NAPBRES
Journal of National Paradigm-Based Resilience Strategy
NAPBRES 2(2): 85–99
ISSN 3047-3799

Institute for Advanced Science, Social and Sustainable Future
MORALITY BEFORE KNOWLEDGE

Integration of cyber defense and conventional security in addressing non-military threats in the digital era

Rosi Fitria[1*], Asep Adang Supriyadi[1]
[1] *Sensing Technology Study Program, Faculty of Defense Engineering and Technology, Universitas Pertahanan Indonesia, Bogor, West Java, 16810, Indonesia.*
*Correspondence: rosi.fitria@tp.idu.ac.id

Received Date: July 16, 2025 Revised Date: August 08, 2025 Accepted Date: August 31, 2025

ABSTRACT

Background: The development of digital technology has transformed the landscape of threats to national security, with non-military threats, including cyberattacks, digital terrorism, and disinformation, becoming increasingly urgent. These threats have the potential to undermine social, economic, and political stability. This study aims to analyze the integration of cyber and conventional defense in strengthening national resilience against non-military threats. **Method:** This research employs a qualitative approach, analyzing literature and policies of national security institutions regarding non-military threats. Primary data were obtained through a literature review of journals and articles accessed via SCOPUS. The study began with brainstorming to identify topics, subthemes, and relationships between concepts. **Findings:** The results indicate that integrating cyber and conventional defense enhances the response to hybrid threats. Joint management of cyber and physical threats, along with sharing resources and information between agencies, enhances the effectiveness of responses to complex threats. **Conclusion**: This study concludes that integrating cyber and conventional defense systems is crucial for addressing threats in the digital age. Its success depends on clear policies, regulations, and strict oversight to ensure effective coordination between relevant agencies. **Originality/Novelty of the Article:** The article's originality lies in proposing an integrated defense model that combines conventional and cyber strategies to address hybrid threats, a topic that has not been extensively discussed in the literature.

KEYWORDS: conventional security; cyber defense; digital era; non-military threat.

1. Introduction

The rapid development of digital technology over time has become one of the primary factors significantly impacting a country's security. In maintaining national security, various threats—both military and non-military—require special attention. Threats to national security consist of military threats, hybrid threats, and non-military threats (Triyana, 2022). Military threats are forms of power used to maintain security through the use of physical force, often marked by armed conflicts. On the other hand, non-military threats include complex emergencies and disasters, which require extraordinary measures from the government to preserve national resilience and security.

Military threats are no longer the primary focus in maintaining national security; non-military threats are playing an increasingly important role and are receiving serious attention from countries worldwide in the rapidly advancing digital era. According to

Cite This Article:
Fitria, R. (2025). Integration of cyber defense and conventional security in addressing non-military threats in the digital era. *Journal of National Paradigm-Based Resilience Strategy, 2*(2), 85-99. https://doi.org/10.61511/napbres.v2i2.2025.2106

Martin (2022), non-military threats have become one of the most significant and pressing security concerns in the digital age. These threats can lead to instability in social, economic, and political spheres. Examples of non-military threats include cyberattacks, terrorism, misinformation, and attacks on vital infrastructure, all of which can disrupt public life and do not require armed force in their process. Therefore, national security arising from non-military threats is considered an important issue for societies and countries today (Prezelj et al., 2020). The new challenges to national security need to be regarded as digital technology continues to evolve, especially in the face of non-military threats. These threats are not only related to the virtual world but also intersect with various sectors of life. The increasing dependence on digital technology and communication has become one of the triggers for non-military threats, thus requiring countries to adjust their defense strategies to address these threats.

Non-military threats not only destroy vital infrastructure but also have widespread impacts that can threaten the economic, governmental, and social sectors of society. One example of a non-military threat is cyberattacks, which have become a significant concern in the digital era. Cyberattacks can occur in various locations and continue to evolve (Guembe et al., 2022). Anything related to technology and communication connected directly to the internet has a high potential to be targeted by cyberattacks. The increasing use of the internet as the most popular source of information and online services (Shaukat et al., 2020) makes it easier for cyberattacks to be carried out through internet systems on connected devices, either by damaging existing systems or spreading viruses that can destroy important data.

Additionally, terrorism has become a non-military threat that is receiving more attention in the digital world. Terrorist groups are now using digital technology to spread ideologies, recruit new members, and plan and carry out attacks. Social media platforms and websites are used as tools to spread propaganda and recruit individuals influenced by radical ideologies. With internet access, terrorist groups can easily reach a wider audience without geographical boundaries, thus increasing the threat to national security. Another form of non-military danger is the spread of inaccurate and harmful information, which can trigger conflicts both online and offline among the public. The increasing number and ease of access to social media make it one of the fastest ways to spread information in the digital age. A typical example is the spread of fake news (hoaxes), where the information may not be accurate and cannot be verified, leading to the erosion of public trust and even causing social harm. For this reason, the government and security institutions must have the ability to identify and address misinformation by filtering available information and conducting thorough verification and analysis of circulating digital content.

