Jurnal Perencanaan Pembangunan:
The Indonesian Journal of Development Planning
Volume VIII No. 2 - August 2024/Page: 150 - 180
https://doi.org/10.36574/jpp.v8i2.566
Article

# The Urgency of Stakeholder Cyberspace Collaboration to Support Indonesia's National Defense

Firdini[1], Rudy Agus Gemilang Gultom[2], Pujo Widodo[3], and Jupriyanto[4]

Corresponding author. Email: firdini@bappenas.go.id

Submitted: 2024-05-31 | Accepted: 2024-08-30| Published: 31th August 2024

*Abstract*

In today's interconnected digital world, stakeholder collaboration in cyberspace is crucial for national defense. Advances in information and communication technology have transformed daily life but also introduced complex cyber threats like cyber warfare, cybercrimes, and cyber terrorism, challenging security and stability. The objective of this study is to emphasize the importance of collaboration among diverse stakeholders in enhancing national defense against cyber threats. The methodology involves analyzing existing literature and case studies to understand the impact of collaboration on cybersecurity maturity and national defense strategies. The research findings, derived from SWOT and PESTLE analyses, have highlighted the strengths and weaknesses in collaboration, underscoring the significance of leveraging strengths and addressing weaknesses to establish a robust defense framework. To enhance national defense against cyber threats, a holistic approach is essential, combining political collaboration, economic partnerships, social awareness programs, technological advancements, legal harmonization, and environmental resilience strategies. Key recommendations include fostering regular communication among stakeholders, pooling resources for cybersecurity investments, promoting cybersecurity education, integrating advanced technologies like AI and IoT security solutions, and aligning legal frameworks across jurisdictions.

**Keywords:** cyberspace; cyber-attacks; cyber security; stakeholder collaboration; national defense.

[1234] Republic of Indonesia Defense University, Jakarta, Indonesia.

## I. Introduction

Information and communication technology has revolutionized the way we live, ushering us into an era of interconnectedness that is globally reliant. The advancement in technology serves as a primary bridge between the physical and digital world, yet it also brings about increasingly complex threats, such as cyber warfare. The interconnectivity of devices, systems, and networks, coupled with the rapid growth of the digital economy, exacerbates this situation. While digital infrastructure has brought various conveniences to daily life (Kaur, 2023), this interconnectedness also brings significant vulnerabilities, such as cyberattacks, cybercrimes, and even cyber terrorism (Tagarev, 2020). In this context, we observe that technological progress not only brings benefits but also complex and significant cyber threats that impact security and stability in the globally connected information age. Dependence on technology across various sectors underscores the importance of a holistic approach in strengthening defense and security frameworks (Brenner, 2013).

Over the past few decades, the military landscape has undergone fundamental changes due to the emergence of cyber threats, exacerbated by increasing reliance on internet technology that heightens network vulnerabilities and the potential for attacks targeting critical infrastructure. The US National Security Strategy recognizes cyber threats as a significant risk to national security and emphasizes the need for strong cybersecurity measures and collaboration between government and private sectors to effectively address cyber threats (Tatal et al., 2014). The military faces various cyber threats, including state-sponsored attacks from countries like Russia, China, Iran, and North Korea, aimed at stealing sensitive data or disrupting critical infrastructure (Garamone, 2018). They also confront cybercrimes for financial gain or operational disruption (Wilson, 2019), insider threats with access to sensitive information (Lyons, 2023), supply chain attacks, and advanced persistent threats (APTs) infiltrating to steal data or disrupt operations (Wilson, 2019). Cyberattacks are also utilized for espionage, subversion, and sabotage that pose threats to military systems and infrastructure such as power grids or water facilities (Wallace, 2013).

Three significant incidents triggered the development of national cybersecurity strategies (Tatal et al., 2014). First, the cyberattack on Estonia's internet infrastructure in 2007 changed perceptions about the impact of cyberattacks. Second, the cyberwar during the conflict between Georgia and Russia in 2008 demonstrated the use of cyberspace as a force multiplier in real conflicts. Third, the Stuxnet cyber incident on Iran's nuclear infrastructure in 2010, also impacted Indonesia, where around 60% of infected hosts were in Iran and Indonesia ranked second as shown in Figure 1.

The development of global cyberspace requires rapid and adaptive responses due to the increasing cyber threats, the recognition of cyberspace as a domain of warfare, dependence on digital infrastructure, and opportunities in the digital economy. The Stuxnet incident has spurred many countries to become active attackers in cyberspace, along with hackers and non-state groups. The response of various countries to these developments is marked by an increase in national cybersecurity strategies, especially after three significant cyber incidents. Figure 2 shows the significant growth of national cybersecurity strategies published between 2008 and 2010 (Tatal et al., 2014).

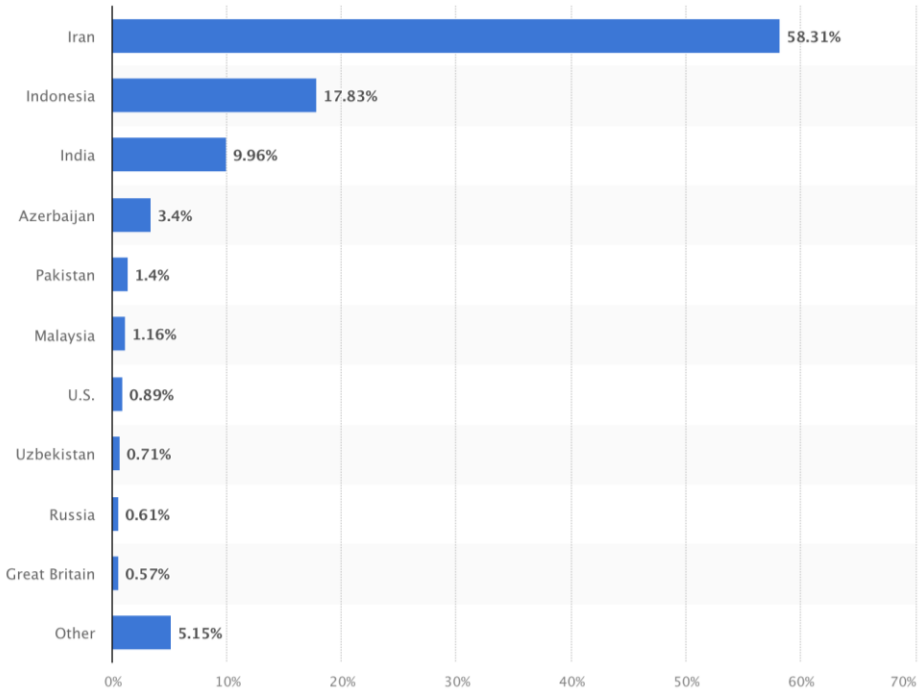


**Figure 1.** Geographic Distribution of Stuxnet 2010 Attacks

**Source:** Statista, 2010

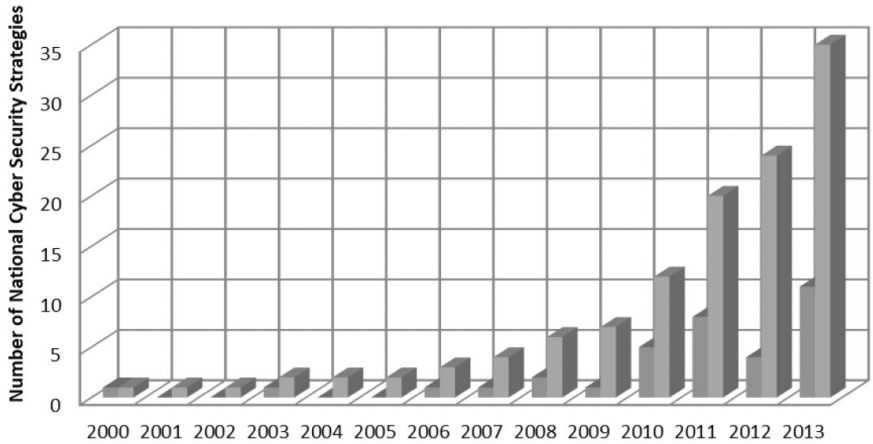


**Figure 2.** Number of National Cybersecurity Strategies 2000 – 2013

**Source:** Tatal., et.al, 2014

At the global level, almost all countries represented by members of the International Telecommunication Union (ITU) have now established national cybersecurity strategies in response to the increasing cyber threats and advancements in information technology, as seen in Figure 2 showcasing the widespread recognition among nations regarding the critical need to fortify their

cybersecurity measures. The establishment of these strategies reflects a collective effort to address the evolving challenges posed by cyber threats, underscoring the importance of proactive and comprehensive approaches in safeguarding digital infrastructure and national security.

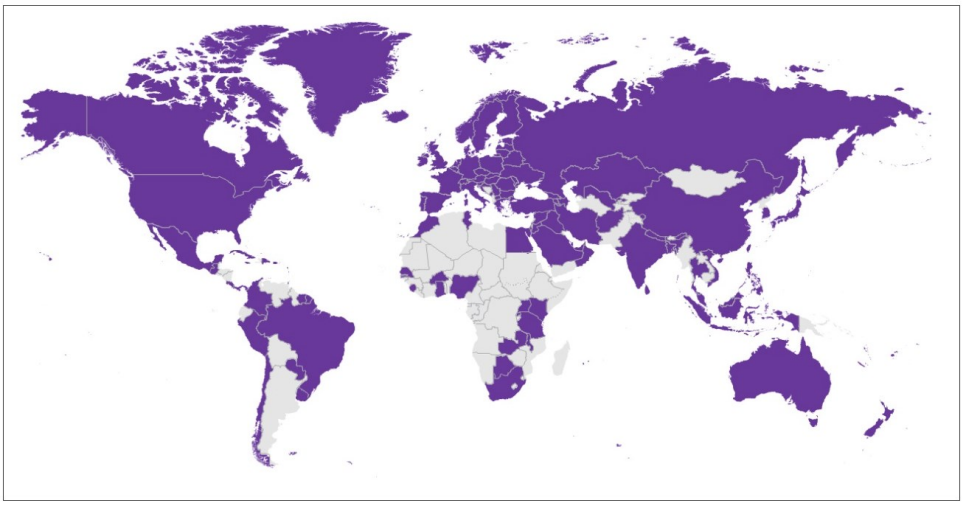

**Figure 3.** ITU Member States with National Cybersecurity Strategies

**Source:** International Telecommunication Union, 2024.

Collaboration across sectors and coordination among various stakeholders are crucial in developing comprehensive and responsive defense strategies against evolving threats. Cybersecurity should be a top priority for central government, providers of national critical infrastructure, local governments, and private organizations, directing efforts toward enhancing the cybersecurity capacity of diverse stakeholders (Preis & Susskind, 2022). The interconnected nature of digital infrastructure means that one breach can have cascading impacts, affecting national security on a wide scale. Therefore, coordinated efforts between government agencies, private sectors, and international partners are essential to enhance resilience and cybersecurity response capabilities. These efforts include the critical and challenging tasks of formulating effective policies to protect cyberspace and addressing cybersecurity incidents (de Bruijn & Janssen, 2017). Failure to foster such collaboration can lead to significant risks, including inadequate protection of critical infrastructure, fragmented security efforts, and slower response times to emerging threats. Lack of coordination can create significant gaps in national defense, making it easier for adversaries to exploit vulnerabilities. Hence, it is crucial to develop a comprehensive and cohesive strategy involving all relevant stakeholders in cyberspace.

