Strengthening management of non-military intelligence organizations in detecting cyber threats to support national security

Rizky Ramadhianto[1*], Teuku Rezasyah[2], Susaningtyas Nefo Handayani Kertopati[3], Mario Arturo Ruiz Estrada[4], Anastasios-Nikolaos Kanellopoulos[5]

[1]Department of Defense Management, Republic of Indonesia Defense University, Jakarta, Indonesia
[2]Department of International Relations, Padjadjaran University, Bandung, Indonesia
[3]Department of Asymmetric Warfare, Republic of Indonesia Defense University, Jakarta, Indonesia
[4]Department of Economics and Administration, University of Malaya, Kuala Lumpur, Malaysia
[5]Department of International and European Economic Studies, Athens University of Economics and Business, Athens, Greece

Article history
Received: 17 April 2025
Revised: 24 April 2025
Accepted: 26 April 2025

Keywords
Strengthening management
Non-military intelligence
Intelligence community
Cyber threats
National security

Abstract
The internet network necessitates the transformation of cyberspace with systematic and integrated implications, directly proportional to its utilization level. Handling cyber incidents in Indonesia becomes a strategic impediment for non-military intelligence in the national security framework. Therefore, it is critically important to strengthen non-military intelligence organizations in detecting cyber threats. The research aims to analyze the management of Indonesian non-military Intelligence Community (IC) in detecting cyber threats. Moreover, the research method employed is qualitative, utilizing an analytical descriptive research design. Data collection is conducted through interviews, documentation, and literacy studies. The collected data is then analyzed using an interactive analysis model. Subsequently, the research findings indicate that cyber threats are evolving and have technical implications for cyber-security systems and non-technical implications to national security. To detect cyber threats, Indonesian non-military Intelligence Community (IC) implements strategic measures in their intelligence security function, which involves coordinating and organizing management and utilizing technology. The security functions have not been optimally implemented, hindering efforts to detect the evolution of future threats. Summing up, the management of non-military intelligence organizations in Indonesia faces challenges in strengthening security against cyber threats, but there are still challenges and obstacles that must be faced. The researcher recommends that the study's results have the theoretical value for the study of state intelligence regulatory systems, the formulation of non-military intelligence fusion, and cyber-infrastructure in the future, meanwhile, the practical value lies in its potential to assist non-military intelligence stakeholders in fulfilling qualified cyber human resources, ratifying cyber-security regulations, and developing cyber-intelligence equipment technology.

1. Introduction

Transformations in the strategic environment at the national, regional, and global scopes have an impact on the form and nature of threats, challenges, obstacles, and disturbances that continue to threaten and endanger Indonesia's national security. Consequently, it is imperative that Indonesia's national security system be continuously strengthened and adjusted periodically to align with the form and nature of threats faced in the modern warfare domain. This can be accomplished by establishing a more robust and capable intelligence network in the 5.0 society era, or "cyber-era intelligence," which is often regarded as a more effective means of preventing, counteracting, and overcoming of any threats that may pose a risk to national interests and jeopardize Indonesia's sovereignty.

Cyberspace, as one of the domains of modern warfare, has the potential to be used as a battlefield by state and non-state actors through the use of the latest cyber technology, resulting in threats to national security becoming increasingly multidimensional and having implications for the complexity of Indonesia's non-military defense. The term "cyber" refers to the use of the internet, computers, applications, and

*Rizky Ramadhianto, email: rizkramdht@gmail.com

interconnected networks. The inherent lack of security considerations in the design of the internet has resulted in numerous threats in cyberspace. These threats are often perpetrated by individuals or entities that aim to exploit the weaknesses of protocol systems to gain unauthorized access to users' security systems. As a result, the available protocol systems can provide access for potential cybercriminals to undermine functionality by forcing their way into users' security systems.

In cyberspace, individuals and organizations are often categorized as enemies or potential enemies based on their capabilities, including the cyber weapons they use and the strength of their personnel. This relates to the artificial world of computers, databases, and networks that may be vulnerable to exploitation (Geers, 2009). Therefore, any individual or organization operating in cyberspace can be considered as a potential target of cyber-attacks.

The application of technology in unconventional warfare can be a cost-effective means of developing weapons that can have a strategic impact on a country's non-military defense, in comparison to conventional weapons. Nevertheless, it is essential to acknowledge that technological transformation in cyberspace also has the potential to create new threats. The advent of cyber threats in contemporary society has given rise to the possibility of severe consequences when one of the adversarial parties possesses more sophisticated cyber weapons capable of causing systematic damage to the target country.

As outlined by Mattioli et al. (2023), individuals who pose threats through cyberspace include state-sponsored actors, cybercriminals, paid hackers, and hacktivists. These actors update their espionage methods using a combination of software, hardware, and component-based code, which can create new forms of cyber threats. It is crucial to recognize that cyber threats can have a profound impact on both physical and non-physical domains. This underscores the fact that cyber threats have evolved and transformed over time.

The pervasive integration of information and communication technologies into everyday life has facilitated the emergence of cyber threats. The spectrum of cyber threats encompasses a wide range of individuals, from teenagers to criminals, terrorists, and even nation-states (Cavelty et al., 2010). By 2024, the frequency and speed of cyber-attacks had increased significantly, exceeding the defensive capacity of potential target countries (World Economic Forum, 2024).

Within the context of digital transformation, cybersecurity assumes a pivotal role in maintaining public trust. Failure to anticipate cyber-attacks can have severe impacts on critical infrastructure and financial stability, resulting in significant economic losses (Maurer & Nelson, 2021). Consequently, it is imperative to adopt a collaborative and proactive approach to address the evolving landscape of cyber-attacks methods, which now encompass emerging sensors, platforms, networks, and other digital devices (Allen, 2023).

In the aspect of contemporary Indonesian society, which is undergoing a period of profound digital disruption, the role of cyberspace and information technology in the economic, socio-cultural, political, and defense and security systems is becoming increasingly important. Given the significant implications of these developments, it is essential to examine the characteristics of threats related to the use of cutting-edge technology and their implications for Indonesia's cyber sovereignty. Failure to address this issue could have serious consequences for national security stability.

In late June 2024, Indonesia experienced a cyber threat incident targeting the government sector. The National Data Center, managed by Ministry of Communications and Informatics of the Republic of Indonesia (Kominfo), was breached by a brain chiper ransomware variant, specifically Lockbit 3.0 ransomware (Karmini, 2024a). This incident not only resulted in the disruption of digital services in numerous Ministries/Institutions but also in the leakage and sale of Automatic Fingerprint Identification System data of Police of the Republic of Indonesia (INAFIS Polri) and confidential data of the Strategic Intelligence Agency of Indonesian Armed Forces (BAIS TNI).

In addition to compromising the data, the hackers demanded a ransom of $8 million. Pratama Persadha, a cyber expert and chairman of Indonesia's Cybersecurity Research Institute (**see Table 1**), has indicated this attack on the government sector was the most severe since 2017 (Karmini, 2024b). This suggests that Indonesia's cyber infrastructure and server systems remain vulnerable.

Table 1. Indonesia's achievement on cybersecurity (Noor et al., 2023).

Index	Variable	Indonesia's Score to the Global Average	Indicator	Criteria
National Cyber Security Index	E-ID & TS	89 (IDN); 52 (GLB)	Implementation of unique persistent identifier; cryptosystem protocol; e-Identification; signature electronic signature; timestamping; electronic registered logistics system; competencies related authorities	Very Good
National Cyber Security Index	Criminal Counteract	78 (IDN); 59 (GLB)	Criminalization of cybercrime; Operational cybercrime enforcement unit; digital forensics unit; 24/7 cyber-crime hotline	Good
	Incident Response	67 (IDN); 51 (GLB)	Operational cyber incident management unit; routine cyber countermeasure reporting; single unit for global cyber incident coordination	Good
	Military Operation	33 (IDN); 27 (GLB)	Operation of cyber military units; Conduct of cyber military exercises; participation in cyber exercises international cyber defense	Good
Global Innovation Index	Market Satisfaction	48,5 (IDN); 47,6 (GLB)	Credit; Investment; Trade, Diversification, and Market Scale	Good
National Cyber Security Index	Education	44 (IDN); 50 (GLB)	Cyber competency education in schools; Availability of bachelor-master-doctoral programs cyber programs; Cybersecurity associations	Bad
	Private Data	25 (IDN); 64 (GLB)	Personal data protection regulations; Competence of relevant authorities	Bad
	Crisis Management	20 (IDN); 25 (GLB)	Establishment of cyber crisis mitigation plans; National cyber crisis exercises; Participation in international cyber crisis exercises	Bad
	Digital Service	20 (IDN); 27 (GLB)	Operational cybersecurity public services; Protocols; Competence of authorities	Bad
	Threat	20 (IDN); 38 (GLB)	Routine cyber threat analysis mechanism; periodic cyber threat report publication; operational cyber threat information channel	Bad
	Global Contribution	17 (IDN); 30 (GLB)	Participation in the formulation of cybersecurity conventions; Attendance at international forums; Host of international activities; Carrying out cybersecurity capacity building activities for other countries	Bad
Global Innovation Index	Infrastructure	41,4 (INA); 41,48 (GLB)	Information and Communication Technology (ICT); Public infrastructure; Ecological sustainability	Bad
	Human Resource and Research	22,4 (INA); 32,7 (GLB)	Education; tertiary education; development and research	Bad
	Knowledge & Technological Output	16,3 (INA); 24,06 (GLB)	Knowledge of creation, impact, and diffusion	Bad
	Creative Output	18,3 (INA); 26,51 (GLB)	Intangible assets; Jada and creative products; Online creativity	Bad
National Cyber Security Index	Essential Service	0 (IDN); 29 (GLB)	Operator identification; Operator protocol; Competence of the supervisory authority; Regular monitoring	Very Bad
	Policy	0 (IDN); 40 (GLB)	Operational work unit; coordination forum; national strategy; security action plan; cybersecurity action plan	Very Bad
Global Innovation Index	Institution	51,2 (INA); 64,94 (GLB)	Environment of politics, regulator, and business	Very Bad
	Business Satisfaction	17,5 (INA); 29,76 (GLB)	Worker knowledge; Innovation linkages; Knowledge uptake	Very Bad

A review of the Indonesian government's achievements in cybersecurity efforts, as illustrated in the table above, reveals that Indonesia has made notable progress in operational aspects of its cybersecurity. Conversely, critical areas such as the handling of cyber-attacks, human resources, infrastructure, threat detection, and accompanying policies remain relatively underdeveloped. This indicates that Indonesia's cybersecurity vulnerability in the future remains significant and unaddressed.

In conjunction with the mounting cyber threats that present a significant risk to Indonesia's national security, it is of paramount importance for Indonesia to acknowledge the cyber revolution because of the increasing vulnerability to cyber-attacks. Despite the observed increase in Indonesia's cybersecurity index ranking over time, as indicated by State Cyber and Crypto Agency of the Republic of Indonesia (BSSN) annual data, the index does not fully reflect the country's cybersecurity practices. This suggests that Indonesia's level of vulnerability to cyber threats remains classified as high. Due to the high intensity of cyber threats, BSSN frequently issues warnings to relevant non-military agencies that are threatened. Nonetheless, the lack of coordination among stakeholders creates opportunities for cyber-attacks.

There are still several government agencies that have experienced data leaks. A significant concern when Indonesia is confronted with non-state actors that are state-sponsored or funded by other countries, Indonesia's cyber capacity is faced with a series of challenges in terms of infrastructure, organizational readiness, technological capabilities, and cyber talent. This is noted by The International Institute for Strategic Studies in 2021.

Following the Presidential Regulation of the Republic of Indonesia Number 47 of 2023 on the National Cyber Security Strategy and Cyber Crisis Countermeasures, the advent of new technologies has the potential to precipitate cyber-attacks that can result in significant social and economic losses and even threaten state sovereignty. To mitigate cyber threats, a more targeted strategic response is required that focuses on higher-level issues rather than just operations. The aim is to cultivate a culture of asset protection and cyber resilience within the organization.

Eventually, to diminish the susceptibility to cyber threats and guarantee authorized access to essential data, it is imperative to integrate the non-military defense system with the national security system through the fortification of the Indonesian non-military Intelligence Community (IC)'s functions to mitigate strategic impediments in cyberspace. This refers to Law Number 17 of 2011 on the State Intelligence, which defines intelligence as the activity of knowing, organizing, and acting to formulate policies, and national strategies, and make decisions based on analysis of information and facts collected through a working process in the context of early detection and early warning to prevent, counteract, and overcome threats to national security.

The evolving phenomenon of cyber intelligence activities is in alignment with the advancements of the modern era, which has led to an expansion of interests in the utilization of intelligence activities, particularly in the domain of cyberspace. In the contemporary era, the scope of cyber intelligence has expanded to encompass the detection of non-military threats. This shift in focus has been enabled by the modification of existing intelligence tools by communities outside the traditional military domain.

Furthermore, the Presidential Regulation of the Republic of Indonesia Number 67 of 2013 on the Coordination of State Intelligence designates the Indonesian Intelligence Community (IC) headed by State Intelligence Agency of the Republic of Indonesia (BIN), which serves as the coordinator of state intelligence. In terms of its relationship with the non-military Intelligence Community (IC), state intelligence plays a strategic role in decision-making related to national security, particularly regarding the interests of the main tasks and functions of agencies outside the military aspect. This includes the utilization of various domains, one of which is the cyber domain.

Based on the aforementioned considerations, it can be argued that the cybersecurity sector should prioritize the optimization of the intelligence security function in terms of detection and early warning. The significance of this research is underscored by the author's presentation of numerous preceding studies that remain pertinent to the subject matter. These studies are compared and contrasted in Table **2** below, offering a more comprehensive understanding of the subject.

