香港社會科學學報

HONG KONG JOURNAL OF SOCIAL SCIENCES

最新第 64 期 (2024 年秋/冬季) **Vol. 64 Autumn/Winter 2024**

Available online at www.hkjoss.com

Research article **https://doi.org/10.55463/hkjss.issn.1021-3619.64.11**

Designing Cyber-Defense System Using Soft System Methodology to Protect the Informatics Infrastructure in Defense Sector

Andi Sutomo* (https://orcid.org/0000-0001-7867-2438), Suyono Thamrin, Pujo Widodo, Yono Reksoprodjo

The Republic of Indonesia Defense University, Bogor, Indonesia

* Correspondence: radar.andisutomo@gmail.com

Abstract:

According to the Indonesian Ministry of Communication and Information, there has been an increase in the use of data-based digital technology, resulting in the exchange of data flowing beyond national borders and increasing the risk of cyber-attacks. This research aims to explore a cyber-defense system design to protect the informatics infrastructure of the defense sector. This study uses a quasi-qualitative approach with case studies on vital information infrastructure in the defense sector. Data were collected through in-depth interviews, observations, and document analyses. The data were analyzed using analysis techniques and a soft system methodology. The conclusion of this research is critical to protecting the vital information infrastructure of the national defense sector, and cross-sector and inter-governmental efforts are needed. This research contributes novel insights by identifying specific areas for investment, such as human capital development, advanced security technology, robust infrastructure, and enhanced international cooperation. Moreover, this study emphasizes the need for adaptability and a rapid response to emerging cyber threats.

Keywords:
Soft system methodology,
Cyber-attacks,
Cyber defense,
Vital information infrastructure
Defense sector

Article History:
Received: September 20, 2024
Revised: October 18, 2024
Accepted: October 26, 2024
Published: November 30, 2024

使用软系统方法设计网络防御系统以保护国防部门的信息基础设施

摘要:

据印度尼西亚通信和信息部称，基于数据的数字技术的使用有所增加，导致数据交换跨越国界，增加了网络攻击的风险。本研究旨在探索一种网络防御系统设计，以保护国防部门的信息基础设施。本研究采用准定性方法，对国防部门的重要信息基础设施进行案例研究。数据是通过深入访谈、观察和文档分析收集的。使用分析技术和软系统方法对数据进行分析。本研究的结论对于保护国防部门的重要信息基础设施至关重要，需要跨部门和政府间的努力。本研究通过确定具体的投资领域（如人力资本开发、先进的安全技术、强大的基础设施和加强的国际合作）提供了新颖的见解。此外，本研究强调了对新出现的网络威胁的适应性和快速反应的必要性。

关键词：软系统方法论、网络攻击、网络防御、重要信息基础设施, 国防部门

1. Introduction

The development of information technology has helped our lives in several positive ways. However, it has also influenced various aspects, including more complex competition between large countries for economic advantages, technological and security domination, regional conflicts due to global geopolitical dynamics, climate change and environmental issues, threats of terrorism, illegal trade, and disease spread. In terms of advances in information technology, automation benefitting from the Internet of Things increases efficiency but is vulnerable to cyber threats. The dynamics of the strategic environment continue to present significant challenges for national defense (Yanuarti, et al., 2020).

Setiyawan, Churniawan, and Faried (2020) stated that the world no longer views the military as the only potential threat. However, it is starting to pay attention to non-military threats, including cyber ones. Cyberspace can threaten a country because it can be used to steal information, propaganda, provocation, or attack information in various fields, such as banking, military, and national defense systems. As argued by Bahri (2020), cyberspace is a computerized and connected infrastructure in a country. This gives rise to parties who have negative goals (hackers and crackers) to disrupt the infrastructure system, which is computerized. However, these parties are no longer individuals but countries, referred to as cyber-attacks.