The objective of this research is to explore the urgency of collaboration among cyberspace stakeholders to support national defense, serving as the foundation for formulating a robust and comprehensive national cyber strategy. Given the significant impact of information and communication technology advancements on various aspects of life, particularly the increasing complexity and significance of cyber threats, this research aims to emphasize the importance of a collaborative approach. The questions in this research are "Why is collaboration among cyberspace stakeholders important for national defense?" and "How can SWOT and PESTLE analyses be used to strengthen this collaboration?". Understanding the urgency of collaboration is crucial given the high interconnectedness in

digital infrastructure and the potential vulnerabilities it entails. In this context, the use of SWOT and PESTLE analyses is appropriate for this research. SWOT analysis helps identify strengths, weaknesses, opportunities, and threats in collaboration among cybersecurity stakeholders, while PESTLE analysis provides a broader perspective by evaluating political, economic, social, technological, environmental, and legal factors influencing cybersecurity stakeholder collaboration. This approach enables the research to provide comprehensive and strategic recommendations for strengthening collaboration in addressing cyber threats.

## II. Research Methods

This study intends to provide a thorough knowledge of the relevance of collaboration among cyberspace stakeholders in supporting national defense, as well as an empirical foundation for future policy formulation. This paper applies a qualitative methodology, primarily derived from a literature study approach. Researching an object's natural state is an effective application for qualitative research methods (Sugiyono, 2005). To get a more comprehensive explanation, qualitative approaches enhance knowledge of an event's basic form (Sofaer, 1999). Researching pertinent sources and using theme analysis to structure the data are important in the research process. The study was conducted through the examination of prior study materials obtained from journals, publications, and reports related to cyberspace, cyber defense, cybersecurity, cooperation, and national security. Analyzing the literature is considered to be vital to assessing important ideas. Qualitative approaches enable greater flexibility in comprehending complex ideas in cyberspace.

SWOT and PESTLE analyses are complementary frameworks that provide a comprehensive understanding of the urgency for collaboration among cyberspace stakeholders to support national defense. While SWOT analysis identifies strengths, weaknesses, opportunities, and threats related to cybersecurity practices and collaboration, PESTLE analysis elaborates on the political, economic, social, technological, legal, and environmental factors influencing these efforts. By combining these frameworks, researchers can achieve both internally and externally impactful analysis (Srdjevic, et al., 2012), offering a structured approach to evaluate the cybersecurity landscape and collaboration dynamics. In this research, SWOT analysis is used to categorize factors that play a crucial role in collaboration among cyberspace stakeholders into internal or external groups according to their domain. Subsequently, these factors are analyzed and grouped into categories of Political, Economic, Social, Technological, Legal, and Environmental, as depicted in Figure 4. This integrated method helps identify critical areas for improvement, uncover potential synergies, and anticipate external challenges, thereby supporting the formulation of effective policies and the development of a robust cybersecurity strategy aligned with national security objectives.

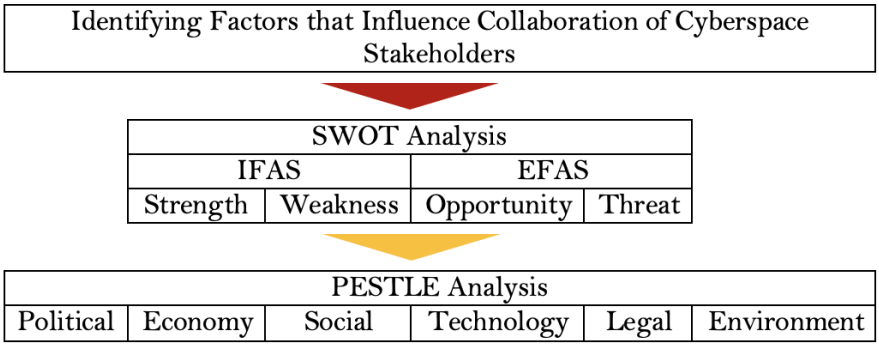


**Figure 4.** Research Methods

**Source:** Authors Formulation

## III. Result and Discussion

In this research, SWOT analysis is used to identify the key factors of strengths, weaknesses, opportunities, and threats that play a crucial role in collaboration, which are then elaborated from the perspectives of Politics, Economics, Social, Technology, Legal, and Environment. The results of the SWOT-PESTLE analysis from this research are presented in Table 1. Through this approach, the research aims to provide a deep understanding of the dynamics of collaboration in cyberspace and support the development of a comprehensive and adaptive cybersecurity strategy.

**Table 1.** The Result of the SWOT-PESTLE Analysis

| ASPECT | Internal Factors Analysis Summary (IFAS) | | External Factors Analysis Summary (EFAS) | |
|---|---|---|---|---|
| | STRENGTH | WEAKNESS | OPPORTUNITY | THREAT |
| | 1 | 2 | 3 | 4 |
| POLITICAL | Involvement of Various Stakeholders<br><br>Security Cooperation<br><br>Joint Strategy Development | Misalignment of Interests<br><br>Lack of Coordination | Building Strong Relations in the Ecosystem<br><br>International Cooperation | Complex and Evolving Cyber Threats<br><br>Security Gaps |
| ECONOMY | Sharing the Burden of Security Investment | Budget Limitations | Joint Investment in Cybersecurity | N/A |

| | | | | |
|---|---|---|---|---|
| **SOCIAL** | Increasing Cybersecurity Awareness | Quantity and Quality of Human Resources Limitation<br><br>Lack of Trust and Cooperation<br><br>Low Digital Literacy | Increasing Public Trust | N/A |
| **TECHNOLOGY** | Enhancing Cyber Operations Capabilities | Complexity in Managing Multiple Security Solutions<br><br>Inadequate Security Controls<br><br>Limited Human Resources and Expertise in Technology Development and Utilization | Technological Development and Innovation | Evolving Cyber Attack Technologies<br><br>Unreliable Technology<br><br>Cyber Espionage |
| **LEGAL** | Framework Standardization<br><br>Compliance Incentives<br><br>Legal Protection<br><br>Ensuring Resource Allocation | Limited Number of Regulations<br><br>Slow Regulatory Development<br><br>Low Compliance with Regulations | N/A | Regulatory Differences at Regional and Global Levels |
| **ENVIRONMENT** | N/A | N/A | N/A | Natural Disasters<br><br>Attacks on Physical Infrastructure |

**Source:** Authors Analysis

## 3.1. Strengths

The strength of collaboration among cyberspace stakeholders in supporting national defense is influenced by political, economic, social, technological, and legal factors. Understanding the strengths of collaboration will be beneficial in identifying resources and capabilities that can be optimized to enhance the effectiveness of national defense.

### 3.1.1. Political

#### 3.1.1.1. Involvement of Various Stakeholders

The involvement of various stakeholders in cyberspace is a significant strength in supporting national defense, as complex cybersecurity requires contributions from multiple parties with diverse expertise and resources. Tagarev and Sharkov (2016) emphasize that collaboration among parties is an essential part of achieving cybersecurity maturity, as demonstrated in Bulgaria's experience. Rondelez (2018) adds that the effectiveness of cybersecurity coordination also depends on good internal design and governance, as seen in Belgium. According to Spinu (2020), the private sector and academia also play a crucial role in national defense by contributing material, technical, and deep knowledge. However, Lebo and Anwar (2020) reveal that the cyber community is not fully empowered to support the government in cybersecurity. This finding aligns with Lewis (2010), who emphasizes the government's role as a policy maker in formulating, regulating, and implementing cyberspace governance, supported by other actors including the cyber community. Cross-sector cooperation and stakeholder collaboration are key in cybersecurity strategies, highlighting the importance of active support from government, institutions, and the private sector related to ICT (Maurer, Levite, & Perkovich, 2017, Lebo & Anwar, 2020). This cross-stakeholder collaboration is essential to building strong and adaptive national defense in the digital era.

#### 3.1.1.2. Security Cooperation

Cooperation is a strong foundation for collaboration among cybersecurity stakeholders in supporting national defense. Maurer, Levite, and Perkovich (2017) highlight the importance of collaboration through formal structures such as Information Sharing and Analysis Centers (ISAC) and Public Private Partnerships (PPP) to enhance detection, rapid response, and mitigation of complex cyber threats. Joint exercises such as Cyber Storm organized by the Cybersecurity and Infrastructure Security Agency (2024) aim to test responses to major cyber incidents, while open-source security projects like OWASP and information-sharing communities like the Cyber Threat Alliance and FS-ISAC enhance the resilience of critical infrastructure. Babys (2021) emphasizes that this collaboration is crucial to addressing cybercrime and conflicts and strengthening national defense in the digital era.

#### 3.1.1.3. Joint Strategy Development

Considering the complexity of cybersecurity issues, the best approach is to involve a combination of various policy instruments. Successful security collaboration enables the development of joint strategies, sharing insights on new trends, and joint research, with governments playing a central role in regulation and coordination (Bauer & Van Eeten, 2009). An example of security collaboration is Moldova's national cybersecurity strategy involving training, collaboration, and the establishment of a national CERT (Spinu, 2020), while in Indonesia, collaboration involves various institutions such as the Ministry of Foreign Affairs, National Cyber and Crypto Agency, and the Indonesian National Army (Saudi, 2018). Synergy among stakeholders, as emphasized by Rizki and Timur (2021), as well as global public-private collaboration, is crucial for a comprehensive strategy that protects national infrastructure and individuals, ensuring the stability of developing countries (Kayode-Ajala, 2023). Through collaboration, the development of more comprehensive and innovative joint strategies becomes possible.