Table 2. Previous studies.

No	Author/s Name (Year)	Research Title	Similarity	Difference
1	(Johnson, 2024)	Intelligence Collection Priorities in an Age of Renewed Superpower Conflict: Toward a More Expansive Perspective	Explore the evolving role of intelligence agencies in responding to threats to national security, tracing its shifts alongside the evolution of the strategic environment across different historical periods and its ramifications for various aspects of state life.	Elaboration of threat assessments is not limited to a cyber intelligence perspective; environmental intelligence, health intelligence, and economic intelligence are also discussed based on the scope of the US government.
2	(Hansel & Silomon, 2024)	Ransomware as a threat to peace and security: understanding and avoiding political worst-case scenarios	As a preliminary step toward developing a comprehensive strategy to protect the country's security system from cyber-attacks, this research aims to gain a more nuanced understanding of the specific risks posed by ransomware.	The scope of this research is constrained to the technical elements of cyber and does not extend to the broader aspects of intelligence.
3	(Moran et al., 2023)	The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying	Illustrate the Intelligence Community's dedication to technological advancement and the significance of collaborative stakeholder engagement.	The Intelligence Community (IC) under examination is the United States, not Indonesia, while technological development unit is concerned with artificial intelligence, rather than cyber issues.
4	(Bodström, 2022)	Strategic Cyber Environment Management with Zero Trust and Cyber Counterintelligence	The implementation of cyber counterintelligence methods can facilitate the attainment of enhanced cybersecurity in a multitude of organizational contexts.	The integration of cyber counterintelligence with the zero-trust network concept, utilizing only literature review data collection methods.
5	(Cline, 2022)	Sharing Intelligence Culture: Working With Foreign Intelligence Services	Formulate a collaborative relationship with other intelligence agencies.	The focus of this study is on the bureaucratic aspects of foreign intelligence.
6	(Trim & Lee, 2021)	The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement	The study, which inquired into cybersecurity and intelligence professionals' perspectives, sought to assess the efficacy of management to mitigate cyber threats.	The subject of this study is global in scope and focuses on the actions of senior managers towards their organization's staff.
7	(Ateş & Erkan, 2021)	Governing the European Intelligence: Multilateral Intelligence Cooperation in the European Union	An examination of the coordination between intelligence agencies.	An analysis of the scope of intelligence reveals that it is multilateral, rather than national.
8	(Mavroeidis et al., 2021)	Threat Actor Type Inference and Characterization within Cyber Threat Intelligence	The objective is to enhance the quality of intelligence utilized in the response to cyber threats.	Prioritize an analysis of the various categories of cybercriminal actors.

No	Author/s Name (Year)	Research Title	Similarity	Difference
9	(O'Connor, 2022)	Cyber Counterintelligence: Assets, Audiences, and the Rise of Disinformation	The research is anchored in the evolution of cyber threats, which have multifaceted effects that demand the advancement of cyber counterintelligence.	A study of cyber threats in the United Kingdom has demonstrated the potential for such threats to be used to further disinformation campaigns and to create conflict with liberal democracies.
10	(Gioe et al., 2020)	Intelligence in the Cyber Era: Evolution or Revolution?	The identification of intelligence entities in response to the strategic environment's evolving dynamics, particularly technological advances.	A key research subject is the fusion of the traditional intelligence cycle model and offensive cyber operations within the Anglo-American context.

Source: Processed by the author (2024)

The existing literature on the table above has primarily concentrated on the utilization of cyber and intelligence instruments, along with the incorporation of diverse improvisations in the methodology of each study. In contrast, the present study's focus on non-military aspects utilizing the security function of intelligence as a national security strategy for detecting threats in cyberspace, offering a more comprehensive and compelling presentation than previous studies.

The dynamics of cyber threats are highly intricate and characterized by a rapid and extensive rate of development, negatively impacting various sectors, including the non-military sector. Intelligence, as the principal instrument of national security, must assume a pivotal role in detecting cyber threats. Accordingly, it is essential to strengthen non-military intelligence entities to maintain national security and stability from strategic impediments posed through cyberspace.

Ideally, the Indonesian non-military Intelligence Community (IC) would be capable of optimizing intelligence excellence in the security function, thereby enabling the early detection and warning of potential cyber threats. Nevertheless, the management of cyber incidents in Indonesia has not been adequately addressed. Indonesia's ascension in the cyber security indexes does not guarantee immunity from cyber-attacks, as the prevalence of cyber-attack anomalies increases dramatically (Id-SIRTII/CC, 2023).

An analysis of this phenomenon indicates a gap in the intelligence security function and cyber threat detection efforts by the Indonesian non-military Intelligence Community (IC). This gap can be attributed to deficiencies in organizing and coordinating management, which leave room for vulnerabilities and strategic negations that could compromise national security.

Building upon the aforementioned background and the urgency of the issue, the author identifies the research problem formulation as "How to Strengthen the Management of Non-military Intelligence Organizations in Detecting Cyber Threats to Support National Security?", consisting of three questions as follows: 1) What are the factual and potential cyber threats to national security currently?, 2) How is the strategy of the security intelligence function in strengthening Indonesian non-military Intelligence Community (IC)?, and 3) Which are the challenges and obstacles faced by Indonesian non-military Intelligence Community (IC) in detecting cyber threats?.

This research aims to establish the efficacy in the management and to enhance the capabilities of Indonesian non-military Intelligence Community (IC) to counteract cyber threats as a manifestation of non-military defense. The specific focuses are as follows: 1) Identifying the factual and potential cyber threats to national security currently, 2) Analyzing the strategy of the security intelligence function in strengthening Indonesian non-military Intelligence Community (IC), and 3) Identifying the challenges and obstacles faced by Indonesian non-military Intelligence Community (IC) in detecting cyber threats.

The benefit of this study is making the implications for the boundaries of knowledge in the field of intelligence, particularly in the domains of non-military intelligence and cybersecurity. The findings of this study may also serve as a theoretical reference for academics and intelligence practitioners looking to advance their understanding of intelligence science. In practice, this research is expected to enhance awareness and comprehension of intelligence conditions, furnish policy recommendations for the government, and yield constructive and beneficial outcomes for relevant stakeholders to prepare for increasingly complex cyber threats in the future.

The implementation of this research is claimed to be original based on the willingness and positive response of the informants. This is evidenced by the use of a list of questions as interview materials, not only by the researcher, but also by the informants. By utilizing this methodology, the informants are able to study the material around the research focus in advance, moreover, the interview process is documented during the research. The researcher underscored the fact-based nature of the research, emphasizing that this research is conducted factually without fabrication.

2. Literature Review

2.1. National Security

Pursuant to Law Number 17 of 2011 on the State Intelligence, national security is a dynamic condition of the nation and the Unitary State of the Republic of Indonesia. This condition is defined as a state of affairs that guarantees the safety, peace, and welfare of citizens, communities, and the nation; the protection of the sovereignty and territorial integrity of the state; and the continuity of national development from all threats. The academic concept of national security is understood to be multidimensional, encompassing four interconnected dimensions: the dimension of human security, the dimension of public security and public order, domestic security, and the dimension of defense.

In an increasingly complex era, security threats are evolving and changing in magnitude (Wæver, 2008). Considering the cyber and asymmetric threats and envisioning a comprehensive approach that includes culture, economic welfare, and social texture in the adopted considerations (Waever & Flockhart, 2014). Accordingly, Buzan et al. (1998) assert that actors play pivotal roles in taking action, utilizing their power to control actual threats or preempt potential threats.

Kuhn (1982) explained the "paradigm shift" in security issues that brings forth new concepts, with primary attention given to existing threats and potential new threats that could endanger the state. Furthermore, this complexity is summarized by several issues that accompany it, such as the maximal use of power to control domestic affairs, national security issues, and military security issues, namely the issues of intelligence concepts, command, and control (Paleri, 2008). The ramifications of national security issues extend to a multitude of domains, both domestic and foreign. Among the most salient are the acquisition of new weapons systems, increases in defense budgets, and the reorganization of intelligence agencies (Chuter, 2011).

Based on the objective understanding of national security, it is estimated that future threats may disrupt Indonesians' daily lives, resulting in shifts in ideology, weakening of nationalism and government authority, reduced political legitimacy, and diminished patriotism. The concept of national security, influenced by technological advancements, must be addressed holistically to ensure comprehensive direction and administration.

To conclude, national security is a multidimensional concept that balances military and non-military methods to ensure domestic stability and protect against all forms of threats, including the securing of the country's values and identity. Therefore, this study utilizes the concept of national security as a grand theory to examine threats that affect domestic instability with the goal of attaining national power.

2.2. Defense Management

Defense management is a multifaceted concept that encompasses legal and conceptual facets via institution building and resource management for operations, international collaboration, and civil defense regulation. Good governance is closely connected to defense management, particularly in generating outputs through processes that are transparent, accountable, effective, and efficient (Tagarev et al., 2002).

As outlined by Bucur-Marcu et al. (2010), defense management is a process that is necessary for the formulation of defense policies. To be effective in this process, it is essential to have an appropriate and sustainable planning mechanism in place. From this concept, it can be inferred that defense management refers to a country's ability to manage its resources strategically for national defense, based on efficiency and effectiveness in the long term and comprehensively, according to the principles of management.

Indonesia's defense management faces a complex challenge concerning maintaining and protecting sovereignty, which is crucial for national security, state sovereignty, and territorial integrity (Kennedy et al., 2017). In conclusion, defense management entails a nation's capacity to strategically manage its resources for national defense, emphasizing long-term efficiency and effectiveness. This holistic approach adopts management principles that are then translated into defense policies.

This study employs the concept of defense management as a grand theory to demonstrate how endeavors to transform national resources in the form of intelligence information into potential resources strategically result in policies aimed at enhancing defense capabilities to counter different types of threats, including those of the cyber variety.

2.3. Intelligence

In the Law of the Republic of Indonesia Number 17 of 2011, the intelligence functions serve to carry out early detection and warning. The purpose of state intelligence is to detect, identify, assess, analyze, interpret, and present information. In scientific contexts, intelligence entities are categorized according to three distinct criteria: knowledge, activity, and organization. Knowledge is the outcome of intelligence designed for detecting and providing early warnings. Activities are the tasks conducted by intelligence agencies throughout the cyclic process, both open and closed. These components serve as inputs for policies and strategies, enabling decision-makers to determine preventive, deterrence, and countermeasure approaches against various threats.

Intelligence can be categorized into four meanings: intelligence as information, process, series of missions, and organization (Johnson, 1996). According to Warner (2019), Intelligence is generally interpreted as decision-making and covert activities to understand and influence foreign entities. The information contained in these foreign entities is often perceived as a threat or adversary, as well as an institution related to information gathering (Lerner & Lerner, 2004).

Prunckun (2014) divides intelligence into four categories: actions, locations where knowledge is produced, organizations that manage knowledge, and reports generated from processes or organizational activities. Prunckun further elaborates on intelligence as both knowledge and a process. Intelligence as a body of knowledge enables the planning and direction of an organization's actions towards current or potential enemies. Clear and concise comprehension of both aspects is essential for effective organization management. Meanwhile, intelligence as a process involves a series of procedures that collectively constitute the intelligence cycle.

Intelligence represents a crucial element in the formulation and implementation of national policies and cyber defense. It contributes directly to the processes, products, and organizations utilized for these purposes. In essence, intelligence constitutes a vital component of the prompt detection and warning apparatus that empowers policymakers to maintain early vigilance. Its principal function is to gather, assess, and disseminate critical information for policymakers to make well-informed and precise decisions. Therefore, this study employs intelligence as a comprehensive framework for analyzing non-military intelligence agencies' role in mitigating potential cyber threats through the execution of counterintelligence and facilitating effective coordination to furnish crucial information for national security planning.

2.4. Intelligence Security Function

The role and function of intelligence are inextricably linked to the execution of security. As Saronto (2018) posit, intelligence, which encompasses data, structures, and actions, is a pivotal factor to secure a country against a multitude of threats, challenges, impediments, and disruptions, both domestic and foreign. It is argued that in Indonesia, intelligence is a product of various experiences, comprising both successful and unsuccessful intelligence activities within the country, alongside socio-political and cultural factors.

Kunarto (1999) explains that operational intelligence activities, such as security, are conducted both publicly and covertly. The intelligence function of security involves securing the organization from becoming a target of adversaries. More specifically, Saronto (2001) classified the main task of intelligence in security as the prevention of certain parties from exploiting weaknesses in the political, economic, socio-cultural, and security fields to create an atmosphere of passive opposition, which may turn active and pose a threat or disturbance to national security stability.

Hendropriyono (2013) asserts that the intelligence security function involves counterintelligence and preventive measures, such as camouflage, to protect personnel, materials, and information, including documents. In the realm of cybersecurity, regulations govern protecting state assets from theft, modification, and destruction in the cyber domain. Therefore, proper governance is necessary to clarify how the Intelligence Community (IC) handles cyber threats when carrying out security functions.

Joint intelligence is an effort to achieve a better understanding of securing important aspects of cyber threats. Therefore, prioritizing collaborative security intelligence is an important first step towards a better model to support the defense of critical cyber infrastructures against national security threats (Borghard, 2022).

To conclude, the function of intelligence as security is to secure state assets from foreign intelligence operations and the impact on national resilience in the form of national security. In this study, security intelligence is presented as a middle theory. The implication is that the non-military Intelligence Community (IC) in Indonesia can achieve measurable gains in comprehending the cyber threat landscape. This implies an additional responsibility for the protection of critical national infrastructure.