According to the Ministry of Communication and Information (KEMENKOMINFO, 2022), there was an increase in the use of data-based digital technology, resulting in the exchange of data flowing beyond national borders, which increases the risk of cyberattacks. In 2020, ransomware attacks increased by 105% and more than tripled the number of attacks in 2019. Cyber-attacks against institutions increased by 31% from 2020 to 2021, with the number of attacks per company (institution) averaging 206 per year to 270 attacks in 2021. The National Cyber and Crypto Agency (BSSN) also published the 2021 Cyber Security Monitoring Annual Report via the official website of the Directorate of Cyber Security Operations, precisely at Id-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center), from this report it can be seen that more than 1.6 billion or to be precise 1,637,973,022 traffic anomalies or cyber-attacks occurred throughout Indonesia in 2021 (Vimy et al., 2022). This shows that cyber-attacks can occur anytime and seriously endanger a country's vital information infrastructure.

In addition, cyber-attacks were carried out by the National Security Agency (NSA-US) against Indonesia by requesting assistance from the Australian Defense Signals Directorate (DSD) to spy on Indonesia during the UN Climate Change Conference in Bali on December 3–14 December 2007, wiretapping was carried out by the United States and Australia to monitor the security of Indonesia's communications network structure (Vimy et al., 2022). Cyber-attacks, as part of cyber warfare, often occur today and can result in considerable losses to the country. The facilities available in cyberspace can be misused to disrupt or paralyze a country's vital/critical infrastructure (Putra et al., 2020).

For this reason, problems related to cyber warfare strategies that need to be addressed include cyber threats that are developing very quickly, the identification of intruders, human resources, regulations and compliance with regulations, system and software vulnerabilities, cooperation, and monitoring (intelligence). Overcoming these problems requires cross-sector efforts, investment in expertise, security technology, robust infrastructure, inter-institutional and inter-state cooperation, adaptability, and rapid response to new threats. Solutions to these problems are the key to ensuring the security and protection of the vital information infrastructure of the National Defense

sector.

Based on this discussion, the ’vital information infrastructure of the Defense Sector must be protected to improve national defense. Further discussion will be provided in this research using the soft system methodology.

2. Literature Review

This research aims to explore a cyber-defense system design to protect the informatics infrastructure of the defense sector. This study uses a quasi-qualitative approach with case studies on vital information infrastructure in the defense sector.

2.1 National Defense System

The national defense system comprises the entire structure, policies, and procedures a country establishes to protect itself from external threats and aggression (Mardhani, 2020). The main objective of the national defense system is to maintain a country’s sovereignty, territorial integrity, and national security. State defense, also known as national defense, refers to all efforts to defend state sovereignty, the territorial integrity of a state, and the safety of the entire nation from threats and disturbances to the integrity of the nation and state.

According to Supriyatno (2014), the concept of national defense also involves the implementation of political policies into strategic defense policies, which are then packaged in several defense products. Therefore, the management aspects of national defense must be considered for the smooth implementation of a country’s defense system.

Indonesia, as a country that adheres to a universal defense system, can be interpreted as a defense system that mobilizes all national resources in the form of human, artificial, natural, and other asset sources. These resources are mobilized for national defense purposes, to protect Indonesia’s interests, to become a wealthy nation, and to participate in implementing world order based on freedom, eternal peace, and social justice. The implementation of *Sishankamrata* was a struggle for independence from 1945 to 1949, where armed and unarmed people’s forces rose together against colonialism and expelled Dutch colonists. The current challenge is to find a form of implementation in the modern state order of all the doctrines, systems, and orders that we have inherited since the physical struggle for independence (Suryokusumo, 2016).

2.2 Cyber Warfare Theory

Imperva (2002), a cyber-security software and services company in California, United States, defines cyber warfare as a cyber-attack or series of attacks targeting a country that can potentially damage government and civil infrastructure, disrupt other systems, and even potentially disrupt the country, even resulting in fatalities. Warta Ekonomi further defined cyber warfare as a cyber-attack carried out between countries or international organizations to attack and attempt to damage other countries’ computers or information networks through computer viruses or denial of service attacks and, as a result, espionage, sabotage, propaganda, and manipulation, including economic war (Warta Ekonomi, 2022).

Tampubolon (2019) explained that cyber warfare is an action by a state that penetrates another country’s network to cause damage or disruption. The trend of controlling a country by using asymmetric ‘weapons’ built systematically by utilizing advances in information technology and cyberspace, such as social media and cyber warfare, has become a strategy to cause losses that have a strategic impact on a country.