### 3.1.2. Economy

#### 3.1.2.1. Sharing the burden of security investment

Collaboration among cyberspace stakeholders has significant strength, especially in sharing the burden of security investment, which can reduce overall costs (Zheng & Lewis, 2015). Sharing information enhances awareness and knowledge of cybersecurity incidents, enabling predictions of attacker behavior and the development of effective preventive measures. This is highly beneficial for organizations with high-risk profiles. The cost of crisis prevention through information sharing is lower than the cost of responding to and recovering from crises, providing a positive economic impact (Gal-Or and Ghose, 2004; Gordon et al., 2015). Thus, this collaboration provides significant economic benefits to stakeholders in supporting national defense in cyberspace.

### 3.1.3. Social

#### 3.1.3.1. Increasing cybersecurity awareness

Cybersecurity awareness is a crucial foundation in combating cybercrime, although it does not guarantee absolute security. Awareness and education of cyber users are key steps in reducing the risk of attacks and strengthening participation in security programs supported by stakeholder collaboration (Aidoo, 2017). Awareness of vulnerabilities in various sectors can strengthen collaboration in addressing increasingly complex cyber threats, with active commitment from individuals to protect themselves online (Bruijn & Janssen, 2017). Governments and law enforcement recognize the importance of cybersecurity awareness at all levels to protect assets and vital infrastructure (Akter et al., 2022). Australia's government investment in cybersecurity defense and encouragement for self-awareness among its citizens demonstrate the importance of these actions, yet their effectiveness depends on businesses educating their employees (Proofpoint, 2021). The increasing cyber-attacks, government commitment, and business needs to address security issues have driven increased awareness and made cybersecurity threats a serious agenda for researchers and practitioners (Karjalainen et al., 2020). With high awareness, cybersecurity priorities can be enhanced, facilitating policies that support collaboration in addressing cyber threats.

### 3.1.4. Technology

#### 3.1.4.1. Enhancing cyber operations capabilities

The development of cyber technology has been a significant force for collaboration among cyberspace stakeholders in supporting national defense. In the military domain, the use of AI in cybersecurity has great potential (Ertan et al., 2020). The integration of advanced technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), Neural Networks, Cyber-Physical Systems (CPS), Brain-Computer Interfaces (BCI), and Virtual Reality (VR) and Augmented Reality (AR) has revolutionized the cyber warfare field, enhancing connectivity, decision-making, and operational efficiency. IoT strengthens data exchange between weapon systems, AI and Neural Networks develop autonomous battle systems, and CPS enables precise control of physical devices. BCI facilitates communication between controllers and battle systems, while VR and AR create simulations to confuse enemies (Kim, Sin-Kon, et al., 2019). These technologies enable rapid threat identification and response by utilizing artificial intelligence (AI), machine learning (ML), blockchain technology, and biometric authentication (Intone Network, 2023). AI enhances network

resilience and reliability (Taddeo et al., 2019), increases autonomy and adaptability of cyber capabilities (Sanchez, 2017), and reduces risks for human soldiers and capital expenditure (Trusilo and Burri, 2021). This integration transforms military operations by improving efficiency, decision-making, and connectivity in cyber warfare (Kim, Sin-Kon, et al., 2019).

### 3.1.5. Legal

#### 3.1.5.1. Framework Standardization

Standardization of frameworks in a legal context is one of the strengths of collaboration among cybersecurity stakeholders in supporting national defense. This occurs because regulations provide a standard framework for conducting cybersecurity practices, ensuring that all stakeholders comply with established protocols and guidelines. Standardization creates consistency and clarity in collaborative efforts. For example, regulatory standards such as the General Data Protection Regulation (GDPR) in the European Union or the Cybersecurity Framework by the National Institute of Standards and Technology (NIST) in the United States establish guidelines and best practices for cybersecurity. These standards help stakeholders align their cybersecurity strategies and collaborate more effectively.

#### 3.1.5.2. Compliance Incentives

Regulations often present various incentives or requirements that encourage stakeholders to invest resources in cybersecurity measures and work effectively to meet established standards. The impact is increased readiness levels and higher coordination among collaborative actors. Many regulations provide incentives such as awards for compliance or sanctions for violations. For instance, financial institutions complying with regulations like the Payment Card Industry Data Security Standard (PCI DSS) will receive certification, demonstrating their commitment to cybersecurity, which in turn strengthens trust and cooperation with their partners. Thus, compliance incentives become a significant driver for enhancing collaboration in supporting national cyber defense.

#### 3.1.5.3. Legal Protection

Legal protection is one of the strengths of collaboration among cybersecurity stakeholders in supporting national defense. Regulations can offer legal protection to stakeholders involved in collaborative cybersecurity efforts. A clear legal framework can determine responsibilities, obligations, and dispute resolution mechanisms, reducing uncertainty and increasing trust among collaborators. Regulatory frameworks such as China's Cybersecurity Law or India's Cybersecurity and Data Protection Laws outline legal protections for stakeholders engaged in collaborative cybersecurity efforts. These laws establish data protection responsibilities, rights, and dispute resolution mechanisms, providing a secure legal ecosystem for collaboration (Wang et. al., 2022; Chaudhary et. al., 2022).

#### 3.1.5.4. Ensuring Resource Allocation

Ensuring resource allocation is one of the strengths of collaboration among cyberspace stakeholders in supporting national defense. Regulations can ensure the availability of adequate resources or budgets for cybersecurity initiatives, allowing stakeholders to invest in the technology, training, and infrastructure needed for effective collaboration in defending national cyber assets. If policy interventions have been established in regulations, it becomes an obligation to implement what has been mandated

in the regulations, including providing sufficient resources as a condition for carrying out activities. Governments often allocate funds or resources to support cybersecurity initiatives mandated by regulations. For example, in Indonesia, the National Medium-Term Development Plan 2020-2024 designates cybersecurity as a major project, enabling more focused and guaranteed resource allocation. This includes forming cyber incident response teams at the central and regional government levels, enhancing human resources in cybersecurity, regional and international cooperation, and strengthening cybersecurity infrastructure. With the establishment of the National Medium-Term Development Plan 2020-2024 under Presidential Regulation No. 18 of 2020, resource allocation, including budget allocation for activity implementation, has been ensured.

## 3.2. WEAKNESSES

Weaknesses in the collaboration among cyberspace stakeholders in supporting national defense are influenced by political, economic, social, technological, and legal factors. Understanding weaknesses in collaboration would be beneficial in identifying areas that require improvement, thus enabling the development of strategies to address existing barriers and vulnerabilities.

### 3.2.1. Political

#### 3.2.1.1. Misalignment of Interests

Misalignment of interests is one of the weaknesses in collaboration among cyberspace stakeholders that hinders efficiency and coordination. This misalignment arises because each entity or stakeholder has different priorities, goals, and interests in cyberspace. It is vulnerable to occur when the government emphasizes strict regulations for cybersecurity while the private industry focuses more on technological innovation, resulting in friction that hampers effective cooperation. Emphasizing collaboration between the government and the private sector through public-private partnerships (PPPs) to enhance the detection, prevention, and mitigation of cyberattacks through information exchange and contributions from both sides has become a priority reflected in various government policies (O'Halloran, 2017). However, these differing interests often result in resource wastage and impede quick responses to cyber threats, as well as slow down the development of holistic security solutions. Therefore, it is important to find common ground that integrates the interests of all parties to ensure effective and sustainable collaboration in cyberspace.

Moreover, misalignment of interests also occurs in an international context. For example, the United States (US) and the European Union (EU), while aligned in the general direction, do have different values. US cybersecurity policy is heavily influenced by the 9/11 terror attacks, emphasizing information access for national security, whereas the German constitution, as part of the EU, guarantees privacy to avoid surveillance of its citizens. These differences lead to tensions or conflicts in collaborative efforts, especially regarding sharing sensitive information or formulating joint policies to address cyber threats. These differences in values or priorities also hinder the level of trust between these countries, which is an essential element in effective collaboration. This creates a paradox where collaboration is needed to address cybersecurity threats but the involved parties mistrust each other because their activities and intentions may only partially be visible or disagree on shared values (Bruijn and Janssen, 2017). These differences can be a weakness in collaboration due to misunderstandings or discrepancies between these countries regarding values, priorities, or security-related policies.

#### 3.2.1.2. Lack of Coordination

Lack of coordination is one of the main weaknesses in collaboration among stakeholders in cyberspace. Without good coordination, various entities and stakeholders tend to work separately, resulting in disjointed actions and often overlap. Complex cybersecurity issues require close cooperation between the government and the private sector, as well as effective coordination among stakeholders. A concrete example comes from Indonesia, where a lack of clear distribution regarding roles and responsibilities related to cybersecurity has led to conflicts and shifting of responsibilities between agencies and ministries, as shown in handling data breach incidents by Bjorka across various institutions (CNBC Indonesia, 2022; Warta Ekonomi, 2022). This results in duplicated efforts, resource wastage, and lack of efficiency in addressing cyber threats. Furthermore, a lack of coordination can also slow down responses to attacks that require rapid and integrated actions. Therefore, it is important to improve coordination among stakeholders by building effective communication mechanisms, promoting open information sharing, and facilitating closer cooperation in maintaining cybersecurity. In situations like this, better coordination and clear responsibility distribution are needed to enhance collaboration effectiveness and response to cybersecurity challenges.

### 3.2.2. Economy

#### 3.2.2.1. Budget Limitations

Budget limitations are one of the weaknesses in collaboration among stakeholders in cyberspace in supporting national defense. The increasing cyber incidents experienced by the government and private sectors raise crucial questions about how much investment should be allocated to cybersecurity, and which types of investments will yield optimal social results (Paul and Wang, 2019). Budget limitations also have consequences in determining investment allocations in cybersecurity. Prevention methods become the main focus as a response to cyber threats (Forbes, 2013; Schilling, 2017). However, prevention alone is not sufficient to address increasingly complex and lethal cyber threats. While effective prevention can block threats, it may not necessarily detect and handle threats that successfully breach defenses. Budget limitations force organizations to choose which strategies will have the best impact in dealing with cyber threats.

The budget limitations make organizations have to choose the approach that will be the intervention in dealing with cyber threats. This is evident from the formation of the Belgian Network & Information Security (BelNIS) as an alternative due to budget limitations, which shows that limited solutions cannot effectively address vulnerabilities. Although the Belgian Cyber Security Center (CCB) was established a few years later, the awareness of the need for a more coordinated and integrated approach became clear (Rondelez, 2018). In Indonesia, budget limitations also pose a major obstacle to supporting collaboration among stakeholders in the cyber realm for national defense. This is evident from efforts to establish cyber incident response teams (CSIRT) as a crucial part of national cybersecurity efforts mandated by Presidential Regulation No. 18/2020 on the National Medium-Term Development Plan (RPJMN) 2020-2024 (Prabaswari et al., 2022). However, reallocation and refocusing of budgets due to the COVID-19 pandemic hinder the optimization efforts of government CSIRT formation. In this context, budget limitations become a hindrance for the government in addressing cyber threats comprehensively and emphasize the urgency of collaboration among stakeholders in supporting national defense.