2.5. Non-Military Defense

As set forth in the 2014 edition of the State Defense Doctrine Book, the term "non-military defense" encompasses the involvement of Ministries/Institutions beyond the field of defense in addressing threats that encompass ideological, political, economic, socio-cultural, technological, and security dimensions. The concept of non-military defense is applicable to proxy warfare (Cragin, 2015) as it can undermine a country not by confronting its military might, but rather by targeting the highest echelons of government power, including the executive, judiciary, and legislature.

In non-military defense, a shared understanding of duties, obligations, and roles for each party involved in the implementation of national defense is crucial. In the absence a shared understanding, achieving synergy among non-military defense forces would be challenging. An illustration of synergy in the realm of non-military defense entails the utilization of security intelligence. This includes the cultivation of professional intelligence talent capabilities and the use of technology to secure national assets, alongside integrated anti-espionage practices.

To address espionage, Ministries and Institutions execute deterrence in accordance with their roles and primary tasks by establishing countermeasure and security systems for activities, documents, news, and personnel. Additionally, they prepare facilities, infrastructure, and human resources with the ability to master anti-espionage technology, and develop laws and regulations pertaining to the prevention, control, and prosecution of espionage.

To summarize, non-military defense adheres to legal provisions on authority and accountability by utilizing the fundamental principles of national defense to anticipate possible ideological, political, economic, social, and cultural threats that may jeopardize the sovereignty, integrity, and safety of the nation. This encompasses the defense activities of all national forces, extending beyond the military domain, with the objective of proactively constructing and cultivating the state's capacity to avert and eradicate such perils.

Based on the aforementioned explanations, this study employs the term "non-military defense" as a middle theory to describe the empowerment of functional components beyond the defense sector, such as the Indonesian non-military Intelligence Community (IC). The objective is to prevent cyber threats and to achieve stability, thereby enabling national development to embody the objectives and interests of the nation.

2.6. Cyber Warfare

As outlined in the Indonesian Defense White Paper in 2015, network-based warfare is contingent upon information superiority and the capacity to engage in cyber warfare, because of advancements in information and communication technology. A number of attacks, including wiretapping, hacking, and damage to software, systems, network infrastructure, and other devices, have led to the recognition that threats to the current strategic security environment are not limited to physical forms, but also exist in the form of digital.

In examining Waldo's (2017) theory on the stability of a nation-state, five factors are identified as contributing to the stability and resilience of a society: legitimacy, authority, knowledge management, bureaucratic control, and confidence. This theory remains pertinent in understanding the impact of cyber warfare on societal functions targeted by strategic negation, which can result in systematic instability within the state.

The growing threat of cyber warfare, which aims to harm and destroy opposing parties through the internet, underscores the crucial role of cyber defense in maintaining a nation's defense and security. According to the Minister of Defence Regulation Number 82 of 2014, the objective of cyber defense is to prevent cyber-attacks from impeding national defense operations.

The strategic threat posed by cyber warfare to national defense is compounded by the inherent vulnerability of internet platforms, which include the creation of propaganda through social media. Therefore, research aimed at improving defense capabilities must consider cyberwarfare as a critical aspect.

This theory proposes a moderate approach to studying cyber warfare. It is necessary for Indonesia to prepare for such attacks, and this entails developing defensive measures that utilize intelligence principles. These measures will enable prompt and accurate responses, thereby supporting the implementation of appropriate strategies to counter cyber threats. Ultimately, the goal is to prevent the possibility of achieving a coordinated cyber defense approach.

2.7. Organizing Theory

The act of organizing is a fundamental aspect of management that requires a comprehensive understanding of the organization's underlying purpose. As posited by Wijayanto (2013), an organization is comprised of two or more individuals who collaborate in a structured manner to achieve goals based on decisions made during the planning phase.

Schermerhorn et al, (2005) defines organizing as the arrangement of diverse resources with the intent of working towards a shared goal. This entails ensuring that each individual is aware of their duties, responsibilities, rights, and authorities. This is consistent with the perspective put forth by Mondy (1990), which idenitifies organizing as a process of establishing formal relationships between individuals and resources with the objective of achieving organizational goals.

In light of the aforementioned explanations, it can be inferred that organizing is a series of activities conducted in a systematic manner with the objective of determining, classifying, organizing, and forming patterns of work relationships in a conducive manner to the organizational goals achievement. For the purposes of this study, the organizing theory framework is employed as an applied theory to facilitate the systematic identification of working relationships within Indonesian non-military Intelligence Community (IC). The objective is to facilitate the security intelligence operations of the aforementioned entities, particularly with regard to the mitigation of cyber threats.

2.8. Strengthening Theory

The theory, known as operant conditioning, is attributed to B. F. Skinner as its primary proponent. This theory is applicable to learning activities. Any object, event, or situation may be regarded as a reinforcer if it is associated with a reduction in the individual's state of deprivation. In other words, if the object, event, or situation is perceived as a means of satisfying a need when responding.

Strengthening theory can be summed up as a significant psychological approach in the utilization of the whole situation to motivate individuals, from biological drives to the rewards they receive. Its central tenet states that a person's needs or motives must be present before learning occurs, and what is learned must reduce or satisfy those needs.

This theory has been selected as an applied theory to determine means in which non-military intelligence organizations can efficiently execute security intelligence measures to combat cyber threats. It will include strategies for determining and selecting the best courses of action, as well as decision-making processes to ensure success.

2.9. Coordination Theory

The concept of coordination as defined by Malone and Crowston (1994), encompasses the management of interdependent relationships between activities that share the same objects, as well as the effective management of dependent relationships. In accordance with Fayol (2010), the process of coordination involves the connection of all organizational units at different levels and the harmonization of their activities to achieve the organization's objectives in a managerial context.

The importance of coordination in the context of planning cannot be overstated, as it plays a pivotal role in ensuring the successful implementation of a plan. As an organization, it assumes a leading role in this endeavor (Gullick & Urwick, 1937). To establish effective coordination, it is necessary to clearly define roles and responsibilities (Viinamäki, 2004). The achievement of collective goals necessitates the establishment of group agreement and coordination, as the fulfillment of obligations is most effectively achieved through reciprocal action (Provis, 2004). Consequently, coordination is intended to address inquiries pertaining to the organization's purpose, methods, timing, and personnel.

The Law of the Republic of Indonesia Number 17 of 2011 concerning State Intelligence and Presidential Regulation of the Republic of Indonesia Number 67 of 2013 on State Intelligence Coordination defines coordination as the process of harmonizing functional relationships, synchronizing efforts, and synergizing intelligences to accomplish intelligence objectives and functions. From this explanation, it can be concluded that coordination is a process which involves mutual agreement and the binding of specific elements or activities. The aim of this process is to direct these elements and activities towards a predetermined goal, while maintaining focus on other goals.

Through the process of coordination, the organization can bring in the necessary resources from the external environment, including personnel and other factors of production, which contribute to achieving the performance objectives. In this study, the theory of coordination is employed as an applied theory to identify the procedure established by Indonesian non-military Intelligence Community (IC) to organize intelligence security function as a means of detecting cyber threats.

2.10. Implication Theory

Silalahi (2005) posited that implications are the consequences of implementing a program that may have either a positive or a negative impact on the parties involved, resulting from the policy formulation process. The overarching concept of implication can be defined as the outcomes and consequences that result from the implementation of specific policies or activities.

In this study, the theory of implication is employed as an applied theory to evaluate the impact of enhancing cyber threat deterrence through the integration of security intelligence function within the Indonesian non-military Intelligence Community (IC). The objective is to elucidate the framework for optimizing organizational management.

3. Method

In the process of crafting this article, the author employed a qualitative methodology, which consists of the basis for the research. The objective is to gain a comprehensive understanding of the meaning and phenomena under study. The research design chosen is descriptive-analytical, adopting an inductive writing perspective to stay focused on individual significance in uncovering the complexity of the problem (Sugiyono, 2018).

The researcher ensures that the research process adheres to the relevant ethical standards by providing each informant, in their capacity as research subjects, with a proper explanation of the research objectives, methodology, potential benefits for each informant's agency, the questions asked, and the guarantee of data confidentiality. All research procedures are a prerequisite of obtaining informant approval. As this research involves the collection of data of an intelligence and national security sensitivity, the researcher is fully conscious of the confidentiality implications. Consequently, the researcher is meticulous in the presentation of the research data to ensure that it is not misused and in no way diverges from the ethical standards of research in the field of intelligence and national security.

The research for this article is conducted within the Indonesian non-military Intelligence Community (IC), encompassing BIN, Ministerial and Non-Ministerial Intelligence, Ministry of Communications and Informatics of the Republic of Indonesia (Kominfo), State Cyber and Crypto Agency of the Republic of Indonesia (BSSN), and relevant institutions. The author selected informants as a research subject based on the characteristics of having extensive knowledge, insight, and competence. These informants included executives, staff, and experts at the research location who possessed the necessary qualifications in the field of non-military intelligence and cyber threats (**see Table 3)**.

Table 3. List of informants.

No	Position	Institution	Code
1	Chief of the Strategic Analyst Council	State Intelligence Agency of the Republic of Indonesia (BIN)	A1
2	Deputy III for Cybersecurity and Ciphering Government and Human Development	State Cyber and Crypto Agency of the Republic of Indonesia (BSSN)	A2
3	Defense and Security Communication Information Coordinator of Directorate General of Public Information and Communication	Ministry of Communications and Informatics of the Republic of Indonesia (Kominfo)	B1
4	Chief	Municipal Resort Police of Bandung	B2
5	Policy Analyst for the Medium and Short-Term National Development Plan	National Resilience Council of the Republic of Indonesia (Wantannas)	B3
6	Head of Threat Intelligence at the Assistant Deputy for Defense Intelligence Coordination	Coordinating Ministry for Politic, Law and Security Affairs of the Republic of Indonesia (Kemenko Polhukam)	B4
7	Junior Expert Immigration Analyst Directorate of Immigration Intelligence	Ministry of Law and Human Rights of the Republic of Indonesia (Kemenkumham)	B5
8	Intelligence and Cyber Expert	State Intelligence College (STIN) and Intelligence & National Security Studies; Al-Kamal Institute of Science and Technology (ISTA); University of Indonesia; and Republic of Indonesia Defense University (Unhan RI)	C1; C2; C3; C4

Source: Processed by the Author (2024)

This research object is on analyzing the organizing management of intelligence security function in Indonesian non-military Intelligence Community (IC) as a proactive measure against future cyber threats. Moreover, the research aims to identify the coordination process and examine the implications of security intelligence in responding to cyber threats. The research object will be analyzed using concepts, procedures, and systematic sequences in accordance with scientific research to yield results that address the research questions.

The data collection techniques employed in this writing include interviews and literature studies. Subsequently, the triangulation method is employed to assess the credibility and confirmability of the data. Then use data analysis as a form of interpretation to provide comprehensive and unbiased solutions to research-related issues.

3.1. Data Collection Techniques

Creswell and Creswell (2017) proposes that data collection methods entail a sequence of interconnected steps for gathering information in pursuit of research questions. When selecting a methodology for data collection, researchers must consider two types of data, primary and secondary (Kothari, 2004).

Meanwhile, Miles et al. (2014) explains that data collection activities are typically carried out in close proximity to a local setting for a sustained period of time. It should be noted that such data is not immediately accessible for analysis but requires processing. In short, data collection is an activity for obtaining research data through various means and sources. The data collection techniques utilized in this research are interview, literature study, and documentation study.

Interviews for this research using structured interview guidelines and an in-depth data collection process. The interview process involved asking questions based on prepared guidelines, which were designed by aligning them with relevant theories to address each issue. In more detail, the interview technique will consist of selecting the interviewee and preparing the subject matter beforehand. The interview results will then be documented in field notes and analyzed to identify important insights.

In this research, the literature study process will be examined by gathering data from various journals, books, electronic and internet media, as well as confidential and public official documents related to organizing managing of security intelligence in countering cyber threats and enhancing non-military intelligence through coordination and implementation. Then, the documentation process in this research entails exploring literature documents associated with Indonesian non-military Intelligence Community (IC)'s security intelligence function to mitigate cyber risks.

3.2. Data Processing Techniques

The researcher processed both primary and secondary data. The primary data is processed through interviews with key informants A1 and A2, who are directly involved in state intelligence coordination and the leading sector of cyber security. Meanwhile, secondary data is processed from scientific papers, journals, books, articles, online news, relevant laws and regulations, and credible information from official websites of relevant agencies.

The interview results from informants B1, B2, B3, B4, and B5, who are the main informants of the non-military IC, are processed by the researcher in accordance with the provisions of the Law of State Intelligence. The processing included both structural and non-structural analysis. The processing of interview results from supporting informants, including C1, C2, C3, and C4, is based solely on their expertise and contributions to scientific works, as well as their involvement in scientific discussions related to the advancement of intelligence and cyber issues. This ensures objectivity and strengthens the research data.

3.3. Data Validity Testing

According to Klosterman (2016), the formulation of information in qualitative research can be compared with other theoretical perspectives to enhance its validity and to avoid potential biases. Meanwhile, Moleong (2017) defines triangulation as a technique for checking data validity by utilizing external resources to confirm the accuracy of the data.

Thus, validity is interpreted as a concept that is updated from the concepts of validity and reliability of data based on the demands of knowledge, criteria, and paradigms. For this study, data validity is established through source triangulation, which involved comparing the documentation data with the data gathered from literature studies and interviews with pre-determined research subjects.

3.4. Data Analysis Techniques

Bogdan and Biklen, as cited on Moleong (2017), argue that data analysis encompasses the organization and sorting of data, followed by the identification of patterns and the determination of what is important and what can be learned. Finally, one can decide what information to share with others. The process of data analysis involves organizing data into categories and chronology, reviewing it repeatedly, and coding it continuously.