Non-military threats impact human security and can trigger conflicts at both the domestic and international levels, ultimately threatening national security stability (Reza, 2021). Another significant non-military threat is the potential disruption of critical infrastructure, including electricity networks, banking systems, transportation, and communications. Threats to infrastructure can take various forms, such as cyberattacks that damage control systems or natural disasters that destroy physical facilities. The impact of these threats extends beyond just the system and affects other sectors that rely heavily on continuous operations. For example, an attack on the energy system could cause a power outage across critical areas such as hospitals, which rely on electricity for medical equipment. If the power supply fails, the consequences would not only be operational losses but could also threaten human lives. Similarly, an attack on the financial system could lead to economic instability and erode public trust in that financial system.

Additionally, attacks can target communication systems by cutting off existing communication networks. In emergencies, this would significantly disrupt the coordination process, making it difficult for the public and the government to carry out rapid and effective responses. If communication systems are disrupted, the flow of critical information needed for crisis management is hindered, and ultimately, accurate decision-making cannot be made. Delays in coordination could exacerbate the impact of a disaster or threat, ultimately jeopardizing public safety and the country's overall stability. Therefore, countries or

governments must protect these infrastructures by developing security policies for internet usage. Additionally, a country needs to have effective cybersecurity management to support its financial growth (AL-Dosari et al., 2024). Cybersecurity management refers to the implementation of technologies, procedures, and practices designed to protect networks, computers, programs, and data from various threats, including non-military threats such as cyberattacks (Sarker et al., 2021).

With the advancement of the digital era, nations must strengthen their security systems, as threats to a country now come not only from military conflicts on battlefields but also from cyberattacks that can damage various vital systems within the country. One step that can be taken is to integrate cyber defense and national security to address threats emerging from the cyber world, such as cyberattacks and cybercrimes (Bellanova et al., 2022). To create a more complete and ideal defense system, conventional security and cyber defense are considered as two interdependent components. Conventional security is a form of national defense against military and physical threats. Steps taken to maintain conventional security include protecting borders, monitoring potential internal and external threats, and providing rapid and direct military responses in emergencies. On the other hand, cybersecurity needs to be strengthened given the continuous increase in technology usage over time.

Cybersecurity focuses on protecting digital systems, networks, and information from threats that can cause damage as severe as physical threats. In this regard, cyber threats such as hacking, computer viruses, ransomware attacks, and attacks on critical infrastructure have become very real threats to national security. The importance of integrating these two forms of security is not only due to the evolving nature of threats but also to the increasing complexity of the threats themselves. Cyber threats do not require direct targets as they can emerge at any time and from any location. In contrast, conventional threats, though still relevant, are insufficient to handle threats originating from the cyber world. Therefore, to face these transnational and varied threats, integration between these two crucial components is necessary.

Moreover, this integration enables the sharing of resources and information between government agencies and the military, which are responsible for maintaining national security. It is not only technology agencies that must be responsible for cybersecurity, but also agencies responsible for sectors such as economics, defense, and energy. Thus, a more comprehensive understanding of threats will enable the country to manage risks better and create more comprehensive laws to address attacks. All parties responsible for national security, including the government, the private sector, and the general public, must be involved in forming these policies.

However, the challenge of integrating these two components is significant due to differences in skills and practical applications. Traditional security focuses more on military readiness, border control, and handling situations requiring physical action, while cybersecurity demands deep technical expertise and an understanding of rapidly evolving digital technologies. Nevertheless, cyberattacks can affect physical infrastructure, while physical threats can exploit weaknesses in cyber systems. Therefore, defense strategies must consider both threats simultaneously (Zhang et al., 2023).

Additionally, the regulatory and policy aspects must also be considered in this integration. The state must create a legal framework that can address emerging issues when cybersecurity and conventional security are combined. This legal framework should encompass data protection, privacy, and regulations related to cyberattacks, while ensuring that defensive actions do not infringe on individual rights or democracy. Overall, to build national resilience against increasingly complex threats in today's digital world, countries can formulate more comprehensive strategies to face the evolving threats, both military and non-military, by integrating these two systems.

2. Methods

This research employs a descriptive qualitative approach, utilizing a library research method, to explore the in-depth integration between cyber defense and conventional security in the face of non-military threats in the digital era. This method was chosen because it provides a conceptual and analytical understanding of the increasingly complex dynamics of national security, which are influenced by the rapid development of information and communication technologies. The primary data sources for this research were obtained from national and international scientific journals indexed in SCOPUS, academic articles, reference books, policy documents, and relevant regulations related to cybersecurity and defense issues.

The research began with a brainstorming session to identify the main topic, essential subthemes, and the relationships between relevant concepts. The results of this process were then visualized in the form of a diagram (Figure 1), which serves as an initial map in designing the structure of the discussion. The diagram systematically illustrates the relationships between the elements of the debate, which include: (1) identification of types of non-military threats, such as economic, social, environmental threats, cyberattacks, and disinformation; (2) integration strategies between cyber defense and conventional security through inter-agency cooperation, development of synergistic policies and regulations, and law enforcement; (3) integration challenges, including resource limitations, differences in organizational culture, and policy mismatches between agencies; and (4) forms of integration implementation through strengthening infrastructure, forming cross-sector joint teams, and utilizing advanced technologies. This visualization helps researchers construct a logical, systematic, and focused writing flow aligned with the research objectives.