### 3.2.3. Social

#### 3.2.3.1. Quantity and Quality of Human Resources Limitation

The limitation in quantity and quality of human resources in cybersecurity is one of the weaknesses in the collaboration of stakeholders in cyberspace in supporting national defense. Despite significant growth in the global cybersecurity workforce, there is still a significant gap between demand and supply of human resources. ISC2 data (2023) indicates a need for up to 4 million professionals to protect digital assets, yet the availability of the workforce falls far below that number. The Global Cybersecurity Skills Gap 2023 report also reveals the challenges many companies face in dealing with cyberattacks, with increasing breach incidents and difficulties in recruiting quality workforce. New challenges such as economic uncertainty, artificial intelligence, fragmented regulations, and skill gaps further complicate the situation, reflecting the security risks companies face due to the lack of quality human resources in cybersecurity (Fortinet, 2023; ISC2, 2023). The limitation in quantity and quality of human resources in cybersecurity becomes a weak point that needs to be addressed to strengthen the collaboration of stakeholders in supporting national defense in cyberspace.

#### 3.2.3.2. Lack of Trust and Cooperation

Lack of trust and cooperation among stakeholders in cyberspace can be a weakness in supporting national defense. Research by Hubner et al (2021) highlights various challenges, including building trust, privacy management, secure authentication, and threat identification. Data leakage incidents often associated with blame-shifting among institutions in Indonesia reflect a lack of comprehensive coordination and cooperation in handling cybersecurity (CNBC Indonesia, 2022; Warta Ekonomi, 2022). Building trust and cooperation is also crucial in collaboration between the government and the private sector. As mentioned by Givens (2013), public-private partnerships (PPPs) have value in reducing duplicate efforts, improving cross-sector communication, and enhancing efficiency in achieving protection goals. However, when these goals are not met, trust in partnerships can erode, contributions become less, and there is a possibility of blaming each other for perceived incapability. As a result, negative attitudes towards these partnerships, coupled with high levels of vulnerability and exploitation by malicious CNOs, indicate that many PPP goals are not fully met and their implementation requires deeper evaluation (O' Halloran, 2017).

#### 3.2.3.3. Low Digital Literacy

Low digital literacy is a weakness in the collaboration of stakeholders in cyberspace to support national defense. Skills and awareness of cybersecurity are crucial in the digital era (van Laar, van Deursen, van Dijk, & de Haan, 2017). Although many efforts have been made to strengthen technology infrastructure security, the focus on humans remains crucial in the context of cybersecurity (Zimmermann and Renaud, 2019). Digital literacy plays a key role in helping individuals understand and effectively address cybersecurity risks, given the risks of data leaks, cyberattacks, and financial losses that may occur due to low literacy.

In Indonesia, digital literacy remains a significant challenge. Indonesia's digital literacy index saw a slight increase to 3.49 in 2021 from 3.46 in 2020, but it still falls into the "moderate" category (Harsono, 2022). Additionally, public awareness of cybersecurity in Indonesia needs to be improved, especially with the continuous growth of internet users, yet

it is not matched with an adequate understanding of cyber risks and threats. Indonesia's cybersecurity awareness ranks 70th globally in the Security Index. Indonesian citizens still struggle to protect their data, especially in terms of regularly changing passwords, as is often done with ATM PINs and email passwords (Ayuwuragil, 2017). This indicates that low digital literacy is a serious obstacle to the collaboration of stakeholders in cyberspace in supporting national defense.

### 3.2.4. Technology

#### 3.2.4.1. Complexity in Managing Multiple Security Solutions

The complexity of managing multiple security solutions can be a weakness in the collaboration of stakeholders in cyberspace to support national defense. Organizations face challenges in managing multiple security solutions from different vendors, with differences in platforms, interfaces, and security policies that are difficult to integrate. Interoperability issues arise from incompatible security solutions, hindering integration and effective information sharing among stakeholders, thus increasing costs for personnel, training, and maintenance. Moreover, managing multiple solutions reduces efficiency as stakeholders have to switch between different systems, causing delays in responding to threats and increasing the risk of security breaches. Incident response becomes difficult, threat intelligence sharing is hindered, and regulatory compliance becomes complex. Managing and maintaining diverse security solutions can also increase operational costs and require significant resources (Acronis, 2021). The difficulty in effectively integrating these solutions can hinder collaborative efforts, reduce responsiveness to cyber threats, and create security gaps that attackers can exploit. Harmonization, standardization, and improving interoperability between security systems are key to addressing these weaknesses in the context of collaboration among stakeholders in cyberspace.

#### 3.2.4.2. Inadequate Security Controls

Inadequate security controls and unsupportive technology can be weaknesses in the collaboration among stakeholders in cyberspace to support national defense. This is because inadequate security controls can lead to vulnerabilities in systems and networks, making them susceptible to attacks and breaches. Inadequate security controls may include weak multi-factor authentication methods, inadequate access controls on networks and services, poor patch management, and misuse of system access controls (Cybersecurity and Infrastructure Security Agency, 2023). In the context of national defense, these weaknesses can limit an organization's ability to collaborate effectively and responsively to cyber threats, necessitating investment in improving security and adopting adequate technology to address these weaknesses.

#### 3.2.4.3. Limited Human Resources and Expertise in Technology Development and Utilization

Limited resources and expertise in technology development and utilization can be a weakness in the collaboration of stakeholders in cyberspace to support national defense, especially when coupled with the low quantity and quality of cybersecurity human resources (HR) and the lack of capability in developing and utilizing technology. Organizations with limited resources struggle to recruit and retain high-quality cyber talents. This is because cyber talents are highly sought after and scarce, and organizations with limited resources may struggle to compete with larger organizations that can offer more competitive salaries,

benefits, and career advancement opportunities (Maurer and Nelson, 2020). Additionally, the lack of capability in developing innovative and adequate cybersecurity technology can also hinder collaborative efforts. Vulnerable infrastructure can be a gap for cyber attacks, reducing trust levels and effectiveness in dealing with increasingly complex threats. Therefore, investment is needed in developing quality cybersecurity HR and enhancing capabilities in developing and utilizing cybersecurity technology that meets current security demands to support collaboration in national defense in cyberspace.

### *3.2.5.* Legal

#### *3.2.5.1.* Limited Number of Regulations

One of the weaknesses in the collaboration of stakeholders in cyberspace to support national defense is the limited number of regulations governing cybersecurity aspects in Indonesia. Although Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law) provides protection for electronic content and transactions and regulates some violations such as illegal content distribution and unauthorized access to computer systems, these regulations still have limitations in addressing crucial cybersecurity aspects. For example, the ITE Law does not cover information infrastructure and networks or human resource expertise in cybersecurity. Furthermore, regulations related to cyber law are scattered across several regulations and laws with limited scope. Therefore, Indonesia does not yet have adequate legal standing in facing cybersecurity challenges, resulting in a lack of security in the digital ecosystem in the country. Regulations regarding cybersecurity in Indonesia are not supported by adequate legal frameworks, thus not providing a sense of security in the utilization of the digital ecosystem in Indonesia (Anjani, 2021).

#### *3.2.5.2.* Slow Technological Regulatory Development

Slow technological regulatory development hinders collaboration among stakeholders in cyberspace to support national defense. Weak regulations that sometimes impede the absorption process of the latest technology domestically cause uncertainty and inefficiency, as seen in the handling of online transportation and taxes for internet companies in Indonesia, where clear and comprehensive regulations only emerged after pressure and urgent needs. This delay results in technology businesses growing without clear guidelines, delaying necessary rule adjustments for security and effective coordination. Additionally, a lack of cross-sector coordination and strong authorities leads to Indonesia "missing out" on the economic value of technological products and hinders preparedness against cyber threats. Therefore, slow regulatory development not only hampers collaboration but also weakens national defense against cyber threats (Agung, 2017). Moreover, the absence of a strong legal foundation in cybersecurity blurs responsibilities and hampers the implementation of cybersecurity practices. Thus, comprehensive regulations governing cybersecurity in Indonesia are needed. A Cybersecurity Law should clearly define the roles, responsibilities, and authorities of relevant institutions in facing cybersecurity threats (Budi et al., 2021). Although efforts to create legal standing such as the Cyber Security Bill have begun, these regulations are still pending (Anjani, 2021).

#### *3.2.5.3.* Low Compliance with Regulations

Low compliance with regulations is a significant weakness in the collaboration of stakeholders in cyberspace to support national defense. Cybercrime has become a rampant threat with perpetrators utilizing global information technology without geographical

limitations, causing widespread impact on the global economy. Cybersecurity experts estimate that the total cost of cybercrime will increase by 15% per year over the next five years, reaching USD 10.5 trillion per year by 2025, up from USD 3 trillion in 2015 (Globe Newswire, 2020). The International Monetary Fund (IMF) also refers to cyber risks as a "new threat to financial stability" and urges strengthening cybersecurity capacities in low-income countries (IMF, 2020).

In Indonesia, data shows a high number of reported cybercrime cases to the Cybercrime Directorate of the Indonesian National Police (Ditipidsiber Polri) from 2017 to 2020, with 16,845 reports of cyber fraud crimes and 2,259 reports in 2020 resulting in economic losses of Rp15.17 billion. In 2022, the Indonesian National Police handled 8,831 cybercrime cases across Indonesia, with the Jakarta Metropolitan Police (Polda Metro Jaya) recording the highest number of cases at 3,709 (Pusiknas, 2021). Despite continued law enforcement efforts, this data reveals that compliance with regulations in cyberspace is still low. This is a weak point in collaboration to combat crimes in the digital realm, hindering the effectiveness of security measures and coordination between the government and private sector. Low compliance indicates the need for a more comprehensive and integrative approach to implementing and overseeing cyber regulations to strengthen national defense against digital threats.

## 3.3. OPPORTUNITIES

Opportunities for collaboration among stakeholders in cyberspace to support national defense are influenced by political, economic, social, and technological factors. Understanding these opportunities in collaboration will be beneficial in adapting to the evolving environment, seizing arising advantages, and anticipating potential threats.