Based on the evaluation of multiple explanations of the qualitative data analysis process, this study will employ data analysis as a form of interpretation to provide comprehensive and unbiased solutions to research-related issues utilizing (Miles et al., 2014) interactive analysis model. The interactive process encompasses four key components (**see Figure 1**).

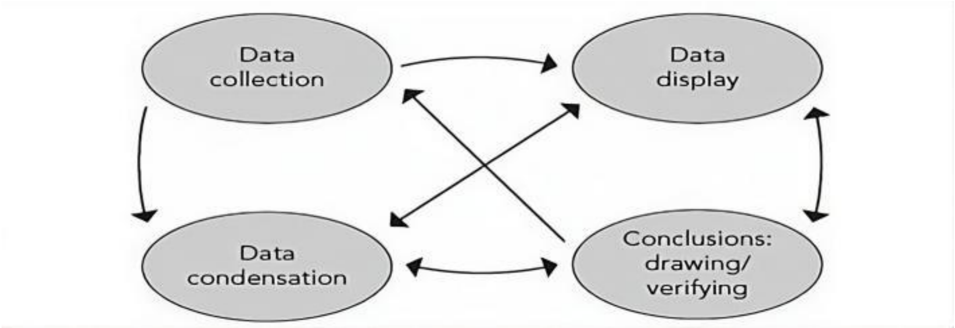

Figure 1. Components of interactive data analysis model (Miles et al., 2014).

The model proposes that qualitative data analysis activities are conducted interactively and continuously until saturation is achieved. These include data collection, data condensation, data display, and conclusion drawing or verification. The entire process is repeated until it produces saturated data and is deemed reliable.

For the purposes of this research, data validity is verified and then categorized and interpreted for analysis in the discussion section. This study analyzes three categories: (1) cyber potential and factual threats to national security; (2) the strategy of intelligence security function in strengthening non-military IC to detect cyber threats; and (3) the challenges and obstacles faced by non-military IC in detecting cyber threats.

4. Result and Discussion

4.1. Cyber Potential and Factual Threats to National Security

This sub-chapter interprets the necessity for Indonesia’s national security to prioritize the consideration of both factual and potential cyber threats. The prevalence of cyber threat activities has increased significantly in recent years and is projected to continue to evolve, particularly within the government sector. These threats are perpetrated by state-sponsored and non-state actors who employ modern techniques to conduct persistent, sophisticated, and clandestine cyber-attacks with the objective of gaining and maintaining access to systems. Indonesia's cyber defense capacity is not yet fully prepared to deal with emerging cyber threats.

The advent of Information and Communication Technology (ICT) has led to an increase in the complexity and scale of cyber threats, rendering cyber warfare an unavoidable phenomenon. This has become a strategic issue in Indonesia. ICT offers a multitude of opportunities for human welfare, including enhanced communication and business operations, particularly within the context of the digital economy. Nevertheless, it is critical to acknowledge that elevated levels of ICT utilization elevate the probability of cyber-attacks. As Brooker (2013) notes, the utilization of cyberspace can be misused for cybercrime, whether state-sponsored or not, which can lead to the destabilization of a country's government.

Accordingly, the orientation of this study encompasses not only cybercriminals but also the broader misuse of cyberspace. In contrast to the previous research conducted by (Mavroeidis et al., 2021), which solely examines the influence of intelligence on cyber threat response, with a particular focus on individuals engaged in cybercrime.

Cyber threat variants can be classified into two categories: factual and potential. To combat potential future cyber threats, it is essential to analyze factual cyber threat entities (**see Table 4**). For instance, the deployment of Artificial Intelligence (AI) technologies, such as OpenAI, which operates a Large Language Model (LLM), could prove beneficial in a range of future endeavors. However, this can be problematic if the resources are diverted to those who intend to commit cybercrime.

Table 4. Potential and factual cyber threats.

No	Type of Threat	Motives	Methods
1	Phishing	Obtaining confidential information, such as account credentials, can also serve as an initiator for other cyber-attacks. Malware can be distributed to the victim's system through emails or malicious URL links.	Perpetrators of fraud often use deceptive tactics such as sending emails, SMS messages, or making phone calls that are designed to attract the victim's attention and provoke them into opening, accessing, or receiving the message.
2	Crypto jacking	The unauthorized use of computing resources to mine cryptocurrencies is illegal. This practice targets all sectors, particularly the financial and industrial sectors.	Mining digital currencies without paying for electricity, hardware, and other resources is becoming increasingly popular due to the rising value of digital currencies, particularly Bitcoin and Monero.
3	IoT Cybercrime and Artificial Intelligence (AI)	AI can detect unusual IoT behavior and be used to commit fraud, such as deepfakes.	Along with the trend of increasing types of IoT devices, AI is also predicted will be utilized more to commit cybercrime.
4	RDP Attacks	Installing ransomware on a network by exploiting open ports can have a significant impact on business processes in organizations across various sectors.	The RDP protocol's connection control utilizes port 3389 for all RDP users through an encrypted channel.
5	Data Breaches	Theft of sensitive data, such as Personal Identifiable Information (PII) and organization-sensitive data, should not be made public without the knowledge of the system owner.	Misconfiguration can lead to sensitive data being accessed publicly on the web. Attackers often insert malicious code into documents or emails, which will be executed when the victim opens the file.
6	APT Attacks	Remaining undetected for a long period of time while gaining unauthorized access to a computer network.	Pre-attack reconnaissance or weaponization could potentially pave the way for an increase in Crime-as-a-Service (CaaS).
7	Web Defacement	Altering the appearance or content of a website to test the skills of defacers or as an act of electronic graffiti is a common practice. It is also used for political agendas, which can harm the reputation or credibility of a particular party.	Exploiting system weaknesses to gain unauthorized access to a server and manipulate website content is a serious security threat. One common method used by attackers is SQL Injection, which allows them to gain administrative access and modify or delete website content.
8	Ransomware	By locking access to a system or data and then demanding a fee to restore access to the rightful owner, attackers such as Ransomware-as-a-Service (RaaS) providers can increase the ransom price. They may also add wiper malware to the ransomware attack, which can result in the loss of data and public embarrassment for the victim.	Deleting data and disrupting the availability of critical systems, such as Operational Technology (OT) or manufacturing equipment and servers, should be avoided. Instead, focus on modernizing proprietary software and preventing data exfiltration and leaks.
9	Social Engineering	The attacker aims to obtain specific information from the target to manipulate the victim's thoughts and actions.	Using human as the main object of attack by communicating with the target directly or indirectly that focuses on psychological manipulation of humans with various media.
10	Distributed Denial of Service (DDoS)	Disabling a website's services can be achieved by sending a large number of requests. This attack can become increasingly sophisticated, complex, and prolonged over time.	The rapid growth of the Internet of Things (IoT) in Indonesia necessitates the implementation of robust security measures to prevent DDoS attacks, such as the use of Anti-DDoS technology.

Source: Processed by the Author (2024)

The data presented in the table above interprets the potential of various types of cyber threats, including Ransomware, Data Leaks, APT Attacks, Phishing, Cryptojacking, DDoS, RDP Attacks, Social Engineering, Artificial Intelligence (AI), IoT Cybercrime, and Web Defacement. These threats are motivated to destabilize a country's government, thereby transforming into crucial, strategic, and urgent threats.

These threats are designed to gain control of users' systems, including the corruption, modification, and deletion of data on web pages, as well as the perpetration of fraud, extortion, and online gambling. The consequences of these actions can be far-reaching, including the paralysis of critical infrastructure, theft of sensitive government, financial, and health data, economic instability resulting in lost productivity, and negative influence on political processes such as elections (**see Figure 2**).

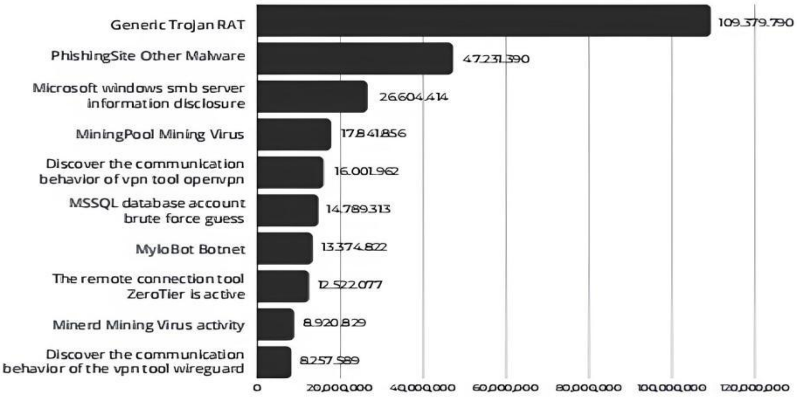

Figure 2. Top 10 anomalous traffic in 2023 (Id-SIRTII/CC, 2023).

The illustration above interprets the highest type of anomalous traffic, namely Generic Trojan RAT. This anomalous traffic activity can have a detrimental impact on device and network performance, the theft of sensitive data, damage to an organization's reputation, and a decreased level of trust in the organization. The Id-SIRTII/CC BSSN 2024 report provides a more detailed explanation of the cause, indicating the presence of backdoor communication activities with malicious domains. These malicious domains are identified as command and control servers belonging to threat actors.

As elucidated in a more comprehensive analysis by BSSN in 2024 through the Cybersecurity Landscape Book 2023, such instability can result in a loss of internal authority, thereby rendering the Indonesian state vulnerable to external influences and hindering the implementation of government strategies. BSSN has identified several cases of cybercrime perpetrated by government agencies in Indonesia. These cases demonstrate that cybercriminals target government administrative systems as their primary objective.

One particularly notable example is the use of ransomware as a means of extortion. Arguably, the most disruptive criminal activities in cyberspace historically have involved types of cyber-attacks such as ransomware. These attacks not only threaten public services and security, including increasingly vulnerable critical infrastructure, but also have the potential to spark conflict between countries (Hansel & Silomon, 2024).

The aforementioned categories of cyber threats have the potential to facilitate the theft of data, gain unauthorized access to systems, and cause damage. Failure to anticipate these threats can have a significant impact on social functions. Moreover, these consequences can become strategic negation targets that systematically destabilize the life of the state. In De Joode's (2011) theory, such instability encompasses social and financial stability, which can be particularly detrimental to sensitive information and personal data.

The strategic cyber threat to non-military intelligence is a result of the inherent vulnerabilities of internet platforms, generated by factual and potential cyber threats because of cyber warfare. These vulnerabilities include the creation of cyber espionage, propaganda, disinformation, and post-truth phenomena through social media. Johnson (2024) posits that cybersecurity is designed to combat the proliferation of disinformation on social and other media. Disinformation is the dissemination of false information and the promotion of fictitious technologies. These tactics are intended to undermine the stability and integrity of a country with the objective of disrupting and ultimately destroying the target country.

In the future, the pace and acceleration of cyber threat development is predicted to exceed current deterrence capabilities. As a preventive measure, a defense system in cyberspace can be created by integrating all components of national defense. This will entail an expansion of Indonesia's defense system beyond its current focus on the military to encompass non-military elements.

The State Defense Doctrine Book in 2014 defines non-military defense as the involvement of ministries and agencies outside the defense sector in addressing threats that include ideological, political, economic, socio-cultural, technological, and security dimensions. This approach provides a comprehensive defense strategy through a clear and common understanding of the duties, obligations, and roles of each party involved in the implementation of cyber non-military defense.

This aligns with the State Defense Strategy Book in 2014, which underscores the significance of a unified comprehension of actual and prospective cyber threats among non-military intelligence agencies. The absence of a shared understanding will inevitably result in bureaucratic challenges to synergy among non-military intelligence services in countering cyber threats.

Cragin (2015) theory identifies the potential application of non-military defense concepts to proxy wars. This approach is predicated on the assumption that a state can be weakened by not directly engaging in combat with its military forces. Within the context of the cyber domain, non-military intelligence institutions assume a role in non-military defense through protecting national strategic assets.

An indispensable element in non-military cyber defense is the availability of human resources. The researcher obtained information from informants indicating that the majority of cybersecurity operational activities are carried out by less qualified human resources, as well as vendors who are not organic employees and are not experts in the cyber field. Another noteworthy aspect is that central government agencies have a composition of cyber talent with a focus on information and technology-based expertise, while local government agencies tend to lack competent cyber human resources. This suggests that the quality of human resources with qualified cyber competencies should also be a priority.

Currently, the Indonesian government lacks a policy to provide independent software, Artificial Intelligence (AI), and Internet of Things (IoT) platforms, as well as servers and search engines, to anticipate the development of cyber threats. This is another reason why Indonesia is susceptible to hacking. Hernandez Ramos et al. (2024) propose that a government should implement a new legislative framework that establishes a set of cybersecurity requirements that organizations should implement. The established requirements should be translated into harmonized standards, which will serve as a reference for cybersecurity specifications for cyber device manufacturers to follow. As further standardization efforts are undertaken to identify the most relevant cybersecurity standards, it is essential to consider the level of coverage and gaps, as well as the harmonization required to ensure comprehensive and consistent horizontal coverage with potential remaining gaps.

As the agency responsible for addressing cyber incidents, BSSN has taken proactive measures to enhance the awareness of cyber threats among government agencies. Nevertheless, these initiatives are constrained by the necessity for time to enter the implementation phase. This is further compounded by the fact that BSSN tends to prioritize the provision of cyber products over the implementation and operational stages, which are usually the responsibility of task forces in regional agencies.