Chandra (2021) describes several methods of attack in cyber warfare. Cyber espionage is a form of collecting secret and sensitive information from individuals, competitors, rivals, other government groups, and enemies in the military, political, and economic fields. The method used is illegal exploitation via the Internet, networks, software, and/or computers of other countries. Confidential information that is not handled by security is a target for interception and alteration.

2.3 Vital Information Infrastructure Theory

According to Wilson (2014), with all of its facilities, vital information infrastructure is used to control or manage telecommunications, air transportation, the financial sector, networks, electric power, and other services directly related to the economy and daily activities. This vital information infrastructure is vulnerable to cyber-attacks in the form of espionage or sabotage via cyberspace. Along with the development of technology, information, and communication, the digitalization of vital infrastructure that accommodates essential sectors of modern society, such as the defense sector, is increasing. Luiijf (2016, as quoted in Robbani 2020) states that critical information infrastructure is not only related to information system security, but also to cyber security as a whole, including the effects of cyber security on the physical, cyber, and human dimensions, including organizations that rely on technology, whether technology information, industrial control systems, cyber-physical systems, and the Internet of Things (IoT).

National Vital Infrastructure is a physical and non-physical infrastructure that has a crucial function in supporting the livelihoods of many people, and if there is disruption, damage, and destruction to the infrastructure, it will have an impact on national defense and security, national economy, health, public safety, state administration, public services, damage to the country’s reputation, loss of public trust, and other impacts in the form of a combination of these. Currently, information infrastructure is determined by

many vital infrastructure elements, and ICT includes everything that connects infrastructure systems and combines them so that they are equal and interdependent (Ervianto, 2017).

3. Research Methodology

This study uses a qualitative approach. Qualitative research is a research method based on post-positivism and is used to research the condition of natural objects, where the researcher is the key instrument, data source sampling is carried out purposively, the collection technique is triangulation, data analysis is inductive/qualitative, and the results of qualitative research emphasize meaning rather than generalization. Qualitative research relies on a holistic natural background, positions humans as research tools, carries out inductive data analysis, prioritizes the process rather than the results, and the research results are agreed upon by the researcher and research subjects (Sugiyono, 2020).

4. Results and Discussion

4.1 Cyber Regulation

In an ever-changing global landscape, where the physical borders of countries are becoming increasingly irrelevant in the face of advances in information technology, cyber defense has evolved into a critical domain in national security strategies. The existence of vital information infrastructure and systems that support various essential sectors, such as energy, finance, transportation, and especially defense, is the center of attention, considering their vulnerability to cyber-attacks. The challenge of protecting these assets is a complex task; it is an endeavor that requires strategic planning, multidisciplinary coordination, and precision execution.

This causes national borders to become biased, especially in cyber matters, which are driven by unformed technological development. To overcome this and protect the country and its citizens, a country must create policies that regulate, bind, and protect its citizens. Policies and regulations related to risk management and risk-management-based cyber defense strategies are very important for protecting defense information infrastructure and supporting national defense. Laws and government regulations that specifically regulate cyber defense in Indonesia are also necessary, because society and the country are increasingly dependent on information technology and complex digital infrastructure.

With increasingly sophisticated and diverse cyber threats, there is a need for a strong legal framework to protect the vital information infrastructure in the defense sector. This regulation provides a legal basis for preventive action, detection, and response to cyber-attacks. The vital information infrastructure in the defense sector is a critical infrastructure that plays a crucial role in national security. Regulations help to develop the security measures needed to protect this infrastructure from cyber-attacks that could harm national interests.

With the existence of regulations regarding cyber defense in Indonesia, awareness of the importance of cyber security can increase, and organizations in the defense sector are believed to be able to comply with good security practices. This regulation will clearly regulate procedures for handling security incidents and responding to cyber-attacks. This will significantly help minimize the impact of attacks and accelerate recovery.

4.2 Defense Sector Vital Information Infrastructure

Cyber security threats continue to develop and become more sophisticated, including ransomware, phishing, and malware attacks; therefore, organizations must be able to effectively manage cyber security risks and protect their sensitive data. According to Akmal (2008) organizations, including the banking industry, are often weak in implementing Good Corporate Governance (GCG) and risk management, where risk management is one of the most important parts of organizational activities, which manages important data and is a component that must be improved to realizing GCG itself.