### 3.3.1. Political

#### 3.3.1.1. Building Strong Relations in the Ecosystem

Collaboration among stakeholders in cyberspace presents a significant opportunity to build strong relations within the cybersecurity ecosystem to support national defense. This collaboration enables the exchange of threat information, learning from each other's experiences, and developing more effective defense strategies. By fostering strong relationships and close cooperation, organizations within the cybersecurity ecosystem can enhance their capabilities to detect, prevent, and respond to cyber threats, reduce duplication of efforts, improve cross-sector communication, and increase efficiency in achieving protection goals. Through investment in collaboration, stakeholders will be engaged, enthusiastic, and committed to achieving these collaborative goals (Givens, 2013).

#### 3.3.1.2. International Cooperation

Cyber threats often transcend national borders, making international cooperation crucial. Collaboration in law enforcement, sharing intelligence information, and other efforts can help identify and respond to emerging threats more effectively (Decker, et al., 2023). International cooperation in the cyber realm presents a major opportunity in combating cyber threats as it allows for information and intelligence sharing, coordination of security standards, skills exchange, cross-border attack responses, and joint security infrastructure development, all of which strengthen collective capabilities in facing increasingly complex and cross-national cyberattacks. Collaboration can be expanded through partnerships with international institutions and other countries. Focusing on technology alone in addressing

challenges in cyberspace is inadequate. Cybersecurity should be viewed as a system involving legal aspects, organizations, skills, cooperation, and technical implementation working synergistically to achieve effectiveness (International Telecommunication Union, 2017).

### 3.3.2. Economy

#### 3.3.2.1. Joint Investment in Cybersecurity

Collaboration among stakeholders in cyberspace offers opportunities for joint security investment, especially considering the increasing cyber incidents indicating potential significant impacts due to failure to address these threats (Choucri, et al., 2013). Although limited budgets often hinder investment in collaborative initiatives, such collaboration can enhance cyber resilience through joint investment. An inspiring example is the Financial Sector Cyber Collaboration Centre (FSCCC), which is a collaborative group among Financial Authorities, industry, the National Crime Agency (NCA), UK Finance, and the National Cyber Security Center (NCSC). FSCCC has created innovative initiatives to enhance the resilience of the UK financial sector by coordinating responses to potential cyber incidents, analyzing information from various sectors, and strengthening cyber intelligence from diverse sources. The collaboration undertaken by FSCCC with various partners, such as the Cyber Defense Alliance (CDA) and the Financial Services Information Sharing and Analysis Center (FS-ISAC), is evidence that joint investment in cybersecurity can provide significant benefits in supporting national defense (National Cyber Security Center, 2021).

### 3.3.3. Social

#### 3.3.3.1. Increasing Public Trust

Increasing public trust in the government is an opportunity arising from collaboration among stakeholders in cyberspace. When the public has high confidence in the government's ability to protect cybersecurity, it creates opportunities to strengthen public support for collaborative efforts between the government, the private sector, and other stakeholders. Moreover, high trust can facilitate closer cooperation, more open information exchange, and more effective policy implementation in addressing cyber threats. To enhance public support for collaboration among stakeholders in cyberspace, education and public awareness of cybersecurity need to be improved through awareness campaigns and educational programs. Transparency and accountability in cybersecurity policies are also essential to strengthen public trust, with clear mechanisms for reporting and addressing cybersecurity incidents (Decker, et al., 2023). Thus, increasing public trust can become a driving force for progress in national defense through more effective collaboration in the cybersecurity realm.

### 3.3.4. Technology

#### 3.3.4.1. Technological Development and Innovation

The evolution of technology and innovation in the cyber realm creates significant new opportunities to strengthen collaboration among stakeholders in cyberspace in responding to evolving threats. With the continuous development of sophisticated functions in cyberattack tools, such as artificial intelligence, big data, deep learning, and neural networks, stakeholders have the opportunity to address threats more effectively. Furthermore, the advancements in information and communication technology enable the creation of superlogical connections, accelerate data transmission, and overcome physical

distance barriers in cyberspace. This provides a strong foundation for developing more responsive and efficient defense strategies against cyberattacks. Additionally, responsive and proactive cyber maneuver tactics can be implemented using artificial intelligence, enabling the development of effective offensive security mechanisms (Sin-Kon Kim, Sang-Pil Cheon, and Jung-Ho Eom, 2019). Therefore, the integration of advanced technologies like artificial intelligence, big data, deep learning, and neural networks is crucial in strengthening collaboration among stakeholders in cyberspace and addressing increasingly complex and dynamic cyber threats in the future.

### 3.4. Threats

Threats in the collaboration among stakeholders in cyberspace to support national defense are influenced by political, technological, legal, and environmental factors. Understanding threats in collaboration will be beneficial in addressing existing risks and enhancing overall security.

#### 3.4.1. Political

##### 3.4.1.1. Complex and Evolving Cyber Threats

The increasingly complex and evolving cyber threats have become one of the main challenges in the collaboration among stakeholders in cyberspace to support national defense. The advancements in technology and tactics in cyber attacks have significantly increased threats to national security, such as attacks sponsored by major countries like Russia, China, Iran, and North Korea, which can steal sensitive information or disrupt critical infrastructure. Such attacks can provide strategic advantages to attacking countries in military operations (Garamone, 2018). Additionally, cybercrimes committed by criminal organizations or individuals also pose a serious threat to cyber security. Advanced malware attacks and theft of sensitive data are real threats that must be taken seriously (Wilson, 2019).

Internal threats are also significant risks, such as when military personnel or contractors unintentionally or intentionally leak sensitive data or disrupt military systems (Lyons, 2023). Supply chain attacks are also a serious threat as they can infect components before they are integrated into military systems (Wilson, 2019). Furthermore, sophisticated and undetected Advanced Persistent Threats (APTs) over a long period, espionage attacks, subversion, and sabotage of military infrastructure through cyberattacks are significant efforts to steal sensitive information, disrupt operations, and manipulate public opinion (Wallace, 2013). Complex and evolving cyber threats bring the potential for economic losses, reputation damage, and harm to individuals and companies. Continuous changes in cyberattack strategies and tactics demand close collaboration among cyber stakeholders to ensure strong and responsive defense against these evolving threats.

##### 3.4.1.2. Security Gaps

Security gaps pose a serious threat to the collaboration among stakeholders in cyberspace that can be exploited by foreign countries or negative actors as a tool for diplomacy or political influence. This has the potential to create political tensions and affect the dynamics of collaboration among stakeholders in cyberspace. Political dynamics also have a direct impact on the formation of regulatory policies related to cyber security. If there is no strong political agreement regarding regulations, or if those regulations are not consistently enforced, security gaps may increase, ultimately threatening effective

collaboration among stakeholders. Differences in cyber security regulations across jurisdictions also pose a threat, with challenges in coordination, compliance, legal risks, and cross-border attacks hindering stakeholder cooperation (Babikian, 2023; Decker, 2023). These security gaps also impact the limited ability of collaboration to address threats comprehensively and consistently. Misalignment in security standards and differing understandings of cyber threats can slow down responses to attacks, and increase vulnerabilities in the cyber security ecosystem. Collective efforts are needed to address these security gaps by enhancing coordination, sharing information, and adopting uniform security standards to effectively and efficiently improve collaboration in maintaining cyber security.

### 3.4.2. Technology

#### 3.4.2.1. Evolving Cyber Attack Technologies

The continuously evolving cyber threats are one of the crucial threats to the collaboration among stakeholders in cyberspace to support national defense. With advancements in information and communication technology, hackers and cybercriminals continuously seek new ways to exploit vulnerabilities and bypass established security measures (Institute of Data, 2024). The progress in cyber technology has resulted in the creation of sophisticated cyberattack tools equipped with self-learning features. By leveraging technologies like artificial intelligence, big data, deep learning, and neural networks, these tools can independently adapt, develop, and discover new attack methods, demanding stronger and adaptive defense strategies in the cyber realm. Advanced pattern recognition capabilities enable these tools to identify and exploit repetitive patterns in network traffic or system behaviors, thus increasing the success rate of attacks. Additionally, cyberattack tools with cross-domain capabilities can operate across physical, digital, and human interfaces, allowing attackers to launch coordinated and multifaceted attacks. Human-centric design principles enable attackers to exploit vulnerabilities and human behaviors through social engineering tactics. Moreover, the integration of physical and virtual worlds in cyberattack tools poses new challenges for cyber security professionals, as attackers can now target digital systems and physical infrastructure. Overall, advancements in cyberattack tools highlight a shift towards more sophisticated, targeted, and persistent cyber threats, necessitating strong defense strategies to mitigate the evolving risks in cyberspace (Sin-Kon Kim, Sang-Pil Cheon, and Jung-Ho Eom, 2019). This underscores the importance of collaboration among stakeholders in cyberspace to continually monitor these technological advancements to anticipate and combat the evolving and detrimental cyber threats to national security.

#### 3.4.2.2. Unreliable Technology

Unreliable technology poses a serious challenge to collaboration among stakeholders in cyberspace to support national defense. Ineffective threat detection systems can lead to failure in identifying potentially damaging cyberattacks, while technology vulnerable to data leaks jeopardizes the security of sensitive information. For example, the development of Quantum Computing promises advancement but also brings risks to data encryption, necessitating quantum-resistant cryptography. The widespread use of Internet of Things (IoT) devices also increases security vulnerabilities, requiring continuous innovation in protection. Although Blockchain Technology has revolutionized trust in digital transactions, challenges related to data privacy still need to be addressed. Biometric

Authentication offers strong security but also raises concerns about data privacy and potential misuse, highlighting the need for responsible implementation (Intone Network, 2023). Similarly, autonomous cyber technology, while promising operational advantages like surpassing human armies in terms of speed and scale, shortcomings in predictability, reliability, and understanding can pose risks, especially in unfriendly and dynamic environments (Stroppa, 2023). Therefore, stakeholders in cyberspace need to consider unreliable technology as a threat that needs to be addressed seriously.

#### 3.4.2.3. Cyber Espionage

Cyber espionage poses a serious threat in the context of national defense as it has the potential to steal sensitive information, disrupt critical infrastructure, and manipulate public opinion (Wallace, 2013). Technological advancements are making it easier for cybercriminals to conduct espionage, increasing the risk to national security with the potential theft of secret information, leakage of sensitive data, and even manipulation of state systems. A concrete example of the cyber espionage threat is the existence of the Snake malware, used in cyberattacks against the German Foreign Ministry and NATO computers (Eckel, 2023). Additionally, hacker groups from China also use ransomware as a disguise for their malicious activities, making identification difficult and causing disruptions to defense efforts (Toulas, 2022). The case of the arrest of an Israeli private investigator in London on charges of conducting a cyber espionage campaign (Tobin, 2024) illustrates the seriousness of this threat, although extradition efforts against the perpetrator were rejected on legal technicalities. All of this underscores that cyber espionage not only damages national security but also threatens public trust and hinders collaborative efforts to strengthen the country's cyber defense.