A significant challenge in addressing the reality of factual and potential cyber threats is the absence of comprehensive cybersecurity regulations in Indonesia. Presently, there exists only a draft law in addition to the recently released Presidential Regulation as a suitable response to the evolving cyber threats and necessary for maintaining cybersecurity stability (Ramadhianto et al., 2023). The enactment of this legislation is of paramount importance for establishing a standardized level of cyber assessment and creating optimal cybersecurity. This is essential to ensure objectivity and prevent subjective assessments.

Without expeditious implementation, the Indonesian non-military Intelligence Community (IC) will confront significant challenges to develop a comprehensive non-military defense in cyberspace. This will compromise the basic principles of national security, as outlined by Silalahi (2005) in his implication theory, where a comprehensive framework for maintaining domestic stability from various threats, including those posed by cyber-attacks, is considered critical and necessary, aiming to defend the values and identity of the country.

Generally, the evolution of the motives, methods, and actors involved in cyber threats to national security, both factual and potential, is proceeding at a rapid pace, creating uncertainty about the nature of these threats. This uncertainty, coupled with the increasing rate of acceleration, exacerbates the situation and will have a significant impact on Indonesia's national security in the future.

The lack of a robust legal framework for cybersecurity is identified as a critical factor hindering the effectiveness and efficiency of efforts to deter actual and potential cyber threats. If not properly addressed, these threats can lead to hoaxes, disinformation, and online fraud, which can escalate into conflicts that disrupt national stability, as evidenced by the outbreak of cybercrime.

There are several ways to address it, such as compromising threat actors in every cyber-attack. Moreover, raising public awareness is essential not only to maintain cybersecurity, but also to prioritize potential and factual cyber threats as national security threats.

Referring to the above, the current level of cyber defense in Indonesian non-military Intelligence Community (IC) is still far from the ideal concept of cyber intelligence beyond the military aspect to anticipate possible ideological, political, economic, socio-cultural, and defense and security threats that could endanger the sovereignty, integrity, and security of the nation. The difficulties encountered in the process of deterring actual and potential cyber threats, as outlined previously, indicate that in the future the government must prioritize initiatives such as developing qualified and diverse cyber intelligence talents in various sectors, allocating budgets for modernizing cyber intelligence equipment, and establishing a cyber security law as a legal framework.

The practical implications of the research results in this sub-chapter are significant for increasing the efficacy of cybersecurity, which relies on the Indonesian government and related stakeholders' readiness to conceptualize cybersecurity. This readiness encompasses budgetary allocations for cyber infrastructure, institutions that become cyber stakeholders, and the qualification of human resources who are experts in the cyber field for the non-military Intelligence Community (IC) in Indonesia.

While the theoretical implications are in the form of increased situational awareness for the public as well as academics and cyber and intelligence practitioners, the research also has implications for the prioritization of potential and factual cyber threats. These implications suggest that these threats should be considered crucial, strategic, and urgent threats to national security.

Although this research can provide implications for new findings, there are limitations as the next dynamics develop and the number of cyber incidents that are periodic. This means that the number of incidents is potentially more extensive and complicated in the future, which certainly raises concerns. This aspect of the study is under-examined, indicating the need for further research focusing on the development of strategic policy references and guidance for non-military intelligence agencies operating in cyberspace.

4.2. Intelligence Security Function Strategy in Strengthening Indonesian Non-Military Intelligence Community (IC)

The results of this sub-chapter interpret the strategy of the intelligence security function in cyberspace as a critical aspect of non-military intelligence activities, especially in relation to counterintelligence that can affect the entity of state assets towards national security stability. In the context of intelligence, prioritizing attention to cybersecurity strategies and the urgency of threats posed through cyberspace is a requisite aspect of any effective intelligence operation.

A review of the State Intelligence Law Number 17 of 2011 reveals that the state intelligence institution is responsible for the execution of intelligence functions and activities. The purpose of the state intelligence organization within the Indonesian constitutional system is to fulfill the duties and authorities entrusted to it and to elaborate the national objectives that underlie the formation of the Indonesian state.

Prunckun's (2014) theory of intelligence posits that intelligence is an organized system for managing information. Concurrently, the gathering of information enables the identification of foreign institutions as potential threats or adversaries. Accordingly, Lerner & Lerner (2004) proposes the implementation of counterintelligence measures to secure the country's valuable assets. In this regard, strategies are designed to protect assets from the impact of cyber threats.

In the context of non-military defense involving intelligence agencies, Supriyatno (2014) defense management theory postulates that before implementing a strategy, potential national resources must first be allocated to benefit national defense. From the perspective of personnel management, the efficacy of non-military intelligence hinges on the implementation of regulatory frameworks, the provision of guidance and support from national leaders, and the deployment of competent and professional cyber human resources, as proposed by George Terry's (1972) management theory.

BIN, in its capacity as the coordinator of non-military intelligence, must collaborate with the Central Intelligence Committee Meeting and Regional Intelligence Committees, as well as BSSN and Kominfo, to enhance the coordination mechanism to mitigate the impact of cyber warfare. BIN facilitates the coordination process of organizing Indonesian non-military Intelligence Community (IC) to counteract cyber threats. The Central Intelligence Committee and Regional Intelligence Committee convene monthly or as circumstances dictate. The meetings include representatives from non-military intelligence agencies at both the central and regional levels. These agencies include the Ministry of Communication and Informatics (Kominfo), the Municipal Resort Police (Polresta), the National Resilience Council (Wantannas), and the Immigration Intelligence of the Ministry of Law and Human Rights (Kemenkumham). Regular coordination meetings are held with the Coordinating Ministry for Political, Legal and Security Affairs (Kemenko Polhukam) for the purpose of discussing special issues related to cyber threats, specifically those involving non-military intelligence.

In the meantime, BSSN, as the cyber-leading sector, and other related institutions, such as Kominfo, have the authority to coordinate with BIN, the state intelligence coordinator, to handle cyber threats. BIN collects materials in the form of cyber information exchange and cyber policy based on the results of the Central Intelligence Committee Meeting and Regional Intelligence Committee Meeting. However, it does not include work programs in the cyber field that are coordinated with BSSN for follow-up to maintain the confidentiality of intelligence agencies. Since the cyber task force coordinating BIN, Kominfo, and BSSN has not been operational for a long time, the government must pay high attention to this matter.

The implementation of intelligence activities to detect cyber threats must be conducted in a manner as discreetly as possible. However, it is also important that the intelligence structure responsible for cyber information adheres to the authority and respects the functions of the state institutions responsible for cyber security. While the data and information obtained from intelligence activities in cyberspace can be sourced from both open and closed sources.

Kunarto (1999) theory argues that intelligence organizations are distinct from other organizations due to their exclusive nature, which is analogous to clandestine operations. This has implications for the regulatory framework of intelligence, which has multiple objectives, including the mitigation of cyber threats to national security. Therefore, it is of the utmost importance to prioritize the development of regulations that can effectively achieve these objectives. This will enable non-military intelligence organizations to produce relevant and valuable products that can assist policymakers in the decision-making process.

It can be stated that non-military intelligence services require a cyber counterintelligence function to enhance their organizational security capabilities. These agencies implement intelligence security functions in the form of preventive measures, such as data backup, to anticipate emergencies and mitigate the disruption process. This reduces the potential for conflict due to cyber threats.

Researchers such as O'Connor (2022) and Bodström (2022) have examined the application and development of counterintelligence methods to address the evolving cyber threats posed to national security, with the aim of attaining higher levels of cybersecurity. Their findings indicate that it is indispensable to prioritize the implications of cyber threats on socio-cultural and ideological aspects, while simultaneously acknowledging the significance of considering economic, political, and defense and security aspects, as well as potential threats to national security.

To ascertain the efficacy of the Indonesian non-military Intelligence Community (IC)'s security function in countering cyber threats and fortifying organizational management, a comprehensive evaluation of each phase of the intelligence cycle is imperative. This analysis will elucidate the complexity of a cyber incident, wherein BIN's counterintelligence and cyber intelligence fields analyze cyber threats such as hacking and conduct threat identification activities. This analysis is predicated on the potential threat, not on subjective evaluation.

The security function is supported by the annual intelligence forecast, which predicts cyber threats for the following year by identifying potential massive cyber threats. The intelligence security function consists of various covert groups that conduct rapid assessments to mitigate potential losses caused by cyber threats. As stated by Hendropriyono (2013), the intelligence security function includes counterintelligence and preventive measures. These measures are based on rapid assessments designed to mitigate potential losses caused by cyber threats.

As the strategic landscape becomes increasingly connected to cyber platforms, non-military intelligence is undergoing a transformation in its role (**see Table 5**). Thus, it is imperative to strengthen the management of non-military intelligence organizations through strategic levels covering aspects of coordination, organization, and technology to respond adequately to these challenges.

Table 5. Strategic aspects to strengthen management of the non-military IC.

No	Aspects	Sub-aspects	Description
1	Coordination	Harmonizing	The efficacy of coordination meetings in countering cyber threats, with a particular focus on the objectives of each non-military intelligence agency, these meetings are coordinated by BIN, which serves as the State Intelligence Coordinator.
		Synchronizing	Indonesian non-military IC along with BSSN and Kominfo must be supported by integrated and non-overlapping policy regulations, moreover, cyber intelligence talents who are objective and impartial not just competent and professional must be allocated to counter cyber threats.
		Synergizing	There will be no non-military intelligence organizations in Indonesia that move individually and feel super-powered or still prioritize sectoral ego, thus, it can work in accordance with the course of non-military intelligence organizations based on applicable regulations.
2	Organization	Dividing Tasks on the Security Intelligence Function (Capable of effectively and efficiently carrying out intelligence activities, including information gathering, analysis, assessment, and dissemination, for the non-military IC to conduct various counterintelligence tasks in cyberspace.).	Security Planning: The formulation of the primary elements of information (UUK) related to personnel, material, and activities that present a challenge to the leadership, the implementing level then seeks to identify solutions to these problems, the issue is concerned with the capabilities and weaknesses of the opponent and the potential actions that the opponent may take within the cyber domain.
			Security Implementation: Routine security measures include continuous cyber patrols provided by BIN to monitor personnel, materials, information, and intelligence operations, in contrast, counterintelligence operations are employed to implement non-routine security measures to detect specific cyber incidents within a certain timeframe.
			Security Results Processing: The incorporation of reports on cyber threats, derived from a diverse array of data sources, including open and covert sources, is a crucial aspect of this process, subsequently, the information will be recorded, processed, analyzed, interpreted, and assessed in relation to the source and its content.
			Security Results Presentation: The report presents cyber intelligence products that must prioritize the principles of *velox et exactus* to the leadership through both verbal and nonverbal means. It covers the development and achievement of targets and operational activities related to cyber security tasks, including guidance and cyber security operations.

No	Aspects	Sub-aspects	Description
		Responsibilities on the Security Intelligence Function (Implementation of counterintelligence in cyberspace to maintain state secrets for targeting personnel, material, information material, and cyber intelligence operations).	Personnel Security: Preventing the infiltration of opposing elements into the personnel structure of the non-military intelligence organization via the cyberspace domain.
			Material Security: To conceal cyber intelligence materials stored in secure storage with multiple levels of security, thereby preventing the opposing party from gaining access to the non-military IC cybersecurity system, achieved by minimizing the potential loss in the event of a cyber access breach, which remains inevitable.
			Information Materials Security: To prevent the information from falling into the hands of opposing parties, confidentiality must be maintained, it includes classified documents resulting from intelligence operations in cyberspace, which contain objects, leadership records, and defense force mapping.
			Cyber Intelligence Operations Security: To guarantee the confidentiality of cyber intelligence operations, achieved by maintaining freedom of action, which prevents the enemy from conducting strategic interventions and accessing organizational information materials.
		Authorities on the Security Intelligence Function	BIN provides collaborative cyber counterintelligence operations through units and joint tasks in coordination with non-military IC to secure assets against cyber incidents.
3	Technology	-	The procurement of technologically advanced cyber equipment is becoming increasingly important in the context of cyber counterintelligence operations, this is due to the growing capacity and development of technology used in cyber-attacks.

Source: Processed by the Author (2024)

As illustrated in the table above, the data interprets various aspects of strengthening for the Indonesian non-military Intelligence Community (IC). Initially, the Indonesian non-military Intelligence Community (IC) creates harmonization among its members, led by BIN, then be able to create synchronization with institutions outside its membership in handling cyber threat issues. To achieve a unified approach, based on the agreed-upon provisions, it is necessary to coordinate the efforts of all parties involved.

In terms of organizational structure within the Indonesian non-military Intelligence Community (IC), the division of tasks is determined to implement the intelligence security function in each non-military intelligence agency based on the scope of each agency with regard to cyber security. The implementation of cyber counterintelligence tasks is accompanied by an emphasis on the aspect of awareness among non-military intelligence agencies regarding the necessity of securing their assets as a form of shared responsibility. These two aspects must be subject to the authority of BIN, as the coordinator of counterintelligence collaboration activities among the Indonesian non-military Intelligence Community (IC). The security intelligence function strategy outlined above can be optimally executed in conjunction with the support of sophisticated and capable cyber equipment that is continually updated to reflect technological advancements in cyberspace.

Based on Presidential Regulation Number 63 of 2017 on the State Intelligence Coordination, non-military Intelligence Community (IC) in Indonesia is established with the objective of enhancing the credibility of non-military intelligence. In this context, it is imperative to optimize the inter-agency collaboration process within the Indonesian non-military Intelligence Community (IC) to provide valuable knowledge as input for policy formulation at the state leadership level more quickly, precisely, and accurately.

The optimization of the inter-agency collaboration process within the Indonesian non-military Intelligence Community (IC) can be realized through effective coordination among their members in dealing with cyber threats. Such coordination must encompass an understanding of sources, nature, and forms of cyber threats, as well as various trends that may emerge as a joint response to the dynamics of the strategic environment that continue to develop at the national, regional, and global levels. This aligns with (Malone & Crowston, 1994) theory of coordination regarding the governance of relationships that share a common goal.