Although cyber defense is not yet as popular in Indonesia as it is in developed countries such as the United States, Australia, and Singapore, it is still necessary to immediately define what is meant by the defense sector vital information infrastructure in Indonesia and what is included in it. The defense sector's vital information infrastructure includes various elements and systems that are very important for maintaining the continuity of operations and national security, including Command and Control Systems, Network Infrastructure, Defense/Military Data and Information Centers, Intelligence Information Systems, Global Navigation and Positioning Systems (GPS), Cyber Defense and Security, Military Logistics Network, Radar and Sensor Systems, Weapon Systems, Ammunition and IT Hardware, Emergency Command Center, and other related institutions, such as police, which have the task of investigating, arresting, and prosecuting cybercriminals, including cyber-attacks such as hacking, data theft, online fraud, and other cyber-attacks.

Regarding cyber resilience, protecting vital information infrastructure in the defense sector in Indonesia is still faced with various challenges in terms of cyber security and defense, including cyber-attacks, which continue to increase both in terms of frequency and complexity; awareness of the importance of cyber security, which still requires education and training; policies and regulations regarding the protection of vital infrastructure and sensitive data that still need

development; the need for international and national collaboration in terms of exchanging information about cyber threats and countering attacks; and the availability of trained human resources in the field of cyber security. Cyber resilience is an ever-evolving global challenge, and rapid changes in technology and cyber threats mean that it is constantly evolving. Therefore, it is important to continue monitoring developments and adapting to changes to increase cyber resilience in Indonesia, especially within the ranks of the Ministry of Defense.

4.3 The Analysis by Soft System Methodology

In this research, the design of a Cyber Defense System to Protect the Defense Sector's Vital Information Infrastructure was analyzed using a Soft System Methodology (SSM).

SSM is a qualitative research analysis methodology developed by Peter Checkland in the 60s. SSM is an analytical method that uses a systematic way of thinking and focuses on humans (systems thinking). SSM begins by looking for P (real-world problem situation) or problems in a situation and the characteristics of interventions to improve these problems so that F (theoretical framework) and A (contribution/novelty/state of the art) are needed. Then, mapping of all actors as stakeholders was carried out, including CPO (Client, Practitioner, Owner of the Issue Addressed) and CATWOE, which aimed to solve this problem.

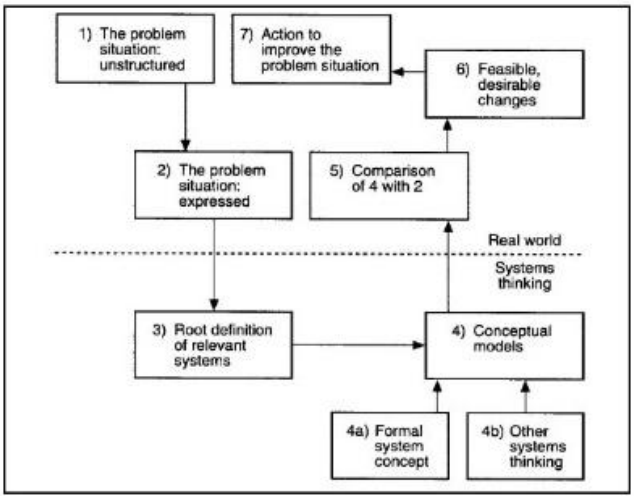

Figure 1. Seven steps of soft system methodology (SSM). Source: Checkland & Scholes (1990)

The data analysis process through SSM is carried out by categorizing problems in analysis boxes so that they can be understood more easily (Checkland & Scholes, 1990). The data analysis using SSM consists of seven stages (Figure 1).

4.3.1. Analysis One (Intervention)

Clients were parties with a direct intervention role in the research being conducted. The Clients (C) of this research are the researcher (Andi Sutomo) and Promoter I (Rear Admiral TNI (Ret.) Dr. Drs. Ir. Suyono Thamrin, M. Eng. Sc., CIQnR., CIQaR., IPU., ASEAN.Eng., CIPA, CIMMR., ACPE)) and Co Promoters 1 and 2 (Maj. Gen. TNI Dr. Ir. Pujo Widodo, S.E., S.H., S.T., M.A., M.Si., M.D.S., M.Si(Han) and Dr. Yono Reksoprodjo) which is an academic group and is under the auspices of the Defense University. Supervisor I (Client I) has the authority to intervene in clarifying the problem formulation according to the research topic. Supervisor II (Client II) provides an intervention to formulate the research questions as a derivative of the problem formulation.