### 3.4.3. Legal

#### 3.4.3.1. Regulatory Differences at Regional and Global Levels

Differences in cybersecurity regulations among jurisdictions pose a significant threat in SWOT analysis regarding collaboration among stakeholders in cyberspace. The lack of harmonization in security standards between jurisdictions hinders coordination and effective information sharing, reducing collective efforts against cyber threats. Additionally, the diversity of cybersecurity requirements in various regions creates compliance challenges for organizations operating globally, thus posing legal and financial risks. Cybercriminals exploit these regulatory gaps by conducting cross-border attacks, making investigations and law enforcement prosecutions more difficult. Furthermore, differences in data privacy laws and concerns about data sovereignty hinder efforts to share data and collaborate among stakeholders, weakening collaborative initiatives aimed at effectively addressing cyber threats (Babikian, 2023).

The development of unique information-sharing and accountability models in various regions and countries exacerbates these challenges. For example, proactive steps taken by some countries in Latin America regarding legislation and the establishment of cyber security bodies may create further complexity in collaborative efforts. Similarly, mechanisms like the African Peer Review Mechanism have the potential for collaboration, but differences in regulatory frameworks can hinder smooth cooperation among stakeholders (Decker, 2023). These unique information-sharing models further exacerbate challenges, reflecting conflicts between cybersecurity priorities and digital growth, necessitating a cohesive and

standardized approach in global cybersecurity regulations to strengthen collaboration and effective knowledge exchange.

### 3.4.4. Environment

#### 3.4.4.1. Natural Disasters

Natural disasters significantly threaten collaboration among stakeholders in cyberspace to support national defense. The interaction between physical environmental conditions and digital infrastructure creates substantial risks, especially during events such as storms, earthquakes, and floods that can severely damage data centers, communication networks, and other technology infrastructures, leading to widespread communication and internet outages. Such disasters can have cascading effects on critical infrastructure, including power grids, communication networks, and transportation systems crucial for societal functions. The destruction witnessed during Hurricane Sandy in 2012 and the flood disasters in Germany in 2013 highlight the vulnerability of critical infrastructure to natural disasters (Mittelstädt et al., 2015). Additionally, cyber-attack threats exponentially increase during natural disasters, as attackers exploit the heightened vulnerabilities of defense systems. With the increasing occurrence of natural disasters due to climate change, cybercriminals strategically launch their attacks during these events, making response and recovery efforts more difficult (Chakraborty et al., 2024). Therefore, addressing environmental threats posed by natural disasters is crucial to enhancing resilience and the effectiveness of cybersecurity collaboration in national defense.

#### 3.4.4.2. Attacks on Physical Infrastructure

Physical attacks on cyber infrastructure are a significant threat to collaboration among stakeholders in cyberspace to support national defense. The availability of resources such as electricity is crucial for the sustainability of cybersecurity services. Threats arise when the supply of these resources is disrupted, either due to natural disasters, infrastructure failures, or even direct cyberattacks on the infrastructure. Cyberattacks can be used to cause physical damage to military systems or infrastructure, such as power grids or water processing facilities (Wallace, 2013). For example, widespread power outages can shut down critical data centers and communication systems vital for cyber operations, causing instability in cybersecurity services essential for national defense. In the context of collaboration among stakeholders in cyberspace, the availability of these resources is essential because vulnerabilities to supply disruptions can create gaps in cyber defense that can be exploited by irresponsible parties, posing a higher risk to national security. Therefore, stakeholders need to pay attention to and address threats related to resource availability as part of their collaborative strategy to support national cyber defense.

## IV. Conclusion and Recommendation

### 4.1. Conclusion

The urgent need for stakeholder collaboration in cyberspace to bolster national defense is paramount in today's interconnected digital landscape. As technology continues to advance, bridging the physical and digital realms, the complexity and severity of cyber threats, including cyber warfare, have escalated. The interconnectivity of devices, systems, and networks, coupled with the rapid expansion of the digital economy, has created a fertile ground for cyberattacks, cybercrimes, and cyber-terrorism. While digital infrastructure has

brought unprecedented convenience to daily life, it has also exposed critical vulnerabilities that can compromise security and stability in this globally connected information age. To effectively mitigate these risks and enhance resilience against cyber threats, it is imperative for diverse stakeholders, including government agencies, private sectors, and international partners, to collaborate closely. This collaborative approach is essential for formulating robust policies, responding swiftly to cybersecurity incidents, and protecting critical infrastructure.

Collaboration among cybersecurity stakeholders significantly strengthens national defense through political, economic, social, technological, and legal avenues. Politically, the involvement of various stakeholders, security cooperation, and joint strategy development enhance cybersecurity maturity and coordinated responses. Economically, sharing the burden of security investment reduces costs and improves preventive measures. Socially, increased cybersecurity awareness among users reduces attack risks and enhances participation in security programs. Technologically, advanced tools like AI and IoT improve operational efficiency and threat response. Legally, standardized frameworks, compliance incentives, legal protections, and ensured resource allocation foster a consistent and well-supported cybersecurity environment. These collaborative efforts are essential for building a robust and adaptive national defense in the digital era.

Weaknesses in collaboration among cybersecurity stakeholders in supporting national defense are multifaceted, and influenced by political, economic, social, technological, and legal factors. Politically, misalignment of interests and lack of coordination impede efficient and cohesive responses to cyber threats. Economically, budget limitations restrict investment in comprehensive cybersecurity measures, forcing stakeholders to prioritize certain strategies over others. Socially, the scarcity of skilled cybersecurity professionals, lack of trust and cooperation, and low digital literacy hinder effective collaboration and proactive security measures. Technologically, the complexity of managing multiple security solutions and inadequate security controls create vulnerabilities, while limited expertise in technology development hampers innovation. Legally, the limited number of regulations, slow regulatory development, and low compliance with existing laws weaken the overall cybersecurity framework and coordination efforts. These weaknesses highlight critical areas that require strategic improvements to enhance national defense against cyber threats.

Opportunities for collaboration among stakeholders in cyberspace to support national defense are influenced by political, economic, social, and technological factors. Politically, collaboration can foster strong relationships within the cybersecurity ecosystem, enhancing threat detection, prevention, and response capabilities through the exchange of information and shared experiences. International cooperation is also pivotal, allowing for coordinated responses to cross-border cyber threats and the development of joint security infrastructures. Economically, joint investments in cybersecurity initiatives, such as the Financial Sector Cyber Collaboration Centre (FSCCC), demonstrate how collaborative efforts can enhance cyber resilience and provide substantial benefits. Socially, increasing public trust in the government's cybersecurity capabilities can drive stronger support for collaborative efforts, facilitated by improved public awareness, transparency, and accountability. Technologically, advancements in artificial intelligence, big data, deep learning, and neural networks offer significant opportunities to develop more effective and responsive defense strategies against evolving cyber threats, thus strengthening the overall collaboration among stakeholders in cyberspace.

Collaboration among stakeholders in cyberspace to support national defense faces significant threats influenced by political, technological, legal, and environmental factors. Politically, the evolving complexity of cyber threats from state-sponsored attacks and cybercrimes, alongside security gaps from regulatory inconsistencies, hinder effective cooperation. Technologically, the rapid advancement of sophisticated attack tools and the unreliability of emerging technologies, such as quantum computing and IoT devices, demand robust defense strategies. Cyber espionage further exacerbates these risks by facilitating the theft of sensitive information and disruption of infrastructure. Legally, disparities in cybersecurity regulations across jurisdictions impede coordination and compliance, weakening collective efforts against cross-border attacks. Environmentally, natural disasters pose substantial risks to digital infrastructure, causing outages and increasing vulnerabilities, while physical attacks on infrastructure disrupt essential resources, creating exploitable gaps in cyber defense. Addressing these threats is crucial for enhancing the resilience and effectiveness of collaborative national cybersecurity efforts.

## 4.2. Recommendation

The interconnectedness of digital infrastructure highlights the crucial requirement for stakeholders to collaborate and strategically plan to enhance cybersecurity response capabilities. This is essential to address the constantly evolving cyber threat landscape and to secure and fortify digital infrastructure. Based on the conclusions from the conducted SWOT-PESTLE analysis, several policy recommendations are important to follow up.

The first policy recommendation highlights the importance of improved political collaboration among stakeholders in cyberspace to strengthen national defense. This involves creating regular communication channels, joint working groups, and strategic meetings between government agencies, private sectors, and international partners. Such collaboration is essential for aligning interests, sharing threat intelligence, and coordinating responses to cyber threats. By fostering a culture of information exchange and joint decision-making, political collaboration can enhance cybersecurity maturity and enable coordinated actions against evolving cyber threats.

The second recommendation emphasizes fostering economic partnerships and joint investments in cybersecurity. Establishing funding mechanisms, incentive programs, and public-private partnerships can encourage stakeholders to pool resources and invest in comprehensive cybersecurity measures. This approach reduces financial burdens on individual organizations and promotes robust security infrastructure, advanced threat detection, and improved incident response. By sharing costs and benefits, stakeholders can enhance cyber resilience and national defense capabilities.

The third recommendation underscores the importance of implementing social awareness programs to promote cybersecurity education among users at all levels. These programs aim to increase understanding of cyber risks, best practices, and responsible digital behavior. By fostering a culture of cybersecurity awareness, stakeholders can empower users to recognize and mitigate threats, participate in security programs, and enhance collective defense efforts. This proactive approach can significantly reduce the attack surface and improve overall cyber resilience.

The fourth recommendation advocates adopting advanced technologies like AI, big data analytics, and IoT security solutions. These technologies improve threat detection, automate incident response, and enhance cybersecurity posture. Leveraging AI-driven

threat intelligence and real-time monitoring can help stakeholders proactively mitigate cyber threats. Additionally, IoT security solutions can enhance device security, network segmentation, and access controls, reducing IoT-based attack risks.

The fifth recommendation emphasizes legal harmonization and regulatory alignment to facilitate effective cybersecurity collaboration. Standardized frameworks, cross-border data protection agreements, and compliance mechanisms ensure legal clarity and consistency. Addressing regulatory gaps and promoting international cooperation will enhance legal protections, streamline collaboration, and strengthen defenses against cross-border cyber threats.

The final recommendation focuses on enhancing resilience against natural disasters and physical attacks on digital infrastructure. Developing disaster recovery plans, infrastructure redundancy, and cyber-physical security protocols can minimize disruptions and protect critical resources. Integrating cybersecurity into disaster preparedness enhances infrastructure resilience, reduces vulnerabilities, and strengthens national defense against environmental threats.

Implementing these policy recommendations necessitates a holistic approach that integrates political commitment, economic incentives, social awareness, technological innovation, legal frameworks, and environmental resilience strategies. Collaboration among stakeholders is essential to navigate the complex and evolving landscape of cyber threats, enhance national defense capabilities, and safeguard critical digital infrastructure in today's interconnected world.

## References

Acronis. (2021). *When More is Not Necessarily Better: The Impacts of Multiple Security Tools*. Available from https://www.cio.com/article/189489/when-more-is-not-necessarily-better-the-impacts-of-multiple-security-tools.html?amp=1. Accessed 5 May 2024.

Aidoo, F.K. (2017). End Users Security Awareness Campaign from Information Security Threats, Vulnerabilities and Concurrent Cyber-Attacks. *Texila International Journal of Academic Research*, 4 (2).

Ajala, O.K. (2023). Establishing Cyber Resilience in Developing Countries: An Exploratory Investigation into Institutional, Legal, Financial, and Social Challenges. *International Journal of Sustainable Infrastructure for Cities and Societies,* 8(9), 1–10. Available from https://vectoral.org/index.php/IJSICS/article/view/27 Accessed 18 May 2024.

Akter, S., Uddin, M.R., Sajib, S., Lee, W.J.T., Michael, K., & Hossain, M.A. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. *Ann Oper Res* (2022). Available from https://link.springer.com/article/10.1007/s10479-022-04844-8#citeas Accessed 4 May 2024.

Anjani, N.H. (2021). Perlindungan Keamanan Siber di Indonesia. *Center for Indonesian Policy Studies.* Available from https://repository.cips-indonesia.org/publications/341780/perlindungan-keamanan-siber-di-indonesia#cite Accessed 18 May 2024.

Ayuwuragil, K. 2017. *Kesadaran Keamanan Siber Indonesia Peringkat ke 70 Dunia. CNN Indonesia*. Available from https://www.cnnindonesia.com/teknologi/20171206162248-185-260555/kesadaran-keamanan-siber-indonesia-peringkat-ke-70-dunia Accessed 19 May 2024.

Babikian, J. (2023). Navigating Legal Frontiers: Exploring Emerging Issues in Cyber Law. *Revista Espanola De Documentacion Cientifica*, 17(2), 95–109. Retrieved from https://redc.revistas-csic.com/index.php/Jorunal/article/view/154 Accessed 23 April 2024.

Babys, S. A. M. (2021). Ancaman Perang Siber di Era Digital dan Solusi Keamanan Nasional Indonesia. *Jurnal Oratio Directa*, 3 (1): 425-442. Available from https://ejurnal.ubk.ac.id/index.php/oratio/article/view/163 Accessed 6 Oktober 2024.

Bauer, J. M., and van Eeten, M. J. G. (2009). Cybersecurity: Stakeholders Incentives, Externalities, and Policy Options. *Telecommunications Policy*, 33: 706–719. Available from https://www.researchgate.net/publication/227426674_Cybersecurity_Stakeholder_incentives_externalities_and_policy_options Accessed 6 Oktober 2023

Bintoro A. (2017). *Regulasi Lambat Jadi Penghambat Perkembangan Teknologi*. Available from https://www.cnnindonesia.com/teknologi/20171109182014-185-254634/regulasi-lambat-jadi-penghambat-perkembangan-teknologi. Accessed 12 May 2024.

Brenner, S. W. (2013). Cyber-threats and the Limits of Bureaucratic Control. *MINN. J.L. SCI. & TECH.* 137. Available from https://scholarship.law.umn.edu/mjlst/vol14/iss1/6. Accessed 18 May 2024

Budi, E., Wira, D., dan Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia Akademi Angkatan Udara* Volume 3, Tahun 2021, hlm. 223-234. Available from https://www.researchgate.net/publication/357360644_Strategi_Penguatan_Cyber_Security_Guna_Mewujudkan_Keamanan_Nasional_di_Era_Society_50 Accessed 21 Juli 2023.

Burri, T., and Trusilo, D. (2021). Ethical Artificial Intelligence: An Approach to Evaluating Disembodied Autonomous Systems (March 31, 2021). In: *Rain Liivoja and Ann Valjataga (eds), Autonomous Cyber Capabilities in International Law, forthcoming 2021*. Available from https://ssrn.com/abstract=3816687 Accessed 18 May 2024.

Camp, L.J., & Lewis, S (2004). Economics of information security, *Springer US* pp. 95-104. Available from https://www.researchgate.net/publication/249908366_The_Economic_Consequences_of_Sharing_Security_Information1 Accessed 4 May 2024.

Chakraborty, S., E. M. Mombeshora, K. P. Clark and T. S. Mbavarira. (2024). *Understanding of Cyber-Attack Vulnerabilities During Natural Disasters and Discussing A Cyber-Attack Resiliency Framework*. Available from https://ieeexplore.ieee.org/document/10500233 Accessed 18 May 2024.

Chaudhari, N., Singh, V., Krishnan, A. (2022). A comparison of cybersecurity regulations: India. *Asia Business Law Journal*, 19 Oktober 2022. Available from https://law.asia/india-cybersecurity-regulations-2022/ Accessed 13 May 2024.

Choucri, N,. Madnick, S., and Ferwerda, J. (2013) "Institutions for Cyber Security: International Responses and Global Imperatives." *Information Technology for Development* 20, no. 2 (October 22, 2013): 96–121. Available from https://dspace.mit.edu/handle/1721.1/109401 Accessed 21 May 2024.

CNBC Indonesia. (2022). *Bjorka Berulah, 2 Instansi Ini Saling Lempar Tanggung Jawab.* Available from https://www.cnbcindonesia.com/news/20220910125507-4-370980/bjorka-berulah-2-instansi-ini-saling-lempar-tanggung-jawab Accessed 6 Oktober 2023.

Cyber Security and Infrastructure Agency. (2024). *Cyber Storm IX: National Cyber Exercise*. Available from https://www.cisa.gov/sites/default/files/2024-04/Cyber%20Storm%20IX%20Fact%20Sheet_v02_508c.pdf Accessed 12 May 2024.

Cybersecurity and Infrastructure Security Agency. (2023). *NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations*. Available from https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a Accessed 5 May 2024.

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34 (1) (2017), pp. 1-7. Available from https://www.sciencedirect.com/science/article/pii/S0740624X17300540?via%3Dihub Accessed 4 May 2024

Decker, D., Rauhut, K., Pytlak, A. (2023). *Fostering Accountability in Cyberspace*. Available from https://www.stimson.org/2023/fostering-accountability-in-cyberspace/ Accessed 28 April 2024.

Gal-Or, E., & Ghose, A. (2004). The economic consequences of sharing security information Environment. *Computers & Operations Research* 85 (2017) 139–153. Available from https://www.sciencedirect.com/science/article/abs/pii/S0305054817300990 Accessed 19 May 2024.

Eckel, M. 2023. The Snake, The FBI, And Center 16: *Why The Takedown Of A 'Most Sophisticated Cyber-Espionage Tool' Is Important. Russia Free Europe Radio Liberty*, 11 May 2023. Available from https://www.rferl.org/a/russia-fsb-malware-snake-takedown/32407612.html Accessed 12 May 2024

Ertan, K. F., Pernik, P., Stevens, T. (2021). Cyber Threats and NATO 2030: Horizon Scanning and Analysis. *NATO Cooperative Cyber Defence Centre of Excellence*. Available from https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf Accessed 18 May 2024.

Forbes. (2013). *How to prevent cybercrime*. Available from https://www.forbes.com/sites/thesba/2013/08/28/how-to-prevent-cybercrime/#62f3ad6efffd. Accessed 6 Oktober 2023.

Garamone, J. (2018). *Cyber Tops List of Threats to U.S., Director of National Intelligence Says*. Available from https://www.defense.gov/News/News-Stories/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/ Accessed 22 April 2024.

Gordon, L.A., Loeb, M.P., Lucyshyn, W., Zhou, L (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, 34 (5) (2015), pp. 509-519. Available from https://www.sciencedirect.com/science/article/abs/pii/S0278425415000423 Accessed 4 May 2024.

Globe Newswire. (2020). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. Available from https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-TheWorld-10-5-Trillion-Annually-By-2025.html Accessed 25 May 2024.

Hübner, S. F., Alcaraz, C., Ferreira, A., Gago, C. F., Lopez, J., Markatos, E., Islami, L., dan Akil, M. (2021). Stakeholders Perspectives and Requirements on Cybersecurity in Europe. *Journal of Information Security and Applications,* 61. ISSN 2214-2126. Available from https://www.researchgate.net/publication/353119907_Stakeholder_perspectives_and_requirements_on_cybersecurity_in_Europe Accessed 19 May 2024.

Institute of Data. (2024). *AI in Cyber Security: Enhancing Protection and Defence*. Available from https://www.institutedata.com/blog/ai-in-cyber-security/ Accessed 7 May 2024.

International Monetary Fund. (2020). *Cyber Risk is the New Threat to Financial Stability*. Available from https://www.imf.org/en/Blogs/Articles/2020/12/07/blog-cyber-risk-is-the-new-threat-to-financial-stability Accessed 25 May 2024.

International Telecommunication Union. (2024). *National Cybersecurity Strategies Repository*. Available from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx Accessed 25 May 2024.

Intone Network, (2023). *The Future of Cybersecurity Emerging Technologies*. Available from https://intone.com/the-future-of-cybersecurity-emerging-technologies/ Accessed 23 April 2024.

ISC2. (2023). ISC2 *Reveals Growth in Global Cybersecurity Workforce, But Record-Breaking Gap of 4 Million Cybersecurity Professionals Looms*. Available from https://www.isc2.org/Insights/2023/10/ISC2-Reveals-Workforce-Growth-But-Record-Breaking-Gap-4-Million-Cybersecurity-Professionals Accessed 4 Maret 2024.

Karjalainen, M., Siponen, M., & Sarker, S. (2020). Toward a stage theory of the development of employees' information security behavior. *Computers & Security,* 101782. Available from

https://www.sciencedirect.com/science/article/pii/S0167404820300675 Accessed 21 May 2024.

Kaur, R., Gabrijelčič, D., Klobučar, T. (2023). Artificial intelligence for cybersecurity: *Literature review and future research directions. Information Fusion,* Volume 97. Available from https://www.sciencedirect.com/science/article/pii/S1566253523001136 Accessed 20 May 2024.

Kim, S.K., Cheon, S.P., Eom, J.H. (2019). A leading cyber warfare strategy according to the evolution of cyber technology after the fourth industrial revolution. *International Journal of Advanced Computer Research*; Bhopal Vol. 9, Iss. 40, (Jan 2019): 72-80. Available from https://www.proquest.com/openview/110828b5fc7cbbc3860947b5b125c2c0/1?pq-origsite=gscholar&cbl=1626343 Accessed 11 May 2024.

Lebo, D., dan Anwar, S. (2020). Pemberdayaan Komunitas Siber oleh Pemerintah Republik Indonesia dari Perspektif Strategi Perang Semesta. *Jurnal Strategi Pertahanan Semesta*, 6 (1): 101-127. Available from https://jurnalprodi.idu.ac.id/index.php/SPS/article/view/653 Accessed 6 Oktober 2023

Lewis, J. A. (2010). Sovereignty and the Role of Government in Cyberspace. *The Brown Journal of World Affairs,* XIV (II): 55-65. Available from https://repository.library.brown.edu/studio/item/bdr:1078801/PDF/?embed=true?embed=tru Accessed 18 May 2024.

Lopez, T.C. (2022). *DOD: It's Not Just State Actors Who Pose Cyber Threat to U.S.* Available from https://www.defense.gov/News/News-Stories/Article/Article/3039462/dod-its-not-just-state-actors-who-pose-cyber-threat-to-us/ Accessed 22 April 2024

Lyons, J. (2023). *US military battling cyber threats from within and without.* Available from https://www.theregister.com/2023/08/01/us_military_cybersecurity/ Accessed 22 April 2024.

Maurer, T., Levite, A., and Perkovich, G. (2017). Toward a Global Norm Against Manipulating The Integrity of Financial Data. *Economics Discussion Papers,* No 2017-38, Kiel Institute for the World Economy. Available from http://www.economics-ejournal.org/economics/discussionpapers/2017-38. Accessed 6 Oktober 2023.

Mittelstadt, S., Wang, X., Eaglin, T., Thom, D., Keim, D., Tolone, W., & Ribarsky, W. (2015). An Integrated In-Situ Approach to Impacts from Natural Disasters on Critical Infrastructures. *2015 48th Hawaii International Conference on System Sciences*. pp. 1118-1127, doi: 10.1109/HICSS.2015.136. Available from https://sci-hub.se/10.1109/hicss.2015.136 Accessed 18 May 2024.

National Cyber Security Center. (2021). *Financial Sector Cyber Collaboration Centre (FSCCC).* Available from https://www.ncsc.gov.uk/information/financial-sector-cyber-collaboration-centre-fsccc Accessed 6 Oktober 2023

Harsono, N. (2022). Despite improvements, Indonesia's digital literacy remains low. *The Jakarta Post,* 20 January 2022. Available from https://www.thejakartapost.com/business/2022/01/20/despite-improvements-indonesias-digital-literacy-remains-low.html Accessed 12 May 2024.

O'Halloran, J. (2017). *Challenges Of Public-Private Partnerships In Cybersecurity*. Available from https://www.academia.edu/36194661/CHALLENGES_OF_PUBLIC_PRIVATE_PARTNERSHIPS_IN_CYBERSECURITY Accessed 28 April 2024.

Paul, J. A., Wang, X. (2019). Socially optimal IT investment for cybersecurity. *Decision Support Systems*, 122(), 113069–. doi:10.1016/j.dss.2019.05.009. Available from https://www.sciencedirect.com/science/article/abs/pii/S0167923619300983 Accessed 6 Oktober 2023.

Preis, B. & Susskind, L. (2022). Municipal Cybersecurity: More work needs to be done. *Urban Affairs Review*, 58 (2), pp. 614-629. Available from https://journals.sagepub.com/doi/10.1177/1078087420973760#fn2-1078087420973760 Accessed 21 May 2024.

Proofpoint (2021). *Proofpoint's State of the Phish Report reveals remote workers in Australia are currently undertrained to deal with cyber threats*. Available from https://www.proofpoint.com/au/newsroom/press-releases/proofpoints-state-phish-report-reveals-remote-workers-australia-are Accessed 4 May 2024.

Rizki, A., dan Timur, F. G. C. (2021). *Synergy of Multi-Stakeholders in Defending Indonesia from Cyber Threats*. Available from https://e-journal.unas.ac.id/index.php/jsps/article/view/80/68 Accessed 6 Oktober 2023

Rondelez, R. (2018). Governing Cyber Security through Networks: An Analysis of Cyber Security Coordination in Belgium. *International Journal of Cyber Criminology*, 12 (1): 300–315. ISSN: 0973-5089. DOI: 10.5281/zenodo.1467929. Available from https://www.cybercrimejournal.com/pdf/RondelezVol12Issue1IJCC2018.pdf Accessed 18 May 2024.

Schilling, A. (2017). *A framework for secure IT operations in an uncertain and changing environment*. Available from https://www.sciencedirect.com/science/article/abs/pii/S0305054817300990 Accessed 18 May 2024.

Sanchez, S.L. (2017). Artificial Intelligence (AI) Enabled Cyber Defence. *European Defence Matters*, no. 14 (2017): 18. Available from https://eda.europa.eu/docs/default-source/eda-magazine/edm-issue-14_web.pdf Accessed 18 May 2024.

Saudi, A. (2018). Kejahatan Siber Transnasional dan Strategi Pertahanan Siber Indonesia. *Jurnal Demokrasi & Otonomi Daerah*, 16 (3): 165-256. Available from https://jdod.ejournal.unri.ac.id/index.php/JDOD/article/view/6811 Accessed 6 Oktober 2023.

Spinu, N. (2020). *Moldova Cybersecurity Governance Assessment. Switzerland: Geneva Centre for Security Sector Governance.* Available from https://www.dcaf.ch/sites/default/files/publications/documents/MoldovaCybersecurityGovernanceAssessment.pdf Accessed 18 May 2024.

Srdjevic, Z., Bajcetic, R. & Srdjevic, B. (2012). Identifying the Criteria Set for Multicriteria Decision Making Based on SWOT/PESTLE Analysis: A Case Study of Reconstructing A Water Intake Structure. *Water Resource Manage* 26, 3379–3393 (2012). Available from https://link.springer.com/article/10.1007/s11269-012-0077-2 Accessed 18 May 2024.

Statista. (2010). *Percentage of Stuxnet-infected hosts by country in 2010.* Available from https://www.statista.com/statistics/271110/stuxnet-infected-hosts-by-country/ Accessed 26 May 2024.

Stroppa, M. (2023). Legal and ethical implications of autonomous cyber capabilities: a call for retaining human control in cyberspace. *Ethics Inf Technol* 25, 7 (2023). Available from https://doi.org/10.1007/s10676-023-09679-w Accessed 19 May 2024.

Taddeo, M., McCutcheon, T., and Floridi, L. 2019. Trusting Artificial Intelligence in Cybersecurity Is a Double-Edged Sword. *Nature Machine Intelligence* 1, no. 12 (2019): 557–60, page 557. Available from https://www.researchgate.net/publication/337176016_Trusting_Artificial_Intelligence_in_Cybersecurity_is_a_Double-edged_Sword Accessed 18 May 2024.

Tagarev. T. (2020). Towards the design of a collaborative cybersecurity networked organization: Identification and prioritization of governance needs and objectives. *Future Internet*, 12 (4) (2020), p. 62. Available from https://www.mdpi.com/1999-5903/12/4/62 Accessed 21 May 2024.

Tagarev, T., dan Sharkov, G. (2016). Multi-Stakeholder Approach to Cybersecurity and Resilience. *Information & Security: An International Journal*, 34 (1): 59-68. Available from https://www.researchgate.net/publication/366216551_Multistakeholder_Approach_to_Cybersecurity_and_Resilience Accessed 18 May 2024.

Tatar, U., Çalık, O., Çelik, M., and Karabacak, B. (2014). *A Comparative Analysis of the National Cyber Security Strategies of Leading Nations*. Available from https://fuse.franklin.edu/cgi/viewcontent.cgi?article=1037&context=facstaff-pub Accessed 18 May 2024.

Tim Maurer, Arthur Nelson. (2020). *International Strategy to better protect the financial system against cyber threats*. Available from https://carnegieendowment.org/2020/11/18/international-strategy-to-better-protect-financial-system-against-cyber-threats-pub-83105 Accessed 5 May 2024.

Tobin, S. *Israeli private eye arrested in London over alleged hacking for US firm*. Reuters, 3 May 2024. Available from https://www.reuters.com/world/israeli-private-eye-arrested-uk-over-alleged-hacking-us-pr-firm-2024-05-02/ Accessed 6 May 2024.

Toulas, B. (2022). *Chinese hackers use ransomware as a decoy for cyber espionage*. Bleeping Computer, 23 Juni 2022. Available from https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/chinese-hackers-use-ransomware-as-decoy-for-cyber-espionage/amp/ Accessed 12 May 2024

van Laar, E., van Deursen, A. J. A. M., van Dijk, J. A. G. M., & de Haan, J. (2017). The relation between 21st-century skills and digital skills: A systematic literature review. *Computers in Human Behavior*, 72, 577–588. Available from

https://www.sciencedirect.com/science/article/abs/pii/S0747563217301590?via%3Dihub Accessed 7 May 2024.

Wallace, I (2013). *The Military Role in National Cybersecurity Governance*. Available from https://www.brookings.edu/articles/the-military-role-in-national-cybersecurity-governance/ Accessed 22 April 2024.

Wang, V., Xinyao, Z., Wang, E. (2022). A comparison of cybersecurity regulations: China. *Asia Business Law Journal,* 19 Oktober 2022. Available from https://law.asia/china-cybersecurity-regulations-2022/ Accessed 13 May 2024.

Warta Ekonomi. 2022. *Saling Lempar: Sebenarnya Siapa yang Bertanggung Jawab Atas Kebocoran Data, Kominfo atau BSSN?* Available from https://wartaekonomi.co.id/read443139/saling-lempar-sebenarnya-siapa-yang-bertanggung-jawab-atas-kebocoran-data-kominfo-atau-bssn?page=all Accessed 6 Oktober 2023.

Wilson, J.R. (2019). *Military cyber security: threats and solutions*. Available from https://www.militaryaerospace.com/trusted-computing/article/14073852/military-cyber-security-tactical-network Accessed 22 April 2024.

Zheng, D. E., & Lewis, J.A. (2015). *Cyber threat information sharing: Recommendations for Congress and the administration*. Center for Strategic and International Studies, Washington, DC (2015). Available from http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150310_cyberthreatinfosharing.pdf Accessed 4 May 2024.

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*. Available from https://www.sciencedirect.com/science/article/abs/pii/S1071581919300540?via%3Dihub Accessed 7 May 2024.