Ateş & Erkan (2021) and Cline (2022) have conducted research on the coordination aspect of intelligence organizations, particularly in terms of reviewing and developing cooperation among intelligence services. Although both studies emphasize coordination, they differ in the scale of the intelligence services studied. The research primarily concerns multilateral foreign intelligence entities.

The State Intelligence Law Number 17 of 2011 defines coordination as the process of aligning functional relationships and synchronizing efforts and synergies in the implementation of intelligence activities to achieve objectives. From a theoretical perspective, the coordination mechanism in countering cyber threats can be idenitified through three primary aspects, such as harmonization, synchronization, and synergy. These three aspects are applied by the Indonesian non-military Intelligence Community (IC) according to the national standard system, which includes basic intelligence, current intelligence, and national intelligence estimates.

To be efficacious, the strategic steps of cyber threat detection must focus on the coordination scheme between parties involved in non-military intelligence activities, a scheme not currently considered optimal. The development of cyber intelligence cooperation continues to pose a challenge, primarily due to the lack of an effective organizational structure for non-military intelligence.

At each phase of the process of strategic planning, discussion, implementation, and evaluation, the coordination between non-military intelligence agencies in dealing with cyber threats has not been aligned with their main tasks and functions. Moreover, the implementation stage of cyber threat management has not been conducted professionally. These issues are evidenced by indications of interest, overlapping information, and sectoral ego in information exchange. The prevalence of sectoralism within the bureaucratic culture is a significant contributing factor to the challenges encountered between ministries and institutions.

Based on the preceding analysis, it can be reasonably asserted that the coordination process among Indonesian non-military Intelligence Community (IC) must be reinforced by mutual trust and effective performance. Performance demands represent a significant concern and a prominent area of study in the field of organizational management. This argument is further reinforced by Radin (2000) coordination theory and Vigoda-Gadot & Cohen (2004) explanation that coordination generates performance by fostering the trust needed to achieve it through networks.

Alternatively, intelligence can be defined as the organizational entity responsible for the collection and analysis of information to meet the needs of policy-making officials. This encompasses preventive measures to secure information and analysis through internal activities and counterintelligence measures based on the mandate of Law Number 17 of 2011 on the State Intelligence.

The rationale behind these precautions is to facilitate the non-military Intelligence Community (IC)'s achievement of its desired outcomes. This conforms to the organizational theory proposed by Mondy (1990) and Wijayanto (2013), which posits that organizations are constituted via structured relationships to attain predetermined objectives. Furthermore, another organizational theory proposed by Freeman & Hannan (1989) postulates that organizational goals can be multifaceted, encompassing a multitude of specific objectives. The objectives of the non-military Intelligence Community (IC) in Indonesia are similar and interrelated, although in the implementation stage, there are differences according to the tasks and functions of each intelligence organization in the non-military field.

In relation to the above, Trim & Lee (2021) conducted research on the governance of the organization, emphasizing the efficacy of the management process in mitigating the impact of cyber threats through qualitative research. The study differs from the extant research in locus, as it has a global scope and focuses on the internal actions of leaders and staff of intelligence agencies.

Organizing the non-military Intelligence Community (IC) to perform intelligence security functions in cyberspace requires a structured approach to collaboration, division of tasks, responsibilities, and authorities to achieve specific goals. The Law Number 17 of 2011 on the State Intelligence delineates the distinction between the intelligence security function, which is further divided into the domains of prevention and intelligence operations. Deterrence is a strategy employed to secure internal assets, including personnel, physical materials, and information materials. In the context of cyber threats, the intelligence-guarding function of any non-military BIN member must be based on the intelligence cycle at all times.

According to Article 10 of the 1945 Constitution, intelligence is a civilian institution distinct from military intelligence. Its primary responsibility is to conduct intelligence activities, including security functions, to build a strategic analysis system. Article 1 of the General Provisions Chapter of Law Number 17 of 2011 on the State Intelligence defines intelligence as a juridical organization that formulates policy, develops national strategy, and makes decisions based on analysis of information and facts collected through various working methods, including detection and early warning in security functions.

As an organization, non-military intelligence must be able to counter cyber threats by assessing, identifying, analyzing, and providing information on potential cyber threats. Such intelligence serves as an early warning to policymakers, enabling them to act quickly and in a manner that is aligned with national security interests. The overarching objective is to preclude the occurrence of strategic impediments to the safety of the nation and state.

In the realm of cyber threat deterrence, intelligence is defined as the collection, processing, and interpretation of information with the purpose of planning and securing an organization's facilities against potential cyber threats. Such facilities include personnel, material, information, and operations. Non-military intelligence organizations are susceptible to a multitude of cyber-attacks, including espionage, sabotage, and conditioning attacks, perpetrated by a diverse array of adversaries, including foreign intelligence services, state-sponsored actors, and non-state-sponsored actors.

It is insufficient to posit that non-military intelligence can effectively counter cyber threats without adequate and high-quality human resources. Nevertheless, the presence of other intelligence resources, such as technologically advanced cyber equipment, can be employed as a supplementary support. Consequently, the Indonesian non-military Intelligence Community (IC) must provide support to government policies in the adaptation of renewable cyber technologies.

Previous research has addressed the intelligence community's commitment to technology development by proposing strategies for strengthening collaboration among intelligence technology stakeholders. Moran et al. conducted research on this topic in 2023. However, the distinction between this research and the previous research is that the previous research focused on the intelligence community in the United States, while this research examination focuses on the same in Indonesia.

The intelligence security function is inextricably linked to counterintelligence activities. Therefore, strengthening non-military intelligence organizations in the context of cyber threats will not be optimal if not accompanied by strengthening cyber counterintelligence capabilities. Conversely, the development of a robust cyber counterintelligence capability is contingent upon the establishment of a robust non-military intelligence organization. This is due to the evolving nature of the threat landscape, resulting in the evolution of cyber counterintelligence as a cybersecurity effort (Duvenage et al., 2018).

The two entities are closely related and mutually reinforced, as they collectively secure state secrets through a series of cyber counterintelligence operations facilitated by the procurement of advanced cyber technologies. In response, Indonesian non-military Intelligence Community (IC) has developed the institutional capacity to collect technology-based intelligence on cyber threats. Such capacity has a significant impact on the analysis and dissemination process within the intelligence cycle.

In more detail, Duvenage and Von Solms (2014) provide a comprehensive description of both defensive and offensive counterintelligence tactics and strategies. Defensive operations disseminate information and serve as a trigger to warn the offensive party. Offensive operations provide the foundation for a proactive defense configuration. The spectrum of other measures lies between passive-defensive and active-offensive, including pre-employment personnel security, in-service personnel security, technical surveillance countermeasures, encryption, surveillance (physical, static, mobile, and electronic), double agents, and continuous monitoring. As the prevalence of hostile cyber actions increases, counter-exploitation also becomes a more significant concern.

Upon reflection of the presented explanations, the necessity for the implementation of strategic measures within the non-military cyber intelligence security function, alongside the increasing capacity and sophistication of the technology utilized in cyber-attacks, becomes increasingly evident. This assertion aligns with the findings of Mattern et al. (2014). In the context of contemporary technology, those engaged in counterintelligence operations must ensure the proactive application of cybersecurity measures (Clark & Mitchell, 2018; National Security Agency, 2023). Consequently, the Indonesian non-military Intelligence Community (IC) must be capable of utilizing sophisticated cyber tools and other counter-surveillance equipment of a high complexity scale.

In principle, surveillance technology is developed with the objective of collecting information about specific entities or individuals. Subsequently, the information is systematically and rationally analyzed, with the resulting output being used to influence the behavior of the surveillance target (Ball, 2021). Therefore, to effectively counteract surveillance with a high level of technological sophistication, it is necessary to possess a robust capacity to reverse the data that has been collected and analyzed. This is to ensure that the influence of irresponsible parties is mitigated. As proposed by Chuter (2011), the implementation of a new system of tools in cyber intelligence activities will result in a more comprehensive direction and administration of the national security system.

The non-military intelligence security function must be capable of providing timely and targeted warnings to policymakers to prevent cyber strategic threats that could endanger citizens, the nation, and the existence of the state. The prioritization of the security function of non-military intelligence is indispensable for the protection of state assets from cyber exploitation and the reduction of potential losses resulting as a consequence of cyber incidents.

This sub-chapter presents the theoretical implications of the research results, providing knowledge for the public and input for academics and practitioners regarding the causes of the non-military intelligence security function's strategy not to integrate with cybersecurity issues. Governance of non-military intelligence in detecting cyber threats in Indonesia is still not optimal. Practically, the implications of this research are for Indonesian non-military Intelligence Community (IC) regarding strategies to establish a formal focal point in the regulation and development of cybersecurity. Currently, this is being implemented through various cybersecurity programs. The findings also indicate that to comprehensively address cyber issues, it is possible to increase the involvement and access to non-military methods that play a very strategic role to ensure national security stability from all forms of cyber threats.

Despite the contribution of this research to the field of non-military intelligence security strategy, there are limitations to be considered. One such limitation is the lack of research on the juridical aspects of cybersecurity, as highlighted by Bendovschi (2015). Eventually, further research is required regarding the regulation and management of non-military cyber intelligence from a legal perspective. This will serve to reinforce non-military intelligence and idenitfy its place within the more significant context of Indonesian governance.

4.3. Challenges and Obstacles Faced by Indonesian Non-Military Intelligence Community (IC) in Detecting Cyber Threats

The research results in this sub-chapter interpret the non-military Intelligence Community (IC) in Indonesia continues to confront a multitude of challenges and obstacles in the cyber threat detection process. Therefore, strengthening the organization in terms of effectiveness and efficiency of non-military intelligence as well as determining threat priorities by the government is pivotal to comprehensively detect cyber incidents in the context of Indonesia's national security.

The government's priorities include budget allocations for cyber infrastructure, cyber-stakeholders' institutions, and the quality of human resources who are experts in the cyber field. In addition, the lack of a robust legal framework for cybersecurity is perceived as a significant impediment to the effectiveness and efficiency of cyber threat detection efforts by non-military intelligence in the future. Indonesia currently lacks a specific law governing cybersecurity, although there is a draft law and a Presidential Regulation. The improper handling of this threat could potentially lead to conflicts that would destabilize national security, as evidenced by the outbreak of cybercrime.

As an integration of cyberinfrastructure, previous research by Gioe et al., (2020) demonstrated that technological advancements in response to the dynamics of the strategic environment affect intelligence challenges and obstacles in the current era. However, the study focused more on the fusion of the traditional intelligence cycle and the implementation of offensive cyber intelligence operations in Anglo-American countries, in contrast to the more passive doctrine in Indonesia as presented in this study.

The Indonesian intelligence function is organized by various government agencies or non-ministerial government agencies, according to their primary responsibilities. As a provider of comprehensive policy recommendations for effective organizational management to provide stimulus related to factual and potential cyber threats, intelligence plays a strategic role at the government leadership level (Prunckun, 2014). Nevertheless, it is evident that not all state intelligence providers fully perform the intelligence function as stipulated in Law Number 17 of 2011 on State Intelligence.

A review of the concept of coordination as outlined in the State Intelligence Law is necessary, as it may potentially lead to several obstacles that could impede the optimal implementation of non-military intelligence activities in the future. Non-military intelligence organizations frequently adhere to existing coordination schemes yet fail to adapt to the nature and form of cyber threats, which are characterized as being extremely fast, extensive, and integrated. Failure to resolve this issue will impede the capacity of non-military intelligence organizations in Indonesia to promptly and accurately identify cyber-attack incidents.

Non-military cyber intelligence activities represent a critical element of a country's defense system. It provides forecasts and warnings to policymakers based on in-depth strategic analysis of cyber threat sources, including motives, objectives, identity, organizational structure, sources of support, and weaknesses.

In the context of cyber incident management, threats are rapidly and intricately integrated into various sectors. Hence, a non-military intelligence service must be cognizant of its security systems and collaborate with other non-military intelligence services to establish parameters for information exchange.

Indonesian non-military Intelligence Community (IC), in collaboration with BSSN and Kominfo, has assumed a pivotal role in the review of cyber data. Cyber threat analysts are tasked with the assessment, identification, and analysis of potential and factual cyber threats. They furnish data on the nature and form of threats, as well as early warnings, to national cybersecurity policymakers. The objective of this initiative is to develop prompt and appropriate policies to prevent the emergence of strategic obstacles in cyberspace, thereby ensuring the safety and security of the country.

Although non-military intelligence organizations have been established at the legal level, the operational effectiveness and dissemination of cyber intelligence information to the intended recipients are often hindered by overlapping responsibilities and sectoral egos among different agencies. This is due to the ego-sectoral nature of intelligence functions between one agency and another, which remains an obstacle to intelligence coordination. As a result, the synchronization of non-military intelligence agencies to counter cyber threats is impeded by sectoral ego at the leadership level and compartmentalization at the operational level. This ego-based approach results in each non-military intelligence agency acting independently in dealing with cyber incidents.

Furthermore, the persistence of a competitive nature impedes the capacity of the non-military Intelligence Community (IC) in Indonesia to collaborate effectively in the detection of cyber threats. Each agency asserts its own importance and authority to anticipate cyber threats. To effectively combat cyber threats and fulfill their duties, non-military intelligence agencies must suppress their sectoral egos.

The issue of bureaucracy is also inextricably linked to this problem. The culture of sectoralism remains a significant contributing factor to the complexity of the problem. Ineffectiveness can be attributed to a number of factors, including insufficient human resources, ineffectual policies, or a lack of political diplomacy. Hence, effective programs, rigorous supervision, and unwavering commitment from the respective leaders are essential to fortify institutions in facing cyber threats.

Non-military intelligence organizations will encounter significant challenges in their capacity to respond to strategic disruptions in cyberspace and will face obstacles in analytical initiatives if BIN analysts, as the Intelligence Community (IC) coordinator, and users of intelligence products are hindered by rigid and lengthy bureaucratic structures in the coordination process. These obstacles can be identified implicitly in Presidential Regulation Number 67 of 2013 on the Coordination of National Intelligence.

The regulation establishes the Regional Intelligence Agency as the coordinator of regional intelligence, which is carried out by the Head of the Regional Intelligence Agency. In addition to these bodies, there is a Regional Intelligence Committee that serves as a forum for coordination meetings. The meetings are attended by the Head of Intelligence of the Regional Police, the High Prosecutor's Office, the National Unity and Political Agency, and the Heads of Ministries and Non-Ministerial Institutions in the regions. A multitude of parties involved in the coordination system inevitably leads to increased complexity when operationalizing cyber-attacks, given the necessity for urgent responses.

The Regional BIN's human resources are comprised of talented professionals occupying functional roles. Nevertheless, the lengthy bureaucratic processes can impede the analytical capacity of analysts, rendering the utilization of intelligence analysis challenging. This can potentially occur when the bureaucratic separation between the intelligence analyst and the head of the intelligence coordinating agency is too extensive. In the case of intelligence products that require rapid delivery to the user, a lengthy and time-consuming process can result in the intelligence product losing its intended value.

As a consequence, inaccuracies in the process of interpreting information related to cyber threats can have a significant impact on the development of information collection schemes and the optimization of early detection systems. This is reflected in the position of the Central and Regional Intelligence Committees as a non-military Intelligence Community (IC) that has mechanisms to exchange information, coordinate meetings, and verify data to counteract cyber incidents. Such a position is potentially threatened due to the risk of data misinterpretation as well as the limitation of not always providing highly classified information.

To address these issues, it is recommended that regular coordination meetings are held to facilitate communication, thereby institutionalizing information sharing at the operational level. This is preferable to relying on individual or interpersonal networks, as this may result in information embargoes or blockades by dominant intelligence agencies. A balanced approach to information sharing is essential to ensure that all parties concerned have access to the necessary information.

A further significant obstacle to the coordination process is the absence of legal consequences such as sanctions for agencies authorized in the cyber prevention and enforcement action-taking mechanism. This may result in the inability to implement actions after receiving reports and data analysis from BIN personnel. Moreover, BIN’s strategic position regarding the functions and tasks pertaining to cyber intelligence also presents potential weaknesses in terms of oversight. BIN lacks the authority to oversee cyber intelligence matters, as this is the purview of the cyber division of each intelligence agency.

When faced with an emergency, even when circumstances require departure from the rule of law, it is critical to ensure that any actions taken by BIN are objective and in accordance with legal guidelines. The preceding case studies illustrate the potential challenges to the efficiency and effectiveness of non-military intelligence in the cyber domain. This implies the necessity of updating state intelligence regulations.

Non-military intelligence agencies ought to prioritize the protection of national security interests. To reduce the potential impact of cyber incidents that could threaten national security, it is necessary to enhance the authority of BIN to facilitate the coordination process and empower it in the cyber response mechanism.

The Indonesian non-military Intelligence Community (IC) faces significant cybersecurity challenges in detecting cyber threats. The utilization of foreign cyber equipment introduces potential risks due to the dependence on foreign-made technology. Although these devices are more advanced and sophisticated than conventional equipment, the security vulnerabilities of the Indonesian Intelligence Community (IC)'s systems can be exploited by foreign intelligence agencies through the portals embedded in foreign-made intelligence equipment. This is a paradoxical situation – while the intention is to conduct espionage against foreign entities, such actions can inadvertently result in the disclosure of secret information to foreign intelligence agencies.

The Cybersecurity and Infrastructure Security Agency (CISA) recommended in its 2017 report that efforts to improve cyber-infrastructure resilience can be achieved through systemic risk management and reduction, establishment of partnerships with the private sector, collaboration with the public sector, and protection of federal government networks. Moreover, Cybersecurity and Infrastructure Security Agency (2017) recommends technical cyber-infrastructure measures that include the following: mitigation strategies for customers of managed service providers, such as managing supply chain risk and managed architecture risk, implementing robust operational controls, and administering effective authentication, authorization, and accounting procedures. Mitigation strategies for managed service providers should include banning deleted Dynamic Link Libraries (DLLs), enforcing restricted directory usage, implementing tools to detect search order hijacking opportunities, and utilizing application whitelisting to block unknown DLLs.

This reliance on cyber equipment from other countries potentially poses a threat to the cybersecurity system of Indonesian non-military Intelligence Community (IC), which is responsible for the maintenance of state secrets. To mitigate these risks, it is indispensable to implement a multi-layered system of oversight and accountability to supervise and regulate the implementation of intelligence security functions in a targeted and measurable manner, particularly regarding cyber threats to national security. Intelligence providers, in particular those operating outside the military domain, must be able to effectively gather global information and implement preventive measures in cyberspace.

Another challenge is ensuring that personnel in the non-military intelligence sector possess the requisite cyber competencies. Indonesian non-military Intelligence (IC) community should employ personnel trained in counterintelligence tactics and operations, as well as relevant expertise to develop effective counterintelligence procedures (Cybersecurity and Infrastructure Security Agency, 2020). Moreover, enhancing the operational intelligence culture and equipping personnel and executives within non-military intelligence organizations with the proficiency to develop more technical skills is essential.

Intelligence culture aims to reinforce the substantive values of intelligence based on a set of shared values and operational functions, shaping perceptions of right and wrong. It encourages intelligence personnel to prioritize the smooth operations and security of Indonesian non-military Intelligence Community (IC), even in the face of routine difficulties and problems (Kanellopoulos, 2022).

Concurrent with those efforts, it is critically important to provide technical training for personnel and executives on the operation of the Internet of Things (IoT), Machine Learning (ML), Artificial Intelligence (AI), and other digital softwares, which are leveraged as decision-making tools and the bedrock for optimizing the role of intelligence in supporting the stability of national security. Ramadhianto et al., (2023) identifies one of the advanced technologies, Machine Learning (ML), as a promising tool for collection, processing, and analysis of intelligence activities. Specifically, it can be leveraged for speech-to-text transcription, including the identification of human speech in noisy environments and cross-language translation.

A robust operational intelligence culture, encompassing both security and counterintelligence functions, is fostered through a continuous observation of the evolving security landscape. Furthermore, it must be able to adapt to new and emerging technological developments that create new security threats and operational opportunities.

The efficacy of cyber counterintelligence is contingent upon the expertise of qualified cyber professionals, whose meticulous analysis of processed information is critical in the context of the voluminous and dynamic information traffic in cyberspace. This phenomenon indicates the necessity for optimization through the recruitment of competent cyber professionals. Therefore, the implementation of an effective combination of human resources and technology is essential in the context of cyber counterintelligence, which serves as a response to the challenges and obstacles faced in the protection of intelligence assets.

The practical implications of this sub-chapter for the government and stakeholders in the fields of cyber and intelligence are the identification of various challenges and obstacles that constrain the Indonesian non-military Intelligence Community (IC) in its efforts to implement a cohesive national security strategy to detect cyber threats and then create solutions. To overcome the aforementioned challenges and obstacles, theoretical implications are recommended for society as well as input for academics and cyber and intelligence practitioners regarding the critical understanding of the situation of cyber incidents in Indonesia, which is increasingly frequent. This situation elevates Indonesia to a high risk of becoming a major target, urgently requiring the creation of numerous solutions to the obstacles and challenges to detecting cyber threats by the Indonesian non-military Intelligence Community (IC), as previously described by the researcher.

A critical analysis on the research results and discussion of new findings described above is inextricably linked to the limitations of aspects that have not yet been sufficiently studied. Therefore, the researcher recommends further research that focuses more on the independence of cyber technology for the Indonesian non-military Intelligence Community (IC). This focus is considered essential due to the highly complex tasks of the Indonesian Intelligence Community (IC), which require high-level security measures to acquire, process, and store intelligence information and data over the internet. Hence, the objective is to develop specific abilities in detecting cyber incidents pertaining to national security stability, as well as to anticipate prospective threats arising due to the advancement of cyber technology in the future.

5. Conclusion

Based on the gap analysis and problem formulation presented in the introduction, the researcher conducted a study with the objective of obtaining factual evidence, and subsequently conducted a thorough analysis of the data collected. This study resulted in the synthesis of findings in the form of a model for strengthening the organizational management of the optimal intelligence security function for the Indonesian non-military Intelligence Community (IC). The model aims to detect cyber threats and provide recommendations for the formulation of cyber defense policies in non-military intelligence, within the context of national security.

A synthesis of the findings can be derived from the responses to the research questions. These include: 1) potential and factual cyber threats, 2) strategies for strengthening the intelligence security function, and 3) challenges and obstacles faced in the process of detecting cyber threats by the Indonesian non-military Intelligence Community (IC).

1) The potential and factual cyber threats continue to evolve through state-sponsored and non-state actors. To adequately address these threats, it is essential to interpret them objectively and comprehensively. The technical and non-technical implications of factual and potential cyber threats are numerous and diverse. Technical implications include data theft and modification, as well as forced access that can damage the target's cybersecurity system. Non-technical implications are comprehensive and can affect state resilience, which is critical for achieving national security. As a result, the government must introduce a new legislative framework prescribing a set of harmonized cybersecurity requirements for non-military intelligence organizations.

2) As part of its strategic security measures, the Indonesian non-military Intelligence Community (IC) is implementing coordinated and organized management, the use of technology, and integrated harmonization, synchronization, and synergy processes. The coordination process among non-military Intelligence Community (IC) in Indonesia follows the authority of state institutions related to cybersecurity. This is because there is no focal point to organize cybersecurity in the country. The strategy is determined as a responsive action to reduce potential losses caused by cyber threats. Moreover, the implementation of cyber counterintelligence serves to enhance organizational capabilities in collecting, processing, and interpreting information as a preventive measure against potential cyber threats, with the ultimate objective of securing organizational assets, including personnel, materials, information, and intelligence operations. Regarding the utilization of technology in cyber counterintelligence operations, the Indonesian non-military Intelligence Community (IC) is

striving to develop technological capabilities that significantly impact the intelligence cycle process, despite the cyber technology employed being in its still-evolving infancy.

3) To strengthen organizational security in the context of cyber threats detection, Indonesian non-military Intelligence Community (IC) faces challenges and obstacles. Challenges include meeting the needs of non-military intelligence personnel with cyber expertise and reducing reliance on foreign-made cyber intelligence equipment, the latter of which is a critical issue as it is vulnerable to potential exploitation by foreign intelligence services. Meanwhile, the current obstacles are the prevalence of ego-sectoral attitudes in coordination mechanisms, along with overlapping responsibilities among non-military intelligence organizations. To resolve these issues, the Indonesian non-military Intelligence Community (IC) must reinforce the culture of intelligence security based on trust and mutual understanding, recognizing its pivotal role in the effective operation to the existence of intelligence services. Moreover, the Cybersecurity Law should be ratified and the State Intelligence Law should be amended to enhance cooperation among non-military intelligence stakeholders, meanwhile, the cyber talent should be optimized through cyber training schemes and advanced cyber technologies should be developed as an investment in technological independence.

The researcher acknowledges the limitations of this research due to the confidential nature of intelligence studies. To address these limitations, the researcher presents several recommendations for further research in both theoretical and practical domains. It will contribute to the advancement of scientific knowledge regarding intelligence.

1) For the purpose of further theoretical research recommendations, a more comprehensive study of the regulatory system governing the coordination of state intelligence agencies is necessary. The current regulatory framework does not prescribe the legal ramifications of non-compliance by non-military intelligence agencies in coordinating with BIN to address cyber threats. While the State Intelligence Law outlines potential administrative sanctions, it lacks specific provisions regarding the legal consequences of non-cooperation. The objective is to serve as a reference for determining the strategic policy of state intelligence and a guide for non-military intelligence agencies in organizing operational activities in cyberspace.

   Moreover, further theoretical research is necessary to pursue the concept of non-military intelligence fusion in the future. Theoretically, the fusion of non-military intelligence facilitates the alignment of non-military intelligence organizations to conduct counterintelligence operations in cyberspace in an integrated manner, thereby establishing a unified strategy for the non-military intelligence security function while minimizing the risk of inter-organizational conflict and overlapping responsibilities. The objective is to situate non-military cyber intelligence into a more strategic framework within Indonesian governance.

2) For practical research recommendations, the researcher emphasizes the importance of research in terms of increasing international cooperation by State Intelligence Agency of the Republic of Indonesia (BIN), State Cyber and Crypto Agency of the Republic of Indonesia (BSSN), and Ministry of Communications and Informatics of the Republic of Indonesia (Kominfo) along with other intelligence stakeholders to develop human resources who specialize in cyber technology. The objective is to enhance the capabilities and expertise of intelligence personnel, enabling them to effectively respond to cyber incidents and integrate them with other national resources to secure state assets.

   Concerning the governance of non-military cyber intelligence, the researcher deems it imperative to conduct further research on the juridical aspects, including research on the urgency of passing the Cybersecurity Law by the House of Representatives of the Republic of Indonesia. This law has the potential to assist Indonesia's non-military Intelligence Community (IC) in navigating the complexities of cyber threat detection and enhance the role of intelligence providers in this domain. Moreover, it would be advantageous to conduct further research assessing the need for revisions to the country's intelligence regulations considering the impact of cyber threats, which will implicate a more proactive role of the Indonesian non-military Intelligence Community (IC). The purpose of this initiative is to strengthen non-military intelligence governance policies to stabilize national security.