Practitioners are parties who conduct studies or research using SSM; in this research, (P) is the researcher (Andi Sutomo). Owners (O) are the instruments involved either as regulators or operators, namely, the Ministry of Defense and BSSN.

4.3.2. Analysis Two (Social)

The categories created based on the roles in the context of this research are regulators, operators, and observers.

1) Regulator Group: In this group are the actors who directly influence policy/regulations, namely the Ministry of Defense and BSSN.

2) Operator Group: This group includes actors who are affected by the policies issued by the Regulator Group and implement these policies. In the context of this research, the operators were the Ministry of Defense and the BSSN.

3) Observer Group, namely actors who are not directly involved but also monitor and review policies and activities, and provide input to the Regulator and Operator Group. In the context of this research, the Observer Group includes BRIN (National Research and Innovation Agency), UKI (Christian University of Indonesia), and the Republic of Indonesia Defense University academics.

The norm element at the SSM stage is to explain how the criteria, standards, and provisions apply to roles and behavior in accordance with their roles. These norms are based on several documents that serve as legal guidelines, such as Law No. 3 of 2002 concerning National Defense, Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE), National Cyber and Crypto Agency Regulation Number 10 of 2021 concerning Amendments to National Cyber and Crypto Agency Regulation Number 5 of 2020 concerning the Agency's Strategic Plan National Cyber and Cryptocurrency 2020-2024, and Law 11/2008 and PP 82/2012 as the Basis for Cyber Security and Universal Cyber Defense.

Meanwhile, informants believed that the value elements in this research strengthen cyber defense strategies based on risk management to strengthen the national defense system.

4.3.3. Analysis Three (Politics)

Political analysis is believed to determine what can or cannot be performed. The disposition of power in this research is that the Ministry of Defense and BSSN are cyber defense policy makers to strengthen the country's defense system. Meanwhile, the Ministry of Defense is an institution that has created the National Defense System. In this case, cyber and national defenses are interrelated and support each other. The nature of power in this study occurs in a military hierarchy based on two aspects: position and rank. The nature of power between the Ministry of Defense and BSSN is a coordinative system.

Systems Thinking Cyber Defense System Design to Protect the Defense Sector's Vital Information Infrastructure Using the following Soft System Methodology:

Table 1. Root definition (developed by the authors)

Root Definitions	**Research Questions (in statement form)**	***Relevant System***
RD 1	Design effective cyber defense systems to protect vital information infrastructure in the defense sector	Design a cyber-defense system (P) by looking for an effective system (Q) to protect the vital information infrastructure of the national defense sector (R).

Meanwhile the CATWOE analysis of the RD above is as follows:

Table 2. CATWOE and 3E analysis (developed by the authors)

RD-1	Develop a risk factor model that influences cyber defense strategy (P) based on risk management (Q) to protect the vital information infrastructure of the national defense sector (R).
	CATWOE ANALYSIS
C (*Customer*)	Ministry of Defense, BSSN, BRIN, CSIRT.ID, and Defense University and UKI Academics
A (*Actor*)	Ministry of Defense and BSSN
T (*Transformation*)	Develop a risk factor model that influences a risk management-based cyber defense strategy to protect the vital information infrastructure of the national defense sector.
W (*Worldview*)	Strong cyber defense will affect the country's defense system.
O (*Owner*)	BSSN and Ministry of Defense
E (*Environment*)	Limited IT and human resources, global IT developments and the dynamics of technological developments and increasingly unstoppable cyber-attacks.
	CRITERIA 3E
Efficacy	Develop a model of risk factors that influence cyber defense strategies by involving all stakeholders to protect the vital information infrastructure of the national defense sector.
Efficiency	Collaborating with all parties from policy makers, government, private sector, academics and society to improve cyber defense to protect the vital information infrastructure of the national defense sector.
Effectiveness	Develop a model of risk factors that influence cyber defense strategies to protect the vital information infrastructure of the national defense sector.