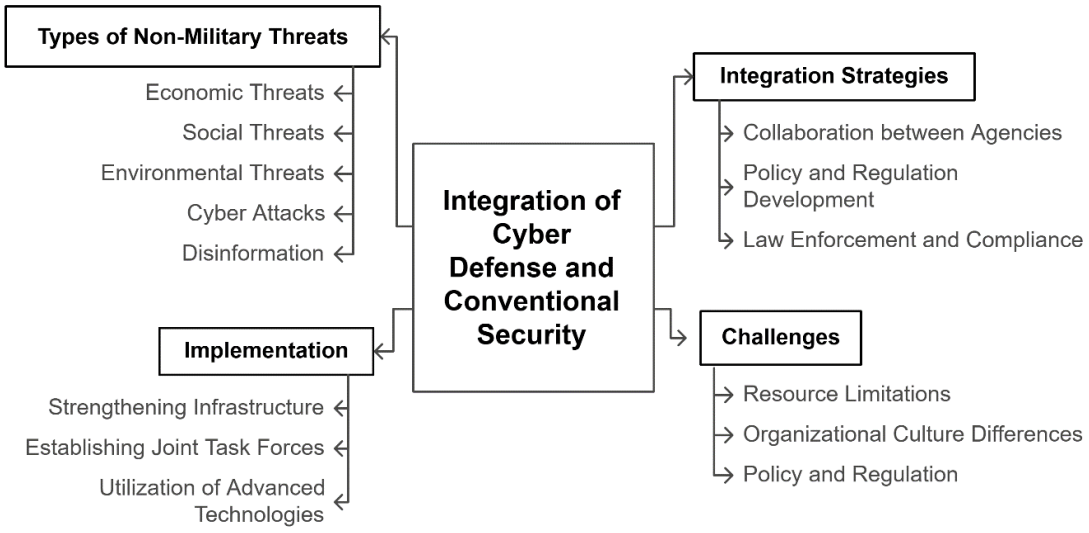

Fig. 1. Brainstorming diagram

3. Results and Discussion

3.1 Identification of non-military threats

In the digital era, non-military threats have become a primary concern in both national and international security. This security has evolved in tandem with technological advancements, where threats initially associated with military attacks have now expanded to include non-military threats. These threats are complex and can occur without regard for national borders, requiring a comprehensive strategy to address them. Identifying non-military threats is one step that society and governments can take to prepare for facing these threats. Non-military threats are more potentially harmful because they operate indirectly, without involving physical force, but rather through technology that we sometimes do not

even realize. Several sectors can be impacted by these threats, including the economy, the environment, technology, and even ideology. Threats related to the economic sector, such as global economic instability and fluctuating prices, can impact people's purchasing power, ultimately weakening national economic resilience. Beyond economic issues, threats from the environmental sector, such as climate change and increasing air pollution, have long-term impacts on the quality of human life, especially in terms of health, as they indirectly threaten human lives. Furthermore, climate change can lead to more frequent natural disasters, such as floods, droughts, and storms, which have become more prevalent in recent years. These disasters cause damage to infrastructure and threaten food security, ultimately impacting the country's political and economic stability. Other threats can also be viewed from a social perspective, where differences in ethnicity, religion, or other social groups can trigger security and political issues within a country. The presence of radical ideological thinking or terrorism in society can disrupt social harmony, divide communities, disturb order, and even endanger the lives of citizens.

The development of digital technology today also presents a new threat that is just as important to be aware of. Public awareness and knowledge of the latest technologies are crucial for minimizing emerging threats. Along with the rapid advancement of digital transformation, several groups have increasingly recognized the benefits that can be gained from modern technology (Jada & Mayayise, 2024). However, the drawbacks of modern technology also present more serious impacts if not used properly. These threats from modern technology include cybercrimes, which heavily rely on technology and the internet. Cyberattacks involve data hacking, identity theft, and attacks on critical infrastructure, leveraging technology and the internet to infiltrate security systems. Some common forms of cyberattacks that frequently occur and have the potential to damage systems include malware, ransomware, and DDoS (Denial-of-Service) attacks (Nguyen & Reddi, 2023).