   Additionally, the researchers recommend further in-depth research into the strengthening of cyber infrastructure to reduce the Indonesian non-military Intelligence Community (IC)’s dependence on foreign technology in its main tasks and functions. This is because Indonesia's cyber infrastructure still lags behind the developed countries. The objective is to establish cyber technology independence to enhance the capabilities of the Indonesian non-military Intelligence Community (IC) and the capacity of the State Intelligence Agency of the Republic of Indonesia (BIN). This focus is critically important because the tasks of the Indonesian Intelligence Community (IC) are highly complex, and anticipating new threats arising from advances in cyber technology is essential. By optimally strengthening cyber infrastructure, it can help fulfill the need for non-military cyber intelligence talents who have specialized and qualified competencies in the context of cyber threat detection.

Acknowledgment

The author expresses his gratitude to Teuku Rezasyah Ph.D. from Padjadjaran University as a mentor and Dr. Susaningtyas Nefo Handayani Kertopati, M.Si. as a supervisor of postgraduate studies at the University of Defense, for their invaluable advice and motivation, which enabled the author to complete the writing of this article. Furthermore, the author would like to express his gratitude to Dr. Mario Arturo Ruiz Estrada from the University of Malaya and Anastasios-Nikolaos Kanellopoulos, MSc. from Athens University, who provided substantial contributions in the form of insightful ideas, grammatical corrections, and recommendations of pertinent literature. These inputs and suggestions have significantly enhanced the quality of the article by reinforcing the adherence to established writing conventions.

References

Allen, B. (2023). *Driving Rapid, Scalable, and Modular ISR & EW Solutions*. https://www.boozallen.com/insights/defense/driving-rapid-scalable-and-modular-isr-ew-solutions.html

Ateş, A., & Erkan, A. (2021). Governing the European Intelligence: Multilateral Intelligence Cooperation in the European Union. *International Journal of Politics and Security*, *3*(3), 230–250.

Ball, K. (2021). *Electronic monitoring and surveillance in the workplace*. European Commission Joint Research Centre.

Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24–31.

Bodström, T. T. (2022). Strategic cyber environment management with zero trust and cyber counterintelligence. *Journal of Information Warfare*, *21*(3), 1–12.

Borghard, E. D. (2022). *Protecting financial institutions against cyber threats: A national security issue*. JSTOR.

Brooker, P. (2013). *Non-democratic regimes*. Bloomsbury Publishing.

Bucur-Marcu, H., Fluri, P., & Tagarev, T. (2010). *Defence management: An introduction*. Geneva Centre for the Democratic Control of Armed Forces.

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Cavelty, M. D., Mauer, V., & Balzacq, T. (2010). *The Routledge handbook of security studies* (Issue s 56). Routledge London.

Chuter, D. (2011). *Governing & managing the defence sector*. Institute for Security Studies.

Clark, R. M., & Mitchell, W. L. (2018). *Deception: Counterdeception and counterintelligence*. CQ Press.

Cline, L. (2022). Sharing intelligence culture: Working with foreign intelligence services. *The Journal of Intelligence, Conflict, and Warfare*, *5*(1), 18–38.

Cragin, R. K. (2015). Semi-proxy wars and US counterterrorism strategy. *Studies in Conflict & Terrorism*, *38*(5), 311–327.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Cybersecurity and Infrastructure Security Agency. (2017). *). Awareness Briefing: Chinese Cyber Activity Targeting Managed Service Providers*. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/c3vp/Chinese-Cyber-Activity-Targeting-Managed-Service-Providers.pdf

Cybersecurity and Infrastructure Security Agency. (2020). *NIAC Insider Threat to Critical Infrastructures: Final Report and Recommendations*. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/niac-insider-threat-final-report-04-08-08-508.pdf

De Joode, A. (2011). Effective corporate security and cybercrime. *Network Security*, *2011*(9), 16–18.

Duvenage, P. C., Jaquire, V. J., & von Solms, S. H. (2018). Towards a literature review on cyber counterintelligence. *Journal of Information Warfare*, *17*(4), 11–25.

Duvenage, P., & Von Solms, S. (2014). Putting counterintelligence in cyber counterintelligence: back to the future. *13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus Piraeus, Greece*, 70.

Freeman, J., & Hannan, M. T. (1989). Setting the record straight on organizational ecology: Rebuttal to Young. In *American journal of sociology* (Vol. 95, Issue 2, pp. 425–439). University of Chicago Press.

Geers, K. (2009). The cyber threat to national critical infrastructures: Beyond theory. *Information Security Journal: A Global Perspective*, *18*(1), 1–7.

Gioe, D. V, Goodman, M. S., & Stevens, T. (2020). Intelligence in the cyber era: Evolution or revolution? *Political Science Quarterly*, *135*(2), 191–224.

Gullick, L., & Urwick, L. (1937). *Papers on the science of administration*. New York: Institute of Public Administration.

Hansel, M., & Silomon, J. (2024). Ransomware as a threat to peace and security: understanding and avoiding political worst-case scenarios. *Journal of Cyber Policy*, 1–20.

Hendropriyono, A. M. (2013). *Filsafat intelijen negara Republik Indonesia*. Penerbit Buku Kompas. https://books.google.co.id/books?id=bhC6nQEACAAJ

Hernandez Ramos, J., Karopoulos, G., Nai Fovino, I., Spigolon, R., Steri, G., Gorniak, S., Magnabosco, P., Atoui, R., Crippa Martinez, C., & Sportiello, L. (2024). *Cyber resilience act requirements standards mapping – Joint Research Centre & ENISA joint analysis*. Publications Office of the European Union. https://doi.org/doi/10.2760/905934

Id-SIRTII/CC. (2023). *Lanskap Keamanan Siber Indonesia 2023*. State Cyber and Crypto Agency of the Republic of Indonesia (BSSN). https://www.academia.edu/115974321/Lanskap_Keamanan_Siber_Indonesia_2023

Johnson, L. K. (1996). *Secret agencies: US intelligence in a hostile world*. Yale university press.

Johnson, L. K. (2024). Intelligence Collection Priorities in an Age of Renewed Superpower Conflict: Toward a More Expansive Perspective. *The Journal of Intelligence, Conflict, and Warfare*, *6*(3), 1–31.

Kanellopoulos, A.-N. (2022). The Importance of Counterintelligence Culture in State Security. *Global Security and Intelligence Note*, *1*(5).

Karmini, N. (2024a). *Indonesia says a cyber-attacks has compromised its data center but it won't pay the $8 million ransom*. The Washington Post. https://www.washingtonpost.com/business/2024/06/24/indonesia-national-data-cyber-attacks-ransomware/91efce20-3235-11ef-872a-1d22f44a0d95_story.html

Karmini, N. (2024b). *Indonesia won't pay an $8 million ransom after a cyber-attacks compromised its national data center*. The Associated Press. https://apnews.com/article/indonesia-ransomware-attack-national-data-center-213c14c6cc69d7b66815e58478f64cee

Kennedy, P. S. J., Tobing, S. J. L., & Lumbantoruan, R. (2017). Manajemen Anggaran Pertahanan Nasional. *Prosiding Seminar Nasional Ekonomi Dan Bisnis (SNEBIS)*, *1*(1), 1–9.

Klosterman, P. J. (2016). *Identification and establishment of social and sociomathematical norms associated with mathematically productive discourse*. Washington State University.

Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International.

Kuhn, T. S. (1982). Commensurability, comparability, communicability. *PSA: Proceedings of the Biennial Meeting of the Philosophy of Science Association*, *1982*(2), 668–688.

Kunarto, K. (1999). *Intelijen: Pengertian dan Pemahamannya*. Cipta Manunggal.

Lerner, K. L., & Lerner, B. W. (2004). *Encyclopedia of espionage, intelligence, and security. Vol. 3: RZ*. Thomson Gale.

Malone, T. W., & Crowston, K. (1994). The interdisciplinary study of coordination. *ACM Computing Surveys (CSUR)*, *26*(1), 87–119.

Mattern, T., Felker, J., Borum, R., & Bamford, G. (2014). Operational levels of cyber intelligence. *International Journal of Intelligence and CounterIntelligence*, *27*(4), 702–719.

Mattioli, R., Malatras, A., Hunter, E. N., Penso, M. G. B., Bertram, D., & Neubert, I. (2023). Identifying emerging cyber security threats and challenges for 2030. *European Union Agency for Cybersecurity (ENISA), Athens-Heraklion, Greece*, *64*.

Maurer, T., & Nelson, A. (2021). The global cyber threat. *Finance & Development*, 24–27.

Mavroeidis, V., Hohimer, R., Casey, T., & Jesang, A. (2021). Threat actor type inference and characterization within cyber threat intelligence. *2021 13th International Conference on Cyber Conflict (CyCon)*, 327–352.

Miles, M. B., Michael Huberman, A., & Saldaña, J. (2014). Qualitative data analysis. A methods sourcebook. In *Sage*

Publications (pp. 485–487).

Moleong, L. J. (2017). *Metodologi penelitian kualitatif (Cetakan ke)*. PT. Remaja Rosdakarya Offset.

Mondy, R. W. (1990). *Management and organizational behavior*. Allyn and Bacon.

Moran, C. R., Burton, J., & Christou, G. (2023). The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying. *Journal of Global Security Studies*, *8*(2), ogad005.

National Security Agency. (2023). *Network Infrastructure Security Guide. Cybersecurity Technical Report, 8-10*. https://media.defense.gov/2022/Jun/15/2003018261/1/1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF

Noor, R., Lestari, I., Sabana, D. R., Prihandoko, R., & Widjajanto, A. (2023). *Indonesia X Geo V*. Lembaga Ketahanan Nasional Republik Indonesia. https://www.lab45.id/detail/249/indonesia-x-geo-v

O'Connor, C. J. (2022). *Cyber Counterintelligence: Assets, Audiences, and the Rise of Disinformation*. The Australian National University.

Paleri, P. (2008). *National security: Imperatives and challenges*. Tata McGraw-Hill.

Provis, C. (2004). *Ethics and Organisational Politics*. Edward Elgar. https://books.google.co.id/books?id=yKIrAQAAMAAJ

Prunckun, H. (2014). *Scientific methods of inquiry for intelligence analysis*. Rowman & Littlefield.

Radin, B. A. (2000). *Beyond Machiavelli: Policy analysis comes of age*. Georgetown University Press.

Ramadhianto, R., Toruan, T. S. L., Kertopati, S. N. H., & Almubaroq, H. Z. (2023). Implementation of Artificial Intelligence on Indonesia's Defense Intelligence Activities. *Jurnal Pertahanan: Media Informasi Tentang Kajian Dan Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism Dan Integrity*, *9*(2), 350–365.

Saronto, Y. W. (2001). *Intelijen: teori, aplikasi dan modernisasi*. Ekalaya Saputra.

Saronto, Y. W. (2018). *Intelijen: teori intelijen dan pembangunan jaringan*. Penerbit Andi. https://books.google.co.id/books?id=iVNCwwEACAAJ

Schermerhorn, J. R., Hunt, & Osborn, R. N. (2005). *Organizational Behavior*. Wiley. https://books.google.co.id/books?id=LcCljskx08QC

Silalahi, A. (2005). *Strategi Pelatihan dan Pengembangan Sumber Daya Manusia*. Surabaya: Batavia Press.

Sugiyono, S. (2018). Metode Penelitian Kualitatif untuk Penelitian yang Bersifat: Eksploratif, Enterpretif, Interaktif dan Konstruktif. *Bandung: CV. Alfabeta*.

Supriyatno, M. (2014). *Tentang Ilmu Pertahanan*. Yayasan Pustaka Obor Indonesia. https://books.google.co.id/books?id=CaxxDAAAQBAJ

Tagarev, T., Fluri, P., Nelson, D., Greenwood, D., Ivanov, T., Bahja, Z., Totev, D., Radicevic, T., Cvrtila, V., Gjoreski, V., Sava, C., Repciuc, T., Popescu, R., Arnejcic, B., & Shalamanov, V. (2002). *Transparency of Defence Policy, Military Budgeting and Procurement*. Geneva Centre for the Democratic Control of Armed Forces.

Trim, P. R. J., & Lee, Y.-I. (2021). The global cyber security model: counteracting cyber attacks through a resilient partnership arrangement. *Big Data and Cognitive Computing*, *5*(3), 32.

Vigoda-Gadot, E., & Cohen, A. (2004). *Citizenship and management in public administration: Integrating behavioral theories and managerial thinking*. Edward Elgar Publishing.

Viinamäki, O.-P. (2004). *A theory of coordination and its implications on EU structural policy: a comparative study of the challenges for coordination in structurel funds in Finland, Ireland, and Sweden*. Vaasan yliopisto.

Wæver, O. (2008). The changing agenda of societal security. In *Globalization and Environmental Challenges: Reconceptualizing Security in the 21st Century* (pp. 581–593). Springer.

Waever, O., & Flockhart, T. (2014). Cooperative Security: A New Concept? *DIIS Report*, *1*, 47–59.

Waldo, D. (2017). *The Administrative State: A Study of the Political Theory of American Public Administration*. Taylor & Francis. https://books.google.co.id/books?id=-NszDwAAQBAJ

Warner, M. (2019). Wanted: A definition of 'intelligence.' In *Secret Intelligence* (pp. 4–12). Routledge.

Wijayanto, D. (2013). *Pengantar manajemen*. Gramedia Pustaka Utama.

World Economic Forum. (2024). *Global Cybersecurity Outlook. The World Economic Forum*. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf