JOURNAL LA MULTIAPP

VOL. 06, ISSUE 04 (1193-1183), 2025
DOI: 10.37899/journallamultiapp.v6i5.2469

Cyber Security Challenges and Solutions in Critical Infrastructure: A Systematic Review of Threat Spectrum, Systemic Vulnerabilities, and Multi-Level Protection Strategies

Andi Dengkeng[1], Agus Halid[1], Gita Pratiwi[1], Andi Ikmal Rachman[1], Suriansyah B[1], Luqman fanani MZ[1]

[1]*Almarisah Madani University, Indonesia*

**Corresponding Author: Andi Dengkeng*
Email: andi.dengkeng@univeral.ac.id

Article Info

Article history:
Received 22 July 2025
Received in revised form 18 August 2025
Accepted 13 September 2025

Keywords:
Security Cyber
Infrastructure Critical
Threat Cyber
Vulnerability Systemic
Multi-Level Protection
Review Systematic
Strategy Mitigation

Abstract

Digital transformation has increased operational efficiency infrastructure critical, but at the same time also open new loophole against attack increasingly complex and destructive cyberspace. This study aims to identify spectrum threat cyber targeting infrastructure critical, analyzing vulnerability accompanying systemic, as well evaluate strategy multi-level protection used in mitigation risk cyber. Using approach qualitative through review methods systematically, this study examines 20 primary sources in the form of scientific journals, policy reports, and studies. case international published 2015–2024. The research results revealed that threats such as ransomware, Advanced Persistent Threats (APT), attacks AI -based, and zero-day exploits are becoming a form of attack dominant, with energy, health, and communications sectors as the main targets. Vulnerabilities systemic found in aspects of old technology that is not updated, governance weaknesse, as well as low awareness cyber at the level operational. Strategy effective protection nature layered, including perimeter security, access management, data encryption, training awareness, to response incidents and system recovery. This study recommends integration strategy adaptive, data -based protection risk, and supported by policies strong national to strengthen resilience cyber sector infrastructure critical.

Introduction

Development digital technology has bring significant impact on various sector infrastructure critical sectors, including energy, transportation, water, health, finance, and communications. Digitalization in these sectors not only increases efficiency and speed operational, but also introduces new challenges related to security cyber. Dependence on digital systems creates vulnerabilities that can be exploited by malicious actors through attacks cyber, which can cause widespread disruption and crisis national (Sitanggang, 2024).

Example real from This threat can be seen in the ransomware attack targeting the Colonial Pipeline in the United States in 2021, which caused material distribution disruption burn in the east area US seas. This incident shows how the infrastructure critical can be threatened consequence vulnerability cyber, resulting from inadequate systems protected (Gunawan & Pane, 2024). Attacks BlackEnergy which causes blackout electricity massive in Ukraine in 2015 emphasized risk serious challenges faced by energy infrastructure. Both This example shows that the attack cyber is not threats of a nature hypothetical, but rather reality that could

ISSN: 2716-3865 (Print), 2721-1290 (Online)

result in the domino effect is not only on the sector being attacked, but also on the economy and society as a whole (Putri & Wisudanto, 2017).

On the side others, developments digital infrastructure and security Cyber is also very important in increasing the resilience and effectiveness of the system. Assurance data security and strengthening system architecture is the steps that need to be taken to reduce risk attack cyber (Hermawan, 2024; Sun et al., 2017). With strengthen infrastructure security and implement collaboration intersectoral, we can minimize impact from targeted attack infrastructure critical. Research shows that the approach holistic that combines physical and digital aspects enables infrastructure critical to be more adaptable in facing modern challenges (Saluky, 2018).

In an increasingly connected digital era, infrastructure critical —such as energy systems, transportation, services health, finance, and communications —are prime targets. attack cyber. These infrastructures are bone back activity social, economic, and governmental, so that disturbance to the system can cause impact wide, including the disappearance vital services, loss financial big, to the point of threat to public safety. Improvement the complexity of digital systems and dependence on technology information has create spectrum threat increasingly broad and sophisticated cyberspace, starting from malware and ransomware to targeted Advanced Persistent Threat (APT) attacks.

One of challenge main in maintaining security cyber infrastructure critical is the existence of vulnerability systemic which is often difficult to detect and control. This vulnerability does not only originate from from weakness technical in device hardware and devices soft, but also includes human factors, management processes, and limitations in existing policies and regulations (Coventry & Branley -Bell, 2018). For example, Coventry and Branley -Bell highlight that the lack of funding for security cyber and expertise in this area in the sector health can worsen condition security, make many fixed systems prone to to attack cyber (Coventry & Branley -Bell, 2018).

Infrastructure system critical many still rely on legacy systems, such as SCADA and Industrial Control Systems (ICS), which were not designed to withstand threat modern cyber. Research by Radoglou-Grammatikis shows that these systems use the protocol insecure communications, so making them very vulnerable to manipulation external (Radoglou-Grammatikis et al., 2022; Radoglou-Grammatikis et al., 2021). This further enlarges potential risk, and as noted by Hadžiosmanović et al., it is important to implement strategy defense layered which combines technical, procedural, and improvement awareness source human resources in order to oppose threat cyber (Malihah, 2022).

Furthermore, there are misalignment between strategy security cyber and risk management organization, as stated by García-Pérez et al. This causes Lots company provider service critical failed building an integrated and effective protection system (García-Pérez et al., 2021). Various effort protection has developed to handle these issues, including implementation strategy security layered that utilizes threat analysis and strengthening techniques infrastructure use create a stronger defense to attacks (Radoglou-Grammatikis et al., 2019). Mkhwanazi and Futcher also stressed government 's responsibility to protect infrastructure information critical at the level national, which includes the implementation of policies and practices more effective security (Mkhwanazi & Futcher, 2024).

Even though previous research contributions quite significantly, there are several gaps (research gaps) that are still not fully developed filled. First, some big the study only focuses on one dimension of the problem, for example type threats or technological aspects, without linking them comprehensively between spectrum threat, vulnerability systemic, and strategic effective protection. Second, the lack of study systematic approach that integrates technical and policy aspects in a security context cyber in the sector infrastructure critical cause gap

ISSN: 2716-3865 (Print), 2721-1290 (Online)

between theory and practice in the field. Third, there is no comprehensive conceptual framework that maps strategy multi-level protection based on characteristics each sector infrastructure, so that the approach applied is often of a generic and less effective.

Based on background background and identification of the gap, this study aims to conduct review systematic to challenges and solutions security cyber in the sector infrastructure critical. Specifically, this study aims to identify and classify spectrum threat the most relevant cyber to infrastructure critical, analyzing vulnerability systemic that emerges from both side technology, resources human resources, as well as policies, as well as evaluate effectiveness strategy multi-level protection that has been developed or implemented in global literature and practice. This research is also expected to produce a framework conceptual which can be a reference for the maker policy, manager infrastructure, and practitioners security cyber in formulating approach mitigation more adaptive, comprehensive and sustainable risk management. With Thus, the results of this study are expected to provide a contribution real to improvement resilience cyber national and protection to vital assets that form the foundation life modern society.

Methods

This research uses an approach qualitative by method review systematic review which aims to explore in depth spectrum threat, vulnerability systemic, as well as strategy multi-level protection in the context of security cyber on infrastructure critical. This approach was chosen Because relevant to understanding a complex and contextual phenomenon, especially related to the dynamics of digital threats that cannot be measured quantitatively. solely.

Research Design

This research design is of a exploratory-qualitative, which is directed at interpreting the findings from various source academic and practical use build a comprehensive understanding of the issues being researched. Researchers utilizing the Systematic Literature Review (SLR) method as a technique major in data collection and analysis. A review was carried out on journal articles, institutional reports official (such as NIST, ENISA, and the World Economic Forum), as well as studies case attack cyber large in the range of 2015 to 2024.

Data Source

Sources in this study consist of: 1) Scientific journal articles published in indexed databases such as Scopus, ScienceDirect, SpringerLink, and IEEE Xplore; 2) Policy reports and white papers from institution international such as NIST (National Institute of Standards and Technology)**,** ENISA (European Union Agency for Cybersecurity)**,** World Bank, and OECD; 3) Studies case real attack cyber to infrastructure critical (e.g. Colonial Pipeline, Stuxnet, SolarWinds).

Criteria inclusion is used for filtering relevant literature, namely publications within the last 10 years, discussing the topic of security cyber and infrastructure critical directly, as well as contain information about the type threat, vulnerability systemic, or strategic protection.

Data Analysis Techniques

Data was analyzed using techniques thematic analysis. Researcher identify themes main thing that appears from data, such as type threat, source vulnerability, as well as approach protection. This process is carried out in stages coding open, data categorization, and synthesis thematic. Every theme analyzed in depth to reveal relatedness between factor threats and strategies recommended mitigation.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Validity and Credibility

To maintain validity of data, researchers use techniques triangulation source, with compare findings from various type publication and authority. In addition, researchers also conduct expert review regarding the interim analysis results, in order to get input from practitioners or academics in the field security cyber.

Results and Discussion

Identification and Classification Threat Cyber to Infrastructure Critical

Threat cyber to infrastructure critical increasingly complex and varied along increasing interdependence of public and industrial systems to digital technology. Attacks do not only come from from individual or group actors criminals, but also from state actors who have geopolitical interests. Through the review systematic to a number of literature and international reports, this study identifies and classifies types threat the most common and most impactful cyber to sectors infrastructure critical.

Table 1. Classification Threat Cyber to Infrastructure Critical Based on Types, Actors, and Target Sectors

Type Threat Cyber	Description Technical	Dominant Actor	Attack Objectives	Target Sector	Example Case
Malware & Ransomware	malicious program that encrypts data/system and demands ransom	Group criminal / non-state	Finance, extortion	Energy, Health, Finance	Colonial Pipeline Attack (2021)
Advanced Persistent Threat (APT)	Attack cyber hidden and ongoing, usually for espionage	Nation-state actors	Espionage, sabotage	Military, Energy, Government	Stuxnet vs. Iran Nuclear (2010)
Distributed Denial of Service	Flooding the system with Then cross fake until the server crashes	Hacktivist / criminal	Disruption service	Telecommunications, Banking	Dyn DNS Attack (2016)
Insider Threat & Human Error	Leaks or sabotage by employees/internal, or human error	Internal (employees/ partners)	Data leaks, sabotage	All sectors	case (2013), email phishing
AI-based Attacks & Zero-Day	Attack automatic and exploitation unrecognized gap (zero-day)	Various (including AI-malware)	Exploitation of unprotected systems	All digital sectors	DeepLocker by IBM (2018 prototype)

Threat cyber to infrastructure critical is very diverse, both from side technique and also motivation attackers. The table above shows that attacks such as ransomware and APT are two the most frequently found and dangerous threats Because its wide -ranging and destructive effects. Energy and health sectors occupy most vulnerable position because it is very dependent on digital systems that cannot stop operating. In addition, the threat from within the organization (insider threat) becomes a challenge a separate thing that is often missed from supervision. On the side other, the emergence attack based on intelligence artificial and zero-day exploits indicate that the pattern threat Keep going develop, so that strategy protection must always be adjusted with development new technologies and modes of attack.

Threat Spectrum Cyber to Infrastructure Critical

Threat cyber to infrastructure critical not only growing in number, but also in level complexity and impact. Attacks can be carried out by various actors, both state and non-state, with various objectives such as sabotage, blackmail, espionage, and disinformation. Through the study

ISSN: 2716-3865 (Print), 2721-1290 (Online)

literature systematic against 20 primary sources such as scientific journals, policy reports, and studies global cases between 2015 and 2024, this study succeeded identify and classify type threat cyber main target sectors infrastructure critical.

Table 2. Threat Spectrum Details Cyber to Infrastructure Critical

Type Threat	Mechanism Attack	Lead Actor	The main purpose	Most Vulnerable Sectors	Example Real
Ransomware	System encryption, demanding Money ransom	Group criminal	Financial	Energy, Health, Government	Colonial Pipeline Attack (2021)
Advanced Persistent Threat	Infiltration term long, data espionage or sabotage	State actor	Intelligence / sabotage	Energy, Military, Communications	Stuxnet vs. Iran Nuclear (2010)
DDoS (Distributed DoS)	Flooding the server with traffic fake to paralysis	Hacktivist/ Non-state	Disruption service	Finance, Telecommunications	Attack Dyn DNS (2016)
Insider Threat	Leaks or sabotage by insiders	Employee/internal	Sabotage / leak	All sectors	case (2013), email phishing
Zero Day Exploits	Exploitation unpatched system loophole	State actors & criminals	System exploit	All digital sectors	WannaCry (2017) used a loophole EternalBlue
AI-driven Attacks	Adaptive malware uses AI to avoid detection	State actors & criminals	Espionage / sabotage	Infrastructure, IoT, Cloud	DeepLocker (AI-malware prototype by IBM, 2018)
Supply Chain Attacks	Infiltrate through third party vendors or software third	Advanced states/actors	System infiltration	Technology, Government	Attack (2020)

Classification results in table shows that the infrastructure critical face diverse threat cyber with increasingly sophisticated modes. Ransomware remains a threat dominant because of strong financial motives and convenience distribution. However, APT and supply chain attacks show significant increase in the geopolitical context, where countries use digital attacks as a tool of intelligence and sabotage. In addition, the threat from within the organization (insider threat) and exploitation gap (zero-day) security continues to be a challenge Serious because they often go undetected until damage occurs. Attacks AI -based which is starting developing also shows that the landscape the threat can no longer be handled with approach conventional only. With Thus, understanding of spectrum This threat is an important first step in designing strategy multi-layered and contextual protection.

Evaluation Strategy Multi-Level Protection on Infrastructure Critical

In facing the threat Cyber is increasingly complex and layered, many organizations and countries implement strategy multi-level protection (multi-layered defense) to maintain resilience infrastructure critical. This strategy involves integration various control technical, administrative, and human resources working at multiple levels from from detection early,

ISSN: 2716-3865 (Print), 2721-1290 (Online)

prevention, response, and recovery. This study evaluates various approach protection based on literature findings and study reports case from institution world security between 2015–2024. Focus evaluation includes effectiveness technical, coverage protection, and adaptability to new threat.

Table 3. Evaluation Strategy Multi-Level Protection for Infrastructure Critical

Layer Defense	Component Main Strategy	Purpose of Protection	Effectiveness (Literature)	Challenge Implementation	Reference Source
Perimeter Security	Firewall, IDS/IPS, segmentatio n network	Prevent unauthorized access	High for threat external	Prone to against insider threats & zero-day	Cardenas et al. (2011), Zetter (2015)
Application Security	Secure coding, patch management , vulnerability scanning	Reduce software exploitation	Medium – High	Dependence on patch cycles & vendors	Boyson (2014); IBM X-Force Report (2023)
Data Protection	Encryption, DLP (Data Loss Prevention), regular backups	Guard data confidentialit y & integrity	Tall	High bandwidth requirements & HR awareness	ENISA (2022); CSA Guidelines (2021)
Identity & Access Managemen t	MFA, Role-Based Access Control (RBAC), privilege restriction	Limit access for users only authorized	Tall	Resistance users & costs initial implementation	NIST SP 800-53; Microsoft (2020)
Human Awareness	Training security cyber, phishing simulation, SOP incident	Mitigation risk of human error	Variative (low – high)	Need training repetitive & cultural aware risk	Hadžiosmano vić et al. (2012); SANS Institute
Incident Response & Recovery	CSIRT Team, response playbook incident, offsite backup, BCP/DRP	Restore service post attack	High if tested routine	Lack of exercises & resources Power technical in the area	ISO/IEC 27035; NIST 800-61
Governance & Compliance	Policy security, internal audit, ISO/NIST compliance	Balance control & regulation	Currently	Overlapping overlap regulation & lack of integration between institution	OECD (2019); World Bank (2021)

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Evaluation to strategy multi-level protection shows that the effectiveness protection is highly dependent on the combination between layer defense, not on one approach single. Perimeter defenses such as firewalls and IDS are important to prevent access from outside, but not enough face internal threats or zero-day exploits. Layers such as access management and training users become crucial to prevent human error and insider threats. The most powerful strategies are found in organizations that are able to integrate response incidents and policies recovery in plan sustainability business (Business Continuity Planning). Although Lots strategy proven technically effective, challenges main lies in the implementation in the field, especially related to limitations budget, gap skills technical, and resistance culture to policy security. Therefore, adaptability and integration cross layers are key in building a protection framework a resilient and dynamic cyber in an era of ever-increasing digital threats develop.

Discussion

The results of the study show that the threat cyber to infrastructure critical nature complex, dynamic, and multidimensional, encompassing technical, institutional, and human behavioral aspects. These threats encompass more than just attack technical actors such as malware and Distributed Denial of Service (DDoS), but also involve strategic actors such as nations and groups. criminal organized running mission espionage and sabotage through Advanced Persistent Threats (APT) and attacks chain supply (supply chain attack) Villalón -Huerta et al. (2024) (Wang et al., 2021). In this context, APT is characterized by capabilities tall as well as source significant power of the perpetrator to penetrate infrastructure technology information from the organizations they target, often going undetected for long periods of time (Guillén et al., 2021; Yu et al., 2021).

Vulnerability systemic in infrastructure critical not only comes from from gap technical such as zero-day attacks, but also from weaknesses in governance, limited policy security, as well as lack of awareness and competence source human resources (Rubio et al., 2018; Lu et al., 2021). Many infrastructure systems, including SCADA and IoT in the energy and water sectors, still use legacy technologies that are not designed to cope with modern digital threats. Research by Guillén et al. shows that older cables and components can increase vulnerabilities, making systems weaker. to more sophisticated attacks (Wang et al., 2021).

In the context of protection, evaluation to multi-level defense strategy shows that there is no One approach single effective overall. On the contrary, it is needed integration various layer defense begins from perimeter security to response incidents and training programs awareness cyber (Katrakazas & Papastergiou, 2024; Hurst et al., 2014). Combination strategies such as access management based on role (RBAC), implementation data encryption, and formation team response incident security computer-assisted (CSIRT) has been shown to provide significant results in improving posture. security infrastructure critical, especially If supported by policy strong security and culture aware risk at level organization (Ani et al., 2019; Settanni et al., 2015).

With Thus, a multi-layered security approach should not only be considered as a solution technical, but also as a risk management framework strategic cyber for a country's vital infrastructure (Ahmad et al., 2019). This is important to maintain resilience and continuity services that are in accordance with characteristics sector and context of threats faced.

Implications from this research is the need shift policy security cyber from approach reactive to proactive and adaptive, with unite perspective technical and policy within one strategic framework national. Government, regulatory agencies, and managers infrastructure critical need to build capacity institutional and technical simultaneously, including through investment in human resource training, strengthening regulations, as well as cooperation cross sector. This research also encourages importance evaluation periodic to effectiveness strategy protection applied, as well as adoption approach based on risk in planning digital security.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

For those who take policy, these findings provide a basis scientific in formulating standard national security cyber sector infrastructure, while for practitioners, the results of this study serve as a reference in selecting and implementing strategy appropriate protection according to the threat context and system capabilities.

However However, this study has several limitations. First, the focus studies limited to secondary data through review literature, so it does not yet cover insight empirical directly from perpetrator industry or stakeholders. Second, the approach generalization to multi-level strategies can ignore characteristics specific to each sector infrastructure (eg. difference between electrical systems with the transportation system). Third, the nature threat cyber that continues change rapidly make this finding of a nature situational and need to be updated periodically. Therefore, the study advanced with approach mixed -method, including studies case in-depth and policy analysis across countries, is essential to produce more applicable and contextual recommendations in the future.

Conclusion

This study concludes that security cyber on infrastructure critical is issue strategic that requires attention comprehensive from various parties, considering its wide impact to stability national, public safety, and sustainability vital services. Threat spectrum cyber issues faced by the sector infrastructure critical is very diverse, starting from from ransomware, Advanced Persistent Threats (APT), Distributed Denial of Service (DDoS) attacks, to cyber attacks based on Artificial Intelligence and zero-day exploits. These threats do not only come from from criminal actors, but also from states and internal actors (insider threats), with objectives that include sabotage, espionage, blackmail, and disinformation.

Vulnerability systemic found spread across various levels, both in the form of weakness technical issues such as the use of outdated and unprotected systems, limitations policies and regulations, to the low awareness and capacity source human resources. Therefore, protection to infrastructure critical is not enough just by technology sophisticated, but need approach integrated and layered multi-level protection. Strategies such as perimeter security, data encryption, access management based on role, training awareness cyber, and preparedness response incident proven to be more effective If applied in an integrated and contextual manner according to the characteristics threats and protected sectors.

With Thus, the approach security resilient and sustainable cyber infrastructure critical must be built through a combination between strengthening technology, governance institutions, involvement of competent human resources, and policy national side in development capacity long term digital security length. This study confirms importance collaboration cross sectors and updates strategy adaptive protection to changes in the landscape threat global cyber.

References

Adegbite, A., Akinwolemiwa, D., Uwaoma, P., Kaggwa, S., Akindote, O., & Dawodu, S. (2023). Review of cybersecurity strategies in protecting national infrastructure: Perspectives from the USA. *Computer Science & IT Research Journal, 4*(3), 200–219. https://doi.org/10.51594/csitrj.v4i3.658

Ahmad, A., Webb, J., Desouza, K., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security, 86*, 402–418. https://doi.org/10.1016/j.cose.2019.07.001

Ani, U., Watson, J., Nurse, J., Cook, A., & Maples, C. (2019). A review of critical infrastructure protection approaches: Improving security through responsiveness to

ISSN: 2716-3865 (Print), 2721-1290 (Online)

the dynamic modeling landscape. *IET Conference Proceedings, 6*, 1–15. https://doi.org/10.1049/cp.2019.0131

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation, 34*(7), 342–353. https://doi.org/10.1016/j.technovation.2014.02.001

Cardenas, A. A., Amin, S., & Sastry, S. (2011). Research challenges for the security of control systems. In *Proceedings of the 3rd Conference on Hot Topics in Security (HotSec)* (Vol. 6, pp. 1–6).

Coventry, L., & Branley-Bell, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas, 113*, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

European Union Agency for Cybersecurity. (2022). *Threat landscape for supply chain attacks*. ENISA. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

García-Pérez, A., Sallos, M., & Tiwasing, P. (2021). Dimensions of cybersecurity performance and crisis response in critical infrastructure organizations: An intellectual capital perspective. *Journal of Intellectual Capital, 24*(2), 465–486. https://doi.org/10.1108/jic-06-2021-0166

Guillén, J., Rey, A., & Casado-Vara, R. (2021). Propagation of the malware used in APTs based on dynamic Bayesian networks. *Mathematics, 9*(23), 3097. https://doi.org/10.3390/math9233097

Gunawan, Y., & Pane, M. (2024). Responsibility for excessive infrastructure damage in attacks: Analyzing Russia's attack in Ukraine. *Petita Journal of Science Studies Law and Sharia, 9*(1). https://doi.org/10.22373/petita.v9i1.213

Hadžiosmanović, D., Bolzoni, D., & Hartel, P. H. (2012). A survey of insider attack detection research. *Computers & Security, 34*, 45–59. https://doi.org/10.1016/j.cose.2013.10.007

Hafiz, M. (2024). Impact of digital economy on social welfare in Indonesia. *Franchise, 1*(2). https://doi.org/10.61590/waralaba.v1i2.143

Hermawan, A. (2024). Peeking gap between the potential and challenges of big data in services guarantee social employment in Indonesia. *Jamsostek, 2*(2), 185–206. https://doi.org/10.61626/jamsostek.v2i2.59

Hurst, W., Merabti, M., & Fergus, P. (2014). A survey of critical infrastructure security. In *Critical Infrastructure Protection* (pp. 127–138). Springer. https://doi.org/10.1007/978-3-662-45355-1_9

IBM Security. (2023). *Threat intelligence index 2023*. IBM X-Force. https://www.ibm.com/reports/threat-intelligence

ISO/IEC. (2016). *ISO/IEC 27035: Information security incident management*. International Organization for Standardization.

Jadidi, Z., Pal, S., Hussain, M., & Nguyen, K. (2023). Correlation-based anomaly detection in industrial control systems. *Sensors, 23*(3), 1561. https://doi.org/10.3390/s23031561

Katrakazas, P., & Papastergiou, S. (2024). A stakeholder needs analysis in cybersecurity: A systemic approach to enhancing digital infrastructure resilience. *Businesses, 4*(2), 225–240. https://doi.org/10.3390/businesses4020015

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Lu, P., Hu, T., Hao, W., Zhang, R., & Wu, G. (2021). G-CAS: Greedy algorithm-based security event correlation system for critical infrastructure networks. *Security and Communication Networks, 2021*, 1–13. https://doi.org/10.1155/2021/3566360

Malihah, L. (2022). Challenges in efforts to overcome the impact of climate change and support sustainable economic development: A review. *Journal of Development Policy, 17*(2), 219–232. https://doi.org/10.47441/jkp.v17i2.272

Microsoft. (2020). *Zero trust security model*. https://docs.microsoft.com/en-us/security/zero-trust/

Mkhwanazi, T., & Futcher, L. (2024). National critical information infrastructure protection through cybersecurity: A national government perspective. *Proceedings of the 19th International Conference on Cyber Warfare and Security (ICCWS)*, 555–564. https://doi.org/10.34190/iccws.19.1.1987

National Institute of Standards and Technology. (2020). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). NIST. https://www.nist.gov/cyberframework

Organisation for Economic Co-operation and Development. (2019). *Good governance for critical infrastructure resilience*. OECD. https://www.oecd.org/governance/good-governance-for-critical-infrastructure-resilience.htm

Putri, E., & Wisudanto, W. (2017). Structure financing development infrastructure in Indonesia to support economic growth. *Science and Technology Journal of Proceedings Series, 3*(5). https://doi.org/10.12962/j23546026.y2017i5.3136

Radoglou-Grammatikis, P., Dalamagkas, C., Laggas, T., Zafeiropoulou, M., Atanasova, M., Zlatev, P., … & Sarigiannidis, P. (2022). False data injection attacks against low voltage distribution systems. In *Proceedings of the IEEE Global Communications Conference (GLOBECOM)* (pp. 1856–1861). https://doi.org/10.1109/globecom48099.2022.10000880

Radoglou-Grammatikis, P., Sarigiannidis, P., Giannoulakis, I., Kafetzakis, E., & Panaousis, E. (2019). Attacking IEC-60870-5-104 SCADA systems. In *Proceedings of the IEEE World Congress on Services*. https://doi.org/10.1109/services.2019.00022

Radoglou-Grammatikis, P., Sarigiannidis, P., Iturbe, E., Rios, E., Martinez, S., Sarigiannidis, A., … & Ramos, F. (2021). Spear SIEM: A security information and event management system for the smart grid. *Computer Networks, 193*, 108008. https://doi.org/10.1016/j.comnet.2021.108008

Rubio, J., Román, R., Alcaraz, C., & Zhang, Y. (2018). Tracking advanced persistent threats in critical infrastructures through opinion dynamics. In *International Conference on Critical Information Infrastructures Security* (pp. 555–574). Springer. https://doi.org/10.1007/978-3-319-99073-6_27

Saluky, S. (2018). Overview of artificial intelligence for smart government. *Information Technology Engineering Journals (ITEJ), 3*(1), 8–16. https://doi.org/10.24235/itej.v3i1.22

SANS Institute. (2018). *The importance of cybersecurity awareness training*. https://www.sans.org/white-papers/importance-cybersecurity-awareness-training/

Settanni, G., Skopik, F., Shovgenya, Y., Fiedler, R., Kaufmann, H., Gebhardt, T., … & Pentikäinen, H. (2015). A blueprint for a pan-European cyber incident analysis system. *Proceedings of the International Conference on Cyber Security* (ICS 2015). https://doi.org/10.14236/ewic/ics2015.9

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Sitanggang, M. (2024). Comparative analysis of cyber sovereignty in Southeast Asian countries, Australia, and New Zealand. *Journal of Social and Science, 4*(7), 653–664. https://doi.org/10.59188/jurnalsosains.v4i7.1477

Sun, C., Tang, Z., & Liu, D. (2017). Research on the integrated security supervision technology of cyber-physical systems in substations. *Destech Transactions on Computer Science and Engineering (CMEE)*. https://doi.org/10.12783/dtcse/cmee2016/5311

Villalón-Huerta, A., Ripoll, I., & Marco-Gisbert, H. (2024). Provisioning the external infrastructure for cyberspace operations: A spotlight on Russian APT groups. *International Journal of Information Security Science, 13*(2), 1–32. https://doi.org/10.55859/ijiss.1431064

Wang, G., Cui, Y., Wang, J., Wu, L., & Hu, G. (2021). A novel method for detecting advanced persistent threat attacks based on belief rule base. *Applied Sciences, 11*(21), 9899. https://doi.org/10.3390/app11219899

World Bank. (2021). *Cybersecurity capacity review: Securing critical infrastructure in developing economies*. https://www.worldbank.org/cybercapacity

Yu, K., Tan, L., Mumtaz, S., Al-Rubaye, S., Al-Dulaimi, A., Bashir, A., … & Khan, F. (2021). Securing critical infrastructures: Deep-learning-based threat detection in IIoT. *IEEE Communications Magazine, 59*(10), 76–82. https://doi.org/10.1109/mcom.101.2001126

Zetter, K. (2015). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown Publishing Group.

ISSN: 2716-3865 (Print), 2721-1290 (Online)