The next stage of SSM is to form a conceptual model (the fourth stage of the seven stages of SSM) by connecting all the activities that will be carried out to carry out the T process (in the CATWOE analysis table), so that it becomes a complete system, as follows:

Table 3. Conceptual model and activities of RD (developed by the authors)

RD-1	**Activity**	**Activity Description**
Develop a risk factor model that influences cyber defense strategy (P) based on risk management (Q) to protect the vital information infrastructure of the national defense sector (R).	Activity 1	Realizing that the risk factors that influence a cyber-defense strategy based on risk management need to be developed to protect the vital information infrastructure of the national defense sector.
	Activity 2	Understanding cyber defense strategies has risk factors that need to be identified to protect the vital information infrastructure of the national defense sector.
	Activity 3	Identifying risk factors that influence risk management -based cyber defense strategies.
	Activity 4	Formulate risk factors that influence risk management -based cyber defense strategies.
	Activity 5	Conduct research related to risk factor models that influence cyber defense strategies based on risk management.
	Activity 6	Develop a model of risk factors that influence cyber defense strategies based on risk management to protect the vital information infrastructure of the national defense sector.

The next stage (the fifth of the seven stages of SSM) is a comparison of the conceptual model with the reality found in the real world, namely, findings in the field during data collection, which is carried out to compare models and the real world.

Table 4. Comparison of RD conceptual models (developed by the authors)

No	**Activity**	**Implementation**	**Actors**	**Probable development**
1	Realizing that risk factors that influence cyber defense strategies based on risk	Implemented	Ministry of Defense, BSSN, BRIN,	Increase public awareness that these risk factors are not only for the government, but are

	management need to be developed to protect the vital information infrastructure of the national defense sector.		CSIRT.ID, and Defense University and UKI Academics	the responsibility of all parties.
2	Understanding cyber defense strategies has risk factors that need to be identified to protect the vital information infrastructure of the national defense sector.	Implemented	Ministry of Defense, BSSN, BRIN, CSIRT.ID, and Defense University and UKI Academics	It is necessary to formulate new strategies that are in line with the demands of current developments and in line with the increase in cyber-attacks.
3	Identify risk factors that influence risk management-based cyber defense strategies.	Implemented	Ministry of Defense, BSSN, BRIN, and Academics	The identification carried out must be based on valid data and information, so it needs to involve many parties.
4	Formulate risk factors that influence risk management -based cyber defense strategies.	Implemented	Ministry of Defense, BSSN, BRIN, and Academics	The formulation of risk factors needs to be tested and information continuously updated in line with developments in global, regional and national dynamics.
5	Conduct research related to risk factor models that influence cyber defense strategies based on risk management.	Implemented	Ministry of Defense, BSSN, BRIN, and Academics	Research results should be developed and synergized between related institutions/parties.
6	Develop a model of risk factors that influence cyber defense strategies based on risk management to protect the vital information infrastructure of the national defense sector.	Not implemented	Ministry of Defense, BSSN, BRIN, and Academics	This needs to be done regularly and in a measured manner by paying attention to all aspects that influence the national defense strategy to protect the vital information infrastructure of the national defense sector.

Based on the results of the SSM analysis, it was found that the most important aspects that have not been carried out in the field are developing risk factor models that influence cyber defense strategies based on risk management to protect the vital information infrastructure of the national defense sector. This is related to national cyber defense which has a comprehensive influence on national defense.

Therefore, the preparation of a Cyber Defense System Design to Protect the Defense Sector's Vital Information Infrastructure Using Soft System Methodology in the future must be based on this.

5. Conclusion

Research has proven the protection of the vital information infrastructure of a country's defense sector. In addition, overcoming cyber problems requires cross-sector efforts, investment in expertise, security technology, and strong infrastructure as well as inter-agency and inter-country cooperation, including adaptability and rapid response to new threats. Preparing a Cyber Defense System Design to Protect the Defense Sector's Vital Information Infrastructure must be prepared by considering the risk factors that influence the cyber defense strategy based on risk management to protect the vital information infrastructure of the national defense sector.

Cyber-attacks not only look for technical weaknesses, but also target the defense sector's vital information infrastructure. Therefore, protection of this infrastructure is crucial for maintaining the integrity of a country's defense. From this research, we hope to develop cyber defense strategies that are adaptive and responsive to cyber threats and attacks. Concrete steps are needed that will involve identifying risks, developing security policies, implementing the latest security technology, and strengthening cyber-defense capabilities.

This research offers practical recommendations for cyber defense, such as identifying risks, developing security policies, implementing the latest technology, and strengthening cyber defense capabilities. This study provides valuable insights for practitioners and policymakers.

Author Contributions

Conceptualization, A.S.; methodology, S.T.; software, P.W.; validation, Y.R.; formal analysis, P.W.; investigation, S.T.; resources, A.S.; data curation, Y.R.; writing—original draft preparation, all authors contributed equally; writing—review and editing, Y.R.; visualization, P.W.; supervision, A.S.; project administration, S.T. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Data Availability Statement

The original contributions presented in this study are included in the article.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] AKMAL, H. (2008). *Good Corporate Governance dan Managemen Risiko di Bank Sharia*. Yogyakarta: Program Pascasarjana UIN Sunan Kalijaga.

[2] BAHRI, I.S (2020). *Cyber Crime Dalam Sorotan Hukum Pidana*. UGM.

[3] CHANDRA, S. (2021). Combating China's Political Warfare: An American Analysis. *National Security*, 4(2), 168–175.
[4] CHECKLAND, P., & SCHOLES, J. (1999). *Soft systems methodology in action*. John Wiley & Sons.
[5] ERVIANTO, W. I. (2017). Tantangan pembangunan infrastruktur dalam proyek strategis nasional Indonesia. *Simposium II UNIID 2017*, 2(1), 98–103.
[6] IMPERVA (2002) What is Cyber Warfare? Examples, Types, Mitigation. Available on htpps://www.imperva.com/learn/application-security/cyber-warfare/
[7] KEMENKOMINFO. (2022). *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik* (2nd ed.). Kementerian Komunikasi dan Informatika Indonesia.
[8] MARDHANI, D. (2020). Keamanan Dan Pertahanan Dalam Studi Ketahanan Nasional Guna Mewujudkan Sistem Keamanan Nasional. *Jurnal Pertahanan Dan Bela Negara*, 10(3), 279–298.
[9] PUTRA, D. A., SARAGIH, H. J. R., & DEKSINO, G. R. (2020). Implementasi Manajemen Risiko Pertahanan Siber Kementerian Pertahanan Untuk Mendukung Pertahanan Negara. *Manajemen Pertahanan: Jurnal Pemikiran Dan Penelitian Manajemen Pertahanan*, 6(1).
[10] ROBBANI, K. S., REKSOPRODJO, A. H. S., & BASTARI, B. (2020). Perlindungan infrastruktur informasi kritikal nasional sektor ketenagalistrikan dari ancaman siber. *Peperangan Asimetris*, 6(1), 65-88.
[11] SETIYAWAN, B.M., CHURNIAWAN, E., & FARIED, F.S. (2020). Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia. *Wahyu Prananda Jurnal USM Law Review*, 3(2), 286-287.
[12] SUGIYONO. (2020). Metode Penelitian Kualitatif. Alfabeta.
[13] SUPRIYATNO, M. (2014). *Tentang Ilmu Pertahanan*. Jakarta: Yayasan Pustaka Obor Indonesia.
[14] SURYOKUSUMO, S. (2016). *Konsep Sistem Pertahanan Nonmiliter: Suatu Sistem Pertahanan Komplemen Sistem Pertahanan Militer Dalam Pertahanan Rakyat Semesta*. Yayasan Pustaka Obor Indonesia.
[15] TAMPUBOLON, K. E. A. (2019). Perbedaan Cyber Attack, Cybercrime dan Cyber Warfare. *Jurisdiction*, 2(2), 539-554.
[16] VIMY, T., WIRANTO, S., RUDIYANTO, R., WIDODO, P., & SUWARNO, P. (2022). Ancaman Serangan Siber Pada Keamanan Nasional Indonesia. *Jurnal Kewarganegaraan*, 6(1), 2319-2327.
[17] WARTA EKONOMI (2022) Apa Itu Cyberwarfare? Available on https://wartaekonomi.co.id/read452254/apa-itu-cyberwarfare?page=all
[18] WILSON, C. (2014). Cyber Threats to Critical Information Infrastructure. In THOMAS, L. J., & Chen, N. (Eds.) *Cyberterrorism: Understanding, Assessment, and Response*. Chapter 7 (pp. 123-136). London: Springer-Swansea University. http://doi.org/10.1007/978-1-4939-0962-9_7.
[19] YANUARTI, I., WIBISONO, M., & MIDHIO, I. W. (2020). Strategi Kerja Sama Indo-Pasifik Untuk Mendukung Pertahanan Negara: Perspektif Indonesia. *Jurnal Strategi Perang Semesta*, 6(1), 41-70.

参考文:

[1] AKMAL, H.（2008）。伊斯兰教法银行拥有良好的公司治理和风险管理。日惹：UIN Sunan Kalijaga 研究生课程。
[2] BAHRI，I. S.（2020）。刑法关注的网络犯罪。UGM。
[3] CHANDRA, S.（2021）。对抗中国的政治战争：美国的分析。国家安全，4(2)，168–175。
[4] CHECKLAND, P., 和 SCHOLES, J. (1999)。软系统方法论的实际应用。约翰· 威利父子。
[5] ERVIANTO, W. I.（2017）。印度尼西亚国家战略项目中的基础设施发展挑战。 UNIID 研讨会 II 2017, 2(1), 98–103。
[6] IMPERVA (2002) 什么是网络战？示例、类型、缓解措施。可在 http://www.imperva.com/learn/application-security/cyber-warfare/ 上获取
[7] 委员会和信息部。（2022）。公共服务提供商信息安全治理实施指南（第二版）。印度尼西亚通信和信息部。
[8] MARDHANI, D.（2020）。国家韧性研究中的安全与防御，以实现国家安全体系。国防杂志，10(3), 279–298。
[9] PUTRA, D. A., SARAGIH, H. J. R., 和 DEKSINO, G. R. (2020)。实施国防部网络防御风险管理，支撑国防。国防管理：国防管理思想与研究杂志，6（1）。
[10] ROBBANI, K. S., REKSOPRODJO, A. H. S., 和 BASTARI, B.（2020）。保护电力部门的国家关

键信息基础设施免受网络威胁。非对称战争，6(1), 65-88。

[11] SETIYAWAN, B.M.、CHURNIAWAN, E. 和 FARIED, F.S.（2020）。面对网络攻击的信息技术监管努力，维护印度尼西亚共和国单一国家的主权。 Wahyu Prananda USM 法律评论杂志，3(2), 286-287。

[12] SUGIYONO.（2020）。定性研究方法。字母.

[13] SUPRIYATNO, M.（2014）。关于国防科学。雅加达：印度尼西亚火炬图书馆基金会。

[14] SURYOKUSUMO, S. (2016)。非军事防御系统概念：保卫全世界人民的军事防御系统的补充防御系统。印度尼西亚一带一路图书馆基金会。

[15] TAMPUBOLON，K.E.A.（2019）。网络攻击、网络犯罪和网络战之间的区别。管辖权，2(2), 539-554。

[16] VIMY, T.、WIRANTO, S.、RUDIYANTO, R.、WIDODO, P. 和 SUWARNO, P. (2022)。网络攻击对印度尼西亚国家安全的威胁。公民杂志，6(1)，2319-2327。

[17] 经济战争 (2022) 什么是网络战？参见 https://warta Ekonomi.co.id/read452254/apa-itu-cyberwarfare?page=all

[18] WILSON, C.（2014）。对关键信息基础设施的网络威胁。摘自 THOMAS, L. J. 和 Chen, N.（主编）《网络恐怖主义：理解、评估和响应》。第 7 章（第 123-136 页）。伦敦：施普林格-斯旺西大学。 http://doi.org/10.1007/978-1-4939-0962-9_7 。

[19] YANUARTI, I.、WIBISONO, M. 和 MIDHIO, I. W. (2020)。支持国防的印太合作战略：印度尼西亚的视角。《世界战争战略杂志》， 6(1), 41-70.