructure and public services through the stages of risk identification, evaluation, and mitigation. The method used is a systematic literature review by reviewing various academic sources, technical reports, and policy documents related to cybersecurity. The results show that cyber threats such as malware, phishing, DDoS attacks, data leaks, and insider threats are the main risks faced by organizations. Risk evaluation is carried out by considering the level of likelihood and impact, thus determining appropriate handling priorities. Effective mitigation strategies include the implementation of security technologies such as firewalls, IDS/IPS, data encryption, the Zero Trust Architecture approach, increasing human resource capacity, and strengthening security policies and governance. Furthermore, the use of artificial intelligence and machine learning technologies provides innovative solutions for detecting threats in real time. Thus, the implementation of comprehensive and sustainable cybersecurity risk management is essential to improve system resilience and maintain the continuity of public services amidst the ever-evolving dynamics of cyber threats.

Keywords: cyber security, risk management, critical infrastructure, public services, risk mitigation

INTRODUCTION

In this context, critical infrastructure and public services are prime targets for cyber attacks, which have the potential to cause system damage, information theft, and disruption of essential services for the public (Ashari, 2018). In today's digital era, infrastructure such as the energy, transportation, healthcare, banking, and telecommunications sectors, as well as information technology-based public service systems, are prime targets for cyberattackers. This is because these two sectors play a crucial role in maintaining the continuity of community activities and national stability. When systems in these sectors are attacked, the impact is felt not only by a single agency but can spread, disrupting the lives of society as a whole.

Cyberattacks on infrastructure can result in system failures, such as the paralysis of computer networks, disruption of industrial control systems, or the disruption of digital services. Furthermore, cybercriminals can steal critical information, such as personal data, financial data, and strategic government information. This data leak has the potential to be misused for illegal purposes, such as fraud, extortion, or even espionage.

Furthermore, cyberattacks can also disrupt critical services that are crucial for the public, such as healthcare, electricity, clean water, and government administration. If these services are disrupted, it can cause panic, economic losses, and even a decline in public trust in the government. Therefore, protecting public infrastructure and services from cyber threats is crucial to ensuring the continuity of services and overall public security. Therefore, comprehensive cyber risk management is needed to identify potential threats, evaluate system vulnerabilities, and formulate effective mitigation strategies. Implementing a structured cybersecurity framework is crucial in addressing the ever-growing complexity of digital threats, given that the escalation of connectivity between devices and infrastructure globally increases the potential for vulnerability (Susanto et al., 2023)**.** Implementing a structured cybersecurity framework is crucial as today's digital threats continue to grow in both number and sophistication. Cyberattacks are no longer simple, but use complex, organized techniques that are often difficult to detect. Therefore, organizations need a clear, systematic, and standardized system or framework to manage cybersecurity effectively and consistently.

Cybersecurity frameworks, such as NIST or ISO 31000, help organizations identify risks, protect systems, detect threats, respond to incidents, and recover after attacks. Without a structured framework, security efforts tend to be reactive, uncoordinated, and less than optimal in the face of

dynamic threats. Furthermore, the increasing connectivity between devices and infrastructure globally is also a major factor increasing the potential for vulnerabilities. Today, various systems are interconnected via the internet, including IoT devices, systems, and other information systems. *cloud*, and industrial networks. This connectivity does facilitate operations, but on the other hand, it opens up more opportunities for cybercriminals to penetrate the system. The more connected devices, the wider the attack surface that can be exploited by attackers. If a single point in the network is vulnerable, it can become a gateway to attack the entire system. Therefore, implementing a structured cybersecurity framework is crucial to ensure every system component is well-protected and capable of dealing with evolving threats.

These threats can manifest in various forms, including malware viruses, hacker attacks, and information leaks caused by internal negligence (Mahendra & Soewito, 2023). In analyzing the impact of cybercrime on national defense, identifying risk management is very important to understand the opportunities and consequences that result.(Sasmito et al., 2020). Implementation of cybersecurity frameworks such as NIST Cybersecurity and CIS Controls can be a strategic guide for the government in managing this risk effectively (Mahendra & Soewito, 2023). This approach is not only applicable to the private sector, but is also vital for the public sector, especially in managing sensitive data such as civil servant personnel information, which is vulnerable to cyber threats such as data theft and cyber extortion.(Yulisuyanti & Soewito, 2023).

The increasing number and complexity of cyber attacks globally underscores the importance of developing stronger cyber security strategies, particularly to protect data and computer systems from various forms of attacks such as data theft,*malware*, and DDoS attacks (Susanto et al., 2023). The shifting cyber threat landscape, particularly with the increasing use of remote-based industrial control system management and industry adaptation to the working conditions of the COVID-19 pandemic, further highlights infrastructure vulnerabilities and the need for adaptive mitigation strategies.(Adegbite et al., 2023). This phenomenon shows that cybersecurity has become a top priority not only for Indonesia, but also for all countries in the world, considering that Information and Communication Technology has been integrated into various aspects of people's lives, including the government sector (Prabaswari et al., 2022).

METHOD/IDEA

This research uses a literature review method, collecting data from various sources, such as academic journals, technical reports, and policy documents related to cyber threats and national security standards (Putri et al., 2022). This process involves summarizing and analyzing various cybersecurity policies and appropriate risk analysis methods to mitigate weaknesses in digital infrastructure systems. Furthermore, the analysis results are aligned with the NIST Cybersecurity Framework to build a more robust system capable of reducing the risk of attacks on critical digital assets (Mahendra & Soewito, 2023; Wibowo et al., 2024). This approach also emphasizes the importance of collaboration between the government, the private sector, and international parties to create a cybersecurity system that is better prepared to face evolving threats (Sendjaja et al., 2024). Furthermore, this research refers to national defense regulations as a basis for maintaining digital security and sovereignty amidst various complex cyber threats (Syafi'i et al., 2023). The strategy used combines cyber intelligence capabilities and legal compliance to strengthen the defense system in the face of threats such as ransomware, phishing,and attack botnets (W.P. et al., 2023).

RESULTS AND DISCUSSION

This analysis focuses on assessing the vulnerability of critical infrastructure to cyberattacks occurring throughout 2025, taking into account a 38% increase in global attacks (Mahendra & Soewito, 2023). The results indicate that without a clear and standardized risk management system, agency preparedness to address operational impacts and financial losses remains relatively low. The disparity between rapid digital development and limited cyber defense capabilities necessitates a more in-depth evaluation of national security policies to ensure systems remain robust against increasingly widespread and transnational threats (Susanto et al., 2023). Furthermore, intersectoral collaboration needs to be enhanced, particularly in sharing information related to cyberthreats (Maesaroh, 2025; Putri et al., 2023). Furthermore, the use of an artificial intelligence-based early detection system is also essential to accelerate responses to suspicious data activity, so attacks can be prevented before they become major problems (Khairunnisa et al., 2024).

Improving human resource capabilities in the public sector through digital literacy and cybersecurity training is urgently needed to reduce the risk of data breaches caused by human error (Maesaroh, 2025). Furthermore, the use of security technologies such as Next-Generation Firewall and standardized data encryption systems must be implemented immediately to close security gaps,

especially in critical parts of public service networks. Furthermore, cooperation between national institutions also needs to be strengthened through clear coordination in handling cyber incidents, so that they no longer operate in isolation (Setiawan et al., 2020). Establishing a Cyber Incident Response Team in each government agency is a crucial step to ensure swift, coordinated, and structured handling of cyber attacks (Prabaswari et al., 2022). Furthermore, implementing a robust approach*Zero Trust*In digital systems, it is also important to ensure that every party connected to critical infrastructure is always verified and monitored, so that system security can be maintained sustainably.

Implementation of this architecture requires strict authentication for every user and device that attempts to access resources, both from inside and outside the network perimeter.(Saydazimova et al., 2025). In addition, the development of a national cyber resilience mechanism must be supported by policy updates that can bridge regulatory gaps, including in the classification of sensitive data and coordination between institutions (Jose, 2021). In addition, organizations need to invest in early detection technology based on machine-learning and quantum-resistant cryptography to anticipate increasingly sophisticated attack methods (Chisty et al., 2022)This strategy must be supported by regular software updates and the implementation of strict security policies that cover technical aspects and ongoing training for staff (Vu et al., 2025). Furthermore, the development of a comprehensive incident response protocol is a must so that every agency is able to identify, isolate, and restore system operations quickly after an attack (Benaichouba et al., 2024). A multidimensional approach encompassing regulatory strengthening, public education, and human resource capacity development is a key pillar in building a sovereign digital ecosystem that is resilient to the dynamics of cyber threats. Furthermore, a systematic integration of disaster recovery plans is necessary to ensure the continuity of public service functions even in the event of disruptions to key systems. This defense strategy aligns with the need to develop a sustainable national security architecture to safeguard national sovereignty through preventative measures, impact assessments, and measured response to attacks (Syafi'i et al., 2023).

In accordance with the principles of ISO 31000:2018, determining effective mitigation measures should be based on periodic risk assessments. This ensures that each security system is implemented according to the importance of the assets being protected (Balafif, 2023). This approach also includes an evaluation of the implementation of the system *Zero Trust Architecture*, which has

proven to be more effective than traditional security methods in detecting threats, especially in complex systems. With this approach, threats from within an organization can be identified more accurately, including activities previously considered safe because they originate from internal users. As technology advances, the use of algorithms *machine learning.* Adaptive security becomes very important to detect real attacks, especially on infrastructure *Internet of Things* dynamic (IoT) (Chisty et al., 2022). In addition, the implementation of network segmentation also plays a crucial role in limiting attacker movement within the system by separating critical sections, preventing attacks from spreading throughout the network. With the principle of "never trust, always verify," every user and device must always be verified before being granted access to critical data or systems (Hassan et al., 2025). This approach, when combined with artificial intelligence and machine learning, can improve the system's ability to detect threats, recognize unusual patterns, and automatically adjust security policies according to the risk level. Overall, this approach enables security systems to be more proactive in detecting new threats and more quickly respond to changing network conditions, thereby increasing system resilience to cyberattacks (Jose, 2021).

Cyber Security Risk Identification

Cybersecurity risk identification is a crucial initial step in the risk management process, aiming to identify potential threats, vulnerabilities, and potential impacts on information systems and digital infrastructure. This stage serves as the primary foundation for determining appropriate security measures, as without a clear understanding of the risks faced, mitigation efforts tend to be ineffective. According to Putri et al. (2022), risk identification is a systematic process for uncovering potential threats that could impact the continuity of an organization's information systems.

In the context of critical infrastructure and public services, the risk identification process involves inventorying all owned digital assets, such as servers, networks, applications, databases, and user devices. These assets are then analyzed to determine their importance and the potential impact in the event of a disruption or attack. This aligns with Mahendra and Soewito's (2023) opinion, which states that cyber risk management must begin with asset mapping and identifying their critical role to the organization's operations.

Next, we identify various types of cyber threats that could potentially attack the system. These threats can originate from both external and internal sources. External threats include attacks from hackers, cybercrime groups, and state actors, while internal threats can stem from employee

negligence or misuse of access. Susanto et al. (2023) emphasized that the increasing complexity of cyber threats requires organizations to comprehensively understand various threat sources, both external and internal. Some commonly identified types of cybersecurity risks include:

1. Malware

   Malware is a program designed to damage or access a system without permission. Types include:*virus, worm, trojan*, and ransoms which can encrypt data and demand ransom. According to W.P. et al. (2023), ransomware attack is one of the most significant threats because it can completely stop system operations.

2. *Phishing*

   Phishing is a fraudulent attempt to impersonate a trusted party to obtain sensitive information. This technique often exploits the weaknesses of human users. Maesaroh (2025) states that human error is one of the main causes of successful phishing attacks.

3. Serangan Distributed Denial of Service (DDoS)

   These attacks aim to paralyze services by flooding servers with massive amounts of data traffic. Prabaswari et al. (2022) state that DDoS attacks can significantly disrupt public services and undermine public trust in government institutions.

4. Data Leak

   Data breaches occur when sensitive information is accessed or shared without authorization. The impact is not only financial but also damaging to an organization's reputation. Yulisuyanti and Soewito (2023) emphasize that data protection is a crucial aspect of digital-based public service systems.

5. Insider Threat

   These threats originate from within the organization, either intentionally or unintentionally. Prabaswari et al. (2022) explain that internal threats are often difficult to detect because they involve parties with legitimate access to the system.

In addition to threats, identification also includes an analysis of vulnerabilities in the system. Vulnerabilities can include outdated software, insecure system configurations, or weak authentication mechanisms. According to Prabaswari et al., (2022), unmanaged vulnerabilities can become the main entry point for cyberattacks. The human factor is also a crucial aspect in risk identification. Lack of

cybersecurity awareness and literacy is often the primary cause of incidents. Maesaroh (2025) emphasized that increasing human resource capacity through cybersecurity training is essential to minimize risks caused by user error. By conducting a comprehensive risk identification, organizations can gain a clear picture of their risk profile. This allows for the development of more targeted and effective security strategies to protect critical infrastructure and public services from various evolving cyber threats (Susanto et al., 2023).

Cyber Security Risk Evaluation

Cybersecurity risk evaluation is the next step after the risk identification process, which aims to assess the severity of each identified risk. This process involves analyzing the likelihood of a threat occurring and its impact on the system, allowing the organization to determine appropriate response priorities. Risk evaluation is a crucial step in risk management because it helps organizations determine their risk tolerance level and appropriate mitigation strategies.

In the context of critical infrastructure and public services, risk assessment becomes increasingly important because any disruption can have a broad impact on society. Therefore, risk assessments consider not only technical aspects but also social, economic, and even national security impacts. Susanto et al. (2023) state that organizations must be able to comprehensively measure risk levels to respond to threats effectively and efficiently.

The risk evaluation process is generally carried out using two main parameters, namely the possibility of the risk occurring (likelihood) and the impacts caused (impact). Probability refers to the likelihood of a threat occurring, while impact relates to the extent of the loss if the risk actually occurs. The combination of these two parameters results in a risk level that can be classified into several categories, such as low, medium, and high.

According to Mahendra and Soewito (2023), the use of the risk matrix is an effective method for evaluating risk because it provides a visual representation of the priority risks that need to be addressed immediately. Risks with a high probability and significant impact are usually categorized as critical risks that require immediate action.

Furthermore, risk evaluations must also consider previously identified system vulnerabilities. Systems with high levels of vulnerability tend to be at greater risk of cyberattacks. Therefore, organizations need to assess the effectiveness of implemented security controls. Wibowo et al. (2024)

emphasize that evaluating security controls is necessary to ensure that existing protection mechanisms are capable of significantly reducing risks. In practice, cybersecurity risk evaluations can also involve the use of international standards such as ISO 31000 and NIST Cybersecurity Framework. These two frameworks provide guidance for conducting systematic and structured risk assessments. According to Putri et al. (2022), implementing these standards can help organizations improve consistency and accuracy in the risk evaluation process.

Furthermore, risk evaluation is not static but must be conducted periodically. This is due to the ever-evolving dynamics of cyber threats and changes in the systems and technologies used. New threats can emerge at any time, so organizations must constantly update their risk assessments to remain relevant to current conditions. Maesaroh (2025) states that ongoing risk evaluation can improve an organization's readiness to face increasingly complex cyber threats. Risk evaluation must also consider the human factor as one of the main sources of risk. User error, lack of security awareness, and policy violations can significantly increase the risk level. Therefore, in addition to technical evaluations, organizations also need to assess behavioral aspects and security culture within the work environment. Thus, cybersecurity risk evaluation is a crucial process in determining risk management priorities and designing effective mitigation strategies. Through comprehensive and ongoing evaluations, organizations can increase system resilience and minimize the impact of cyberattacks on critical infrastructure and public services.

Risk Mitigation Strategy

A cybersecurity risk mitigation strategy is a crucial stage in the risk management cycle, aiming to reduce the likelihood of threats occurring and minimize the impact if a cyber incident cannot be avoided. After risk identification and evaluation, organizations are required to formulate systematic, adaptive, and sustainable mitigation measures. The effectiveness of risk mitigation depends heavily on the alignment of the risk level with the implemented security controls. In the context of critical infrastructure and public services, mitigation strategies focus not only on technological protection but also encompass organizational governance and human resource readiness. This is due to the multidimensional nature of cyber threats, which can exploit both technical and non-technical vulnerabilities. Susanto et al. (2023) emphasize that a comprehensive mitigation approach is needed to address the increasingly complex and dynamic escalation of cyber threats.

One of the key strategies is the implementation of integrated cybersecurity technical controls. These controls include the use of firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and data encryption systems to protect the confidentiality and integrity of information. In addition, the implementation of Next-Generation Firewalls (NGFWs), which are capable of performing deep traffic inspection, has become increasingly important in addressing modern cyber threats. W.P. et al. (2023) state that the integration of various security technologies can significantly improve attack detection and prevention capabilities. Furthermore, the implementation of vulnerability management through regular system updates (*patch management*) is a crucial step in risk mitigation. Many cyberattacks exploit security vulnerabilities in outdated software. Therefore, organizations need to ensure that all systems and applications are always up-to-date. Vu et al. (2025) emphasize that effective patch management can significantly reduce the risk of vulnerability exploitation.

An increasingly adopted mitigation strategy is the implementation of Zero Trust Architecture (ZTA). This approach is based on the principle *"*never trust, always verify*"*, where every access to the system must go through a strict authentication and authorization process. No entity is automatically trusted, either from within or outside the network. Prabaswari et al., (2022) explain that this approach is effective in reducing the risk of lateral movement of attackers within the system. Furthermore, organizations need to implement network segmentation to limit access between systems and prevent the spread of attacks. By dividing the network into several segments, potential damage from attacks can be controlled and prevented from spreading throughout the system. Susanto et al. (2023) state that network segmentation is an important strategy in increasing system resilience against internal and external attacks.

From a non-technical perspective, improving human resource capacity is a crucial part of risk mitigation. The human factor is often a weak point in cybersecurity, both due to a lack of awareness and skills. Therefore, cybersecurity training and education need to be carried out continuously. Maesaroh (2025) emphasized that increasing cybersecurity literacy can significantly reduce the risks caused by user error (human error). Organizations also need to develop and implement comprehensive information security policies. These policies cover access management, device usage, data protection, and incident response procedures. Clear and structured policies will help create a

security culture within the organization. Putri et al. (2022) state that good security governance is a key foundation for cyber risk mitigation.

Furthermore, developing an incident response plan is a crucial step in ensuring an organization's readiness to face cyberattacks. This plan includes procedures for identifying, isolating, handling, and recovering systems post-incident. Benaichouba et al. (2024) stated that organizations with a well-developed response plan tend to be able to significantly reduce the impact of an attack. Furthermore, implementing a data backup strategy is also a crucial mitigation measure, especially when dealing with ransomware threats. Securely backed up data allows organizations to restore systems without relying on criminals. Rosidah et al. (2023) emphasized that data recovery systems are crucial for maintaining operational continuity.

In the face of increasingly sophisticated threats, organizations are also starting to adopt artificial intelligence-based technologies and machine learning to detect anomalies and attacks in real time. This technology enables systems to recognize new attack patterns and respond adaptively. Susanto et al. (2023) stated that the integration of AI in cybersecurity can significantly increase the effectiveness of threat detection. Finally, cross-sector collaboration is a crucial element in risk mitigation strategies. Cooperation between the government, the private sector, and the international community enables the exchange of information related to cyber threats and the strengthening of collective defense capacity. Sendjaja et al. (2024) emphasized that collaboration is key to building a resilient and sustainable cybersecurity ecosystem. Therefore, cybersecurity risk mitigation strategies must be designed holistically and adaptively, encompassing technological, human, and governance aspects. An integrated and sustainable approach will increase system resilience and ensure the continued operation of critical infrastructure and public services amidst the ever-evolving dynamics of cyber threats.

CLOSING

1. Conclusion

   Based on the discussion, it can be concluded that cybersecurity risk management plays a crucial role in protecting critical infrastructure and public services from increasingly complex digital threats. The risk identification process demonstrates that cyberthreats originate not only from external factors such as hackers and malware, but also from internal factors such as user negligence and system weaknesses. This confirms that cybersecurity is a shared responsibility

involving technological, human, and governance aspects. Risk evaluation is a crucial step in determining the priority level of handling, taking into account the likelihood of the risk occurring and its impact. Through this approach, organizations can allocate resources effectively to address the most critical risks. Meanwhile, risk mitigation strategies must be implemented comprehensively through the implementation of security technology, regular system updates, increased cybersecurity literacy, and the implementation of international policies and standards such as NIST and ISO 31000. In addition, the implementation of a risk management approach *Zero Trust Architecture*, the use of artificial intelligence, and strengthening cross-sector collaboration are crucial factors in increasing system resilience against cyberattacks. With an integrated and sustainable strategy, organizations can minimize the impact of attacks and ensure the continuity of public service operations. Therefore, a strong commitment from all stakeholders is needed to continuously improve cybersecurity capacity, through strengthening regulations, investing in technology, and developing human resources, to create a secure, resilient, and sustainable digital ecosystem.

2. Suggestion

Based on the research and discussion on cybersecurity risk management in critical infrastructure and public services, several suggestions can be used as recommendations to improve system resilience against cyber threats: First, the government needs to strengthen regulations and policies related to cybersecurity, particularly in protecting critical infrastructure and public data. Clear and mandatory security standards will help create a more secure and controlled system. Second, organizations need to regularly conduct cybersecurity training and education for employees. Increasing digital literacy and security awareness is key to reducing risks caused by human error. Third, government agencies and related organizations are advised to adopt advanced security technologies such as Next-Generation Firewalls (NGFWs), intrusion detection systems, and artificial intelligence for real-time threat detection.

BIBLIOGRAPHY

1. Adegbite.At.Al (2023) Review Of Cybersecurity Strategies In Protecting National Infrastructure: Perspectives From The Usa. Computer Science & It Research Journal, Volume 4, Issue 3, 200-219. 10.51594/Csitrj.V4i3.658
2. Aditya, A. R. M,dkk (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator). Global Political Studies Journal. Volume 6 Nomor 1 . DOI DOI 10.34010/gpsjournal.v6i1

3. Briliyant, O. C., & Ashari, R. A. (2018). *Rencana penerapan cyber-risk management menggunakan NIST CSF dan COBIT 5*. Jurnal Sistem Informasi (Journal of Information System), 14(2).
4. Chisty,dkk. (2022). Strategic Approaches to Safeguarding the Digital Future: Insights into Next-Generation Cybersecurity. Engineering International, Volume 10, No. 2
5. Daniel, S. A., & Victor, S. S.(2024). Emerging Trends In Cybersecurity For Critical Infrastructure Protection: A Comprehensive Review Computer Science & IT Research Journal, Volume 5, Issue 3,
6. Jose (2021). Politisasi Agenda Keamanan Siber Pada Era Industri 4.0 di Forum Multilateral POPULIKA/Vol. 9 No. 2 T hal.70-85
7. Khairunnisa,dkk.(2024). Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI: Studi Kasus di Indonesia. (2024). *Teknik: Jurnal Ilmu Teknik Dan Informatika*, *4*(2), 9-16. https://doi.org/10.51903/teknik.v3i1.570
8. Mahendra, V., & Soewito, B. (2023). Penerapan Kerangka Kerja NIST Cybersecurity dan CIS Controls sebagai Manajemen Risiko Keamanan Siber. *Techno.COM*, 22(3), 527-538.
9. Prabaswari, Alfikri & Ahmad. (2022). Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah . Matra Pembaruan, 6(1), 1 https://doi.org/10.21787/mp.6.1.2022.1-13
10. Purnomo Widyanto Pudyo,Dkk (2023). Study Of The Influence Of Legal Security And Cyber Intelligence Capacity On Strengthening Governance Of Cyber Defense In Indonesia. Rjoas: Russian Journal Of Agricultural And Socio-Economic Sciences. Issn 2226-1184 (Online) | Issue 12(144)
11. Putri, E.A. Pratama, G.A. & Fithri, B.S. (2023). Keamanan Nasional dalam Menghadapi Perubahan Cyber Warfare. Jurnal Mercatoria, 16 (2): 201-208.
12. Sasmito, G. W., Nishom, M., & Wibowo, D. S. (2020). Studi Mengenai Kejahatan dan Keamanan Internet bagi Guru dan Siswa SMK Muhammadiyah Bulakamba. *E-DIMAS: Jurnal Pengabdian kepada Masyarakat*, 11(3), 267-273.
13. Setiyawan,dkk. (2020). Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia. Jurnal USM Law . Vol 3 No 2. e-ISSN : 2621-4105
14. Susanto, E., Antira, L., Kevin, K., Stanzah, E., & Majid, A. A. (2023). *Manajemen keamanan cyber di era digital*. Jurnal Bisnis dan Kewirausahaan (Journal of Business and Entrepreneurship), 11(1), 23–33. https://doi.org/10.46273/job&e.v11i1.365
15. Syafi'i, dkk.(2023). Kajian Ilmu Pertahanan dalam Strategi Pertahanan Negara Guna Menghadapi Ancaman Teknologi Digital di Indonesia. Journal on Education. Volume 05, No. 02, 4063-4076
16. Theodorus Sendjaja (2024). Cybersecurity In The Digital Age: Developing Robust Strategies To Protect Against Evolving Global Digital Threats And Cyber Attacks. International Journal of Science and Society, Volume 6, Issue 1

17. Umida Saydazimova,dkk. (2025). Cybersecurity Threat Models and Linguistic-Pedagogical Approaches in Korean Critical Infrastructure Education. Journal of Internet Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 285-296.
18. Vu,dkk. Two-phase modeling and performance evaluation of plate heat exchangers in ejector refrigeration systems with low-GWP refrigerants.
19. Yulisuyanti,Eka & Benfano Soewito (2023). Model Manajemen Risiko Sistem Informasi Untuk Sistem Informasi Manajemen Kepegawaian. Techno.COM, Vol. 22, No. 3, Agustus 2023: 783-795