Malware refers to software designed to damage, access, or control computer systems by infiltrating them without the user's permission. Malware can take the form of viruses, worms, trojans, spyware, and adware. A typical example encountered daily is when a virus warning appears on our personal computers or laptops. A virus spreads through systems by attaching itself to existing programs, while worms can directly copy data from an infected system to another system without needing a host file. Meanwhile, trojans disguise themselves as legitimate software, causing users to unknowingly install them. In reality, these trojans are hacking into the installed systems. On the other hand, spyware and adware collect users' personal information by displaying unwanted ads. Another form of cyberattack is ransomware, which demands a ransom from the user or victim by locking or encrypting data on infected devices. A recent case in Indonesia in 2024 involved a ransomware attack on the National Data Center, where not all of the locked data could be restored, and further attacks could occur even if a ransom payment solution were implemented. Another type of cyberattack is a Distributed Denial of Service (DDoS) attack, which makes an online service or website inaccessible to legitimate users by overwhelming the target server with excessive internet traffic. This DDoS attack exploits weak passwords and unencrypted data transmission (Nimmy et al., 2023). The attack uses a botnet, a group of devices infected with malware and controlled remotely. These devices are then used to send large amounts of requests or data to the targeted server, overloading the system and causing delays or complete service failure.

Another threat that has emerged in society and is frequently encountered in the digital era, easily accessible through the internet, is the spread of misinformation or disinformation. Disinformation is often spread through social media, as nearly all members of society use these platforms with ease. The purpose of disinformation is to disseminate false or misleading information, thereby undermining public trust in an institution and ultimately leading to social tension. This disinformation often becomes a highly effective tool for spreading information on digital media, especially during elections, which can trigger political instability by providing inciting and misleading information whose accuracy is questionable. Therefore, the information officially disseminated by the government is of great importance (Kurnia et al., 2024). Additionally, data security poses a significant threat.

This threat involves the theft of personal data and sensitive information by irresponsible parties (Qammar et al., 2022). For example, personal data such as identification numbers, bank account information, or medical records can be hacked and misused for fraudulent purposes, leading to criminal activities. Another threat related to infrastructure can also affect the daily lives of people. Attacks on infrastructure such as power, water, or transportation systems can disrupt the continuity of operations. Furthermore, attacks involving infrastructure, such as hacking control systems, can cause significant disruptions in the provision of vital services. If these attacks succeed, it can lead to a national or international crisis that disrupts economic stability, endangers public safety, and worsens political tensions. Therefore, countries need to develop strategies to address non-military threats by creating well-structured policies and practical measures to mitigate their impact. Not only is government cooperation essential, but also cooperation between security agencies and the public is crucial to support this strategy by identifying non-military threats on the ground. The role of both the public and private sectors in introducing technology and regulations is necessary to strengthen policies (Bellanova & de Goede, 2022). Thus, the active involvement of various sectors, both public and private, along with public awareness, should not rely solely on military power, but also on joint efforts to prevent and address non-military threats.

3.2 Strategy for integrating cyber defense and conventional security

The digital era requires us to keep up with the rapidly advancing technology and internet developments. With the advent of this technology, threats to data and infrastructure have become vulnerable and can be carried out unknowingly across almost all sectors of life. The growth of technology also correlates with the increasing emergence of non-military threats, which are more concerning and can disrupt the social fabric. Therefore, integrating cybersecurity and conventional security systems is crucial to address hybrid threats (Bıçakcı & Evren, 2022). The combination of cyber technology and conventional systems can create an effective defense strategy (Ghosal & Conti, 2020). These two aspects represent a blend of threats originating from both the cyber world and the physical world, where they are interconnected and can have adverse effects if not appropriately managed. An unsuitable strategy can affect a country's defense policy (Wolfley, 2021). In practice, the integration of cyber defense and conventional security cannot be carried out separately. Conventional security systems are not equipped to handle dynamic digital attacks (Binnar et al., 2024). If these two aspects are handled separately, responses to emerging threats will become slow, overlapping, and ultimately ineffective. This has been demonstrated in several countries where two different agencies often manage cyber defense and conventional security aspects. Cybersecurity is handled by a specialized agency that manages information and communication technology, while national security agencies manage conventional security. In Indonesia, for example, cyber defense is managed by the National Cyber and Encryption Agency/*Badan Siber dan Sandi Negara* (BSSN), which is responsible for protecting national cybersecurity from cyberattacks and coordinating policies, strategies, and implementations related to information and communication technology. On the other hand, conventional security is handled by agencies such as the Indonesian National Armed Forces/*Tentara Nasional Indonesia* (TNI) and the National Police/*Kepolisian Negara Republik Indonesia* (POLRI), which are responsible for maintaining the nation's security and defense. Therefore, these two agencies should not be separated but must actively collaborate and communicate with each other. Secure communication and adherence to good security standards can be key to enhancing cyber resilience (Hou et al., 2024).

Cooperation between cyber defense and conventional security agencies must be supported by clear policies and regulations that establish a clear division of responsibilities between the two institutions to avoid shifting responsibilities. More comprehensive legal policies and strategies are essential to address digital threats (Poornima, 2022). Therefore, the development of policies and regulations becomes a crucial security strategy (Ghelani,

2022). This development relies not only on hardware and software but also requires a legal framework to guide these two aspects, ensuring effective coordination. Cyber defense and conventional security policies must be structured to avoid overlap and ensure active coordination between the various agencies involved. In Indonesia, the policies between BSSN, TNI, and POLRI must clearly outline how cyber defense supports conventional security, and vice versa, in protecting vital infrastructure and national data. These policies should include long-term goals, such as improving national resilience in cyberspace and establishing guidelines for cooperation involving various government agencies, private institutions, and society. Not only at the national level, but policies should also be developed to collaborate with the international community in achieving the integration of cyber defense and conventional security. International collaboration is crucial in strengthening military defense (Wieslander, 2022). Not only policies, but regulations are also vital to establish a legal framework for cooperation between agencies involved in cyber defense and conventional security. Government institutions, such as the Ministry of Communication and Information (Kominfo) and the Ministry of Defense, should be involved in supporting this integration with clear legal regulations concerning the roles and responsibilities of each agency in handling threats related to these two aspects. For example, when a cyber threat targets the national financial system, institutions such as Bank Indonesia and the Financial Services Authority/*Otoritas Jasa Keuangan* (OJK) can collaborate with BSSN and other defense agencies to promptly identify and address the threat. On the other hand, TNI and POLRI should also participate in ensuring the physical and operational security of critical infrastructure by being granted access to data and information from cyber defense. Therefore, alignment between policies and regulations in cyber defense and conventional security is essential.

Clear policies and regulations in the integration of conventional security and defense must also be supported by enhanced oversight and law enforcement. The policies and regulations implemented should not only be normative but also translated into concrete actions. Oversight of these policies and regulations must be carried out regularly, such as through inspections of critical infrastructure readiness, involving audits and evaluations of systems vulnerable to cyberattacks. These inspections aim to identify security gaps that irresponsible parties could exploit. In this regard, cybersecurity audits are crucial as they help ensure that existing defense systems are capable of facing threats, whether from internal or external sources. In addition to audits, ongoing monitoring must also be performed, particularly on critical infrastructure such as communication networks, energy infrastructure, and the financial and health sectors, which heavily rely on digital technology. With this oversight, preventive measures or mitigation efforts can be swiftly addressed. Furthermore, the government must ensure that agencies responsible for handling cyberattacks, such as BSSN, continue to update and enhance their cybersecurity capabilities through training and updates on newer technologies. On the other hand, the government must also enforce strict laws against cybercriminals, whether individuals or groups. The laws applied must be fair and appropriate to each perpetrator involved in criminal actions such as data theft, hacking, and others. Additionally, the government should establish an effective and fair reporting system that facilitates active participation by both the private sector and the public in reporting potential cyber threats. Thus, strict oversight and robust law enforcement can create a solid foundation for maintaining both cybersecurity and conventional security. Moreover, the defense system built should involve all levels of society, both the public and private sectors, to help reduce threats and respond to emerging threats quickly and effectively. Equally important is international cooperation, which is essential for exchanging information in the effort to combat cybercrime at any time and under any circumstances.

3.3 Challenges in integrating cyber defense and conventional security

Collaboration between cybersecurity and conventional security is crucial to strengthen responses to increasingly complex cross-border threats (Bellanova & Glouftsios, 2022). However, many intricate challenges in the process hinder the overall effectiveness and efficiency of the national defense system. Security challenges arise due to the growing dependence of society on the internet (Khan et al., 2022). One of the challenges is the limited availability of resources, both in terms of budget and personnel. Limited resources are a significant challenge in implementing both cyber and conventional security (Hameed et al., 2021). Regarding the limited budget, defense agencies face difficult choices when allocating resources between maintaining existing conventional capabilities and developing relatively new cyber capabilities. The development of cyber defense infrastructure requires substantial budget allocations for advanced technology procurement, specialized software, and the latest threat detection systems. Not only is the development of infrastructure required, but the ongoing development and maintenance of cyber defense systems also demand continuous updates to keep up with the latest technological advancements, which are driven by the constantly evolving nature of cyber threats. As a result, the budget allocation may change over time and needs to be sustained. This limitation in budget allocation results in an imbalanced prioritization between conventional and cyber defense, with the current budget being more heavily allocated to conventional defense. In contrast, cyber defense receives limited funding despite the rapidly increasing cyber threats. Another limitation is seen in the human resources available for cybersecurity, which presents a significant challenge due to the lack of knowledge and technical expertise (Moyo & Loock, 2021). The number of experts in government agencies is limited because most experts with high technical skills in the cyber field tend to choose private sector jobs. On the other hand, in the conventional security sector, the number of human resources is relatively higher, but not all possess cybersecurity skills, as they generally focus on physical operations. Therefore, the challenge is to train personnel in both fields, conventional skills as well as cyber skills, which is a need that must be addressed. However, conducting this training requires sufficient resources, both in terms of budget and time.

The organizational cultural differences between cyber defense agencies and conventional security agencies present another challenge that hinders the integration of these two aspects. Conventional security agencies generally have a clear hierarchical structure with standardized and strict operational procedures, as well as a high-discipline culture. In contrast, cyber defense agencies have a more flexible structure, focusing on innovation and relying more on collaboration among various parties involved, as well as the ability to quickly adapt to digital developments. Personnel in cyber defense agencies tend to have civilian backgrounds focused on technology and innovation. In contrast, personnel in conventional security agencies generally have military backgrounds that are more structured, adhering to established doctrines and procedures. Additionally, the decision-making process in conventional security agencies typically takes longer because it must proceed through hierarchical levels and adhere to strict procedures. In contrast, cyber defense agencies require rapid responses and quick decision-making. This difference creates a misalignment in practice, leading to difficulties in coordination between the agencies when responding to cyber threats, which are highly dynamic and rapidly changing. This issue is also supported by the high culture of privacy and secrecy in conventional security agencies, which tends to limit information sharing. On the other hand, cyber defense agencies require collaboration and information sharing, combining strengths from both the public and private sectors (Paalo et al., 2024). This difference becomes evident when a country faces an emergency involving both cyber and physical threats simultaneously. The organizational culture contributes to delays in responding to these threats because each agency has a distinct approach and timeline for addressing them. To overcome these differences, it is necessary to foster a supportive work culture between the agencies by conducting joint training sessions to exchange information and understand the challenges and working methods of each agency.

Challenges in policies and regulations also become obstacles that need to be addressed in the integration of these two aspects. Policy is a critical domain in cybersecurity

management (Liebetrau, 2024). In many cases, the policies and regulations between the two do not align with each other and are often contradictory. Moreover, the lack of clarity regarding authority and responsibility in addressing cyber threats leads to overlaps or even a lack of response to these threats. For example, some countries have yet to determine which agency should respond when a cyberattack occurs and which resources they will choose to deploy. Another example is that strict personal data protection policies may hinder cyber defense agencies from accessing the necessary information to detect and respond to threats in a timely manner. On the other hand, in conventional security agencies, regulations prioritize physical protection and focus more on direct threats, such as military attacks or terrorism, without considering cyber threats that could compromise vital infrastructure. Therefore, precise and robust standard regulations and security systems are crucial for protecting sensitive data from cyberattacks (Sadhu et al., 2022). Another challenge is the existence of privacy and data security policies, which create difficulties in information sharing between agencies, the private sector, and even with other countries. These policies make it difficult to obtain the data needed for identification efforts, which complicates the response to emerging cyber threats. Therefore, the government must ensure that policies and regulations support the rapid and effective exchange of information between relevant agencies without compromising data security and privacy. Additionally, the government can create international standards that facilitate information exchange and collaboration between countries worldwide, enabling them to work together in facing cross-border cyber threats.

3.4 Implementation in the integration of cyber defense and conventional security

Digital technology has a profound impact on national security, with increasingly complex potential threats emerging. The growing use of digital media today can be an effective strategy in facing these threats (Li et al., 2020). Threats not only come from conventional forms but also from more sophisticated and hidden threats that are more dangerous. Conventional security, which once operated separately from cyber defense, must now collaborate and integrate to protect the country from all aspects of security threats. Hybrid threats necessitate the coordination of all sectors—government, the private sector, and the general public—to respond to these threats more quickly and effectively. Therefore, the implementation of a defense system that integrates cyber defense and conventional security has become essential in addressing cyberattacks, particularly in protecting sensitive data and user privacy, which are vulnerable to such attacks (Ahmed et al., 2022). During the implementation process, several key components, including strengthening infrastructure, forming joint teams, and utilizing advanced technology, are crucial to consider. Adequate infrastructure is expected to support the smooth operation of the defense. A strong infrastructure will serve as the primary foundation for integrating cyber defense and conventional security. Strengthening infrastructure should involve systems or other elements used to ensure operational continuity, even in the event of a disruption. In this case, the country can build backup data centers and disaster recovery systems supported by physical facilities that can store IT infrastructure equipped with special protections, such as fire detection systems, temperature control systems, and secure electrical networks. Additionally, this infrastructure strengthening is carried out by developing data centers that can securely handle sensitive information. These data centers are expected to facilitate the integration of both aspects, allowing them to exchange information quickly and efficiently while ensuring the security of the data exchanged between agencies. This data security can be protected using encryption systems (Faragallah et al., 2020). Communication networks are another crucial aspect to support infrastructure strengthening. These network infrastructures must be designed to detect and block infected components, preventing them from spreading throughout the network system. The development of protection systems also contributes to infrastructure strengthening, utilizing technologies such as artificial intelligence (AI) that can quickly and efficiently detect and respond to cyber threats (Ding et al., 2022).

The formation of a joint team is another step in the process of integrating both security aspects. This joint team comprises various defense elements with diverse skills and expertise, structured within a robust security framework where both cyber and conventional security work together as a unified entity. The team should at least have expertise in risk management, responding to attacks, and understanding regulations. Strong collaboration between these two teams facilitates faster detection and response to hybrid threats involving both physical and digital components. In this case, establishing an organizational structure and developing clear operational procedures are crucial for operating optimally in addressing the continuously evolving threats. The organizational structure of the joint team should ensure that the security operations center has a leader responsible for the overall security strategy and operations. Under this leader, the heads of cybersecurity and conventional security must regularly coordinate to unify their understanding and implementation of uniform security measures. Therefore, cross-training between these two crucial components is necessary to develop the joint team by sharing training, such as training conventional security personnel in basic cybersecurity knowledge, and vice versa. This training program is designed to prepare the joint team to address more complex threats, including both physical and cyber attacks. On the other hand, the development of operational procedures must allow for interaction and have precise mechanisms. For example, the highest hierarchy in the security operations center is responsible for collecting data from various sources, analyzing potential threats, and ensuring smooth coordination among the relevant teams. Meanwhile, the joint team is responsible for handling threats by designing and executing appropriate mitigation strategies and emergency plans according to the severity of the threats faced.

The utilization of advanced technologies is a key factor in integrating cyber defense and conventional security. This is supported by the synergy between cyber and conventional technologies that can improve operational efficiency and security (Khan et al., 2024). The development and use of technology are highly beneficial in protecting national infrastructure and safeguarding it from cyber threats ("The United States and Bahrain Sign Comprehensive Security Integration and Prosperity Agreement," 2024). Emerging technologies, such as artificial intelligence (AI), the Internet of Things (IoT), blockchain, and cloud-based monitoring systems, can be leveraged to enhance coordination and improve the ability to detect and mitigate complex threats. AI can be used to monitor and analyze threats in real-time by identifying suspicious attack patterns and providing early warning information. In computer network operations, AI can automate the detection and mitigation of cyberattacks (Shandilya et al., 2022). Additionally, AI can identify potential threats that might otherwise go undetected by manual methods through the analysis of big data. Another technology, blockchain—a relatively new development—can be a solution to strengthen data security and protect user privacy (Hafeez et al., 2023). Information shared on this technology can be ensured for authenticity and regulated to prevent data manipulation by using a secure and transparent record-keeping system. Furthermore, the Internet of Things (IoT) is a technology that connects physical devices using the internet, allowing them to collect, share, and analyze data. IoT can develop communication systems that support multiple users for various applications (Irshad et al., 2023). The IoT can also connect various devices, including surveillance cameras, motion sensors, drones, weather monitoring tools, and other devices. All the information from these devices can then be collected and analyzed simultaneously to detect incoming threats. Cloud-based monitoring systems are also crucial in integrating these aspects. These systems enable various agencies to access data and information in real-time efficiently, without being hindered by geographical limitations. Thus, in the implementation process, strategic steps and a comprehensive approach are necessary to create an adaptive defense system that is prepared to face various future threats.

4. Conclusions

Threats to national security are no longer limited to conventional military attacks; non-military threats have become a more crucial aspect, given the rapid advancement of digital technology today. Non-military threats have become increasingly visible, including cyberattacks, economic crises, environmental damage, social issues, and the spread of misinformation or hoaxes. Therefore, the national security system must integrate cyber defense and conventional security to effectively respond to both physical and cyber threats. Non-military threats are more complex because they are not immediately visible, yet they have a significant impact on a country's security and stability. Economic threats can disrupt national financial stability, while environmental threats, such as environmental damage, disrupt societal activities. Social threats, including division and the spread of hatred on social media, also cause internal instability. On the other hand, cyberattacks also pose a significant threat, as they can incapacitate critical infrastructure. Meanwhile, the spread of fake news undermines public trust in the government. Thus, an integration strategy between cyber defense and conventional security systems becomes an essential step to address the complexity and diversity of these threats. A strategy that can be implemented is through cooperation between agencies, the development of fair policies and regulations, and the enforcement of strict laws. Information exchange and the sharing of responsibilities are crucial for cooperation between agencies, supported by clear and firm policies and regulations. These policies and regulations provide the legal foundation for strengthening collaboration and ensuring that each agency involved has a clear and organized role. Proper oversight and law enforcement also assist this integration in maintaining national stability and security more effectively.

In the process, the integration of national defense and security faces many challenges that need to be addressed and overcome. For instance, challenges arise from limited resources, both in terms of budget and human resources. Additionally, differing viewpoints resulting from organizational cultures within the relevant agencies create obstacles in the implementation of planned strategies. Furthermore, policies and regulations that are not aligned also pose challenges in this integration process. Efforts that can be made to implement this integration include strengthening national digital infrastructure, forming joint teams across various agencies, and utilizing advanced technology. A strong infrastructure is expected to ensure that security systems are resilient to threats, supported by joint teams that collaborate effectively in combating those threats. This joint team comprises various agencies, including the military (TNI), police (Polri), and cyber intelligence agencies, working together to ensure that responses to potential threats are carried out swiftly and in a coordinated manner. Additionally, the use of advanced technologies, such as the Internet of Things (IoT), blockchain, artificial intelligence (AI), and cloud-based monitoring systems, can help detect threats and provide data analysis, enabling faster and more accurate solutions. With coordinated efforts and strong policies, it is hoped that the government can maintain the country's sovereignty and security in this digital era, with support from various sectors. Thus, the integration of cyber defense and conventional security becomes a necessity in addressing dynamic and complex non-military threats, in line with the continuous development of technology.

Acknowledgement

The authors would like to express their sincere gratitude to the anonymous reviewers for their invaluable comments and insightful suggestions, which greatly contributed to improving the quality and clarity of this manuscript.

Author Contribution

Conceptualization, R.F.; Methodology, R.F.; Formal analysis, R.F.; Investigation, R.F.; Resources, R.F.; Data curation, R.F.; Writing –original draft preparation, R.F.; Writing – review and editing, R.F., Supervisor, A.A.S.

Funding
This research did not receive funding from anywhere.

Ethical Review Board Statement
Not available.

Informed Consent Statement
Not available.

Data Availability Statement
Not available.

Conflicts of Interest
The authors declare that they have no conflict of interest.

References
Ahmed, M., Cox, D., Simpson, B., & Aloufi, A. (2022). ECU-IoFT: A Dataset for Analysing Cyber-Attacks on Internet of Flying Things. *Applied Sciences (Switzerland), 12*(4). https://doi.org/10.3390/app12041990

AL-Dosari, K., Fetais, N., & Kucukvar, M. (2024). Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges. *Cybernetics and Systems, 55*(2). https://doi.org/10.1080/01969722.2022.2112539

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: an introduction. *European Security, 31*(3). https://doi.org/10.1080/09662839.2022.2101887

Bellanova, R., & de Goede, M. (2022). Co-Producing Security: Platform Content Moderation and European Security Integration. *Journal of Common Market Studies, 60*(5). https://doi.org/10.1111/jcms.13306

Bellanova, R., & Glouftsios, G. (2022). Formatting European security integration through database interoperability. *European Security, 31*(3). https://doi.org/10.1080/09662839.2022.2101886

Bıçakcı, A. S., & Evren, A. G. (2022). Thinking multiculturality in the age of hybrid threats: Converging cyber and physical security in Akkuyu nuclear power plant. *Nuclear Engineering and Technology, 54*(7). https://doi.org/10.1016/j.net.2022.01.033

Binnar, P., Bhirud, S., & Kazi, F. (2024). Security analysis of cyber physical system using digital forensic incident response. In *Cyber Security and Applications* (Vol. 2). https://doi.org/10.1016/j.csa.2023.100034

Ding, M., Liu, W., Xiao, L., Zhong, F., Lu, N., Zhang, J., Zhang, Z., Xu, X., & Wang, K. (2022). Construction and optimization strategy of ecological security pattern in a rapidly urbanizing region: A case study in central-south China. *Ecological Indicators, 136*. https://doi.org/10.1016/j.ecolind.2022.108604

Faragallah, O. S., Afifi, A., El-Shafai, W., El-Sayed, H. S., Alzain, M. A., Al-Amri, J. F., & El-Samie, F. E. A. (2020). Efficiently Encrypting Color Images with Few Details Based on RC6 and Different Operation Modes for Cybersecurity Applications. *IEEE Access, 8*. https://doi.org/10.1109/ACCESS.2020.2994583

Ghelani, D. (2022). Cyber Security in Smart Grids, Threats, and Possible Solutions. CC-BY *American Journal of Applied Scientific Research, 169*.

Ghosal, A., & Conti, M. (2020). Security issues and challenges in V2X: A Survey. *Computer Networks, 169*. https://doi.org/10.1016/j.comnet.2019.107093

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. In *Applied Artificial Intelligence* (Vol. 36, Issue 1). https://doi.org/10.1080/08839514.2022.2037254

Hafeez, S., Khan, A. R., Al-Quraan, M. M., Mohjazi, L., Zoha, A., Imran, M. A., & Sun, Y. (2023). Blockchain-Assisted UAV Communication Systems: A Comprehensive Survey. *IEEE Open Journal of Vehicular Technology, 4.* https://doi.org/10.1109/OJVT.2023.3295208

Hameed, S. S., Hassan, W. H., Latiff, L. A., & Ghabban, F. (2021). A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. *PeerJ Computer Science, 7.* https://doi.org/10.7717/peerj-cs.414

Hou, J., Hu, C., Lei, S., & Hou, Y. (2024). Cyber resilience of power electronics-enabled power systems: A review. *Renewable and Sustainable Energy Reviews, 189*. https://doi.org/10.1016/j.rser.2023.114036

Irshad, R. R., Hussain, S., Hussain, I., Nasir, J. A., Zeb, A., Alalayah, K. M., Alattab, A. A., Yousif, A., & Alwayle, I. M. (2023). IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Approach Toward a Trustworthy Cloud Computing. *IEEE Access, 11*. https://doi.org/10.1109/ACCESS.2023.3318755

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management,* 8(2). https://doi.org/10.1016/j.dim.2023.100063

Khan, A. R., Yasin, A., Usman, S. M., Hussain, S., Khalid, S., & Ullah, S. S. (2022). Exploring Lightweight Deep Learning Solution for Malware Detection in IoT Constraint Environment. *Electronics (Switzerland), 11*(24). https://doi.org/10.3390/electronics11244147

Khan, S. I., Ray, B. R., & Karmakar, N. C. (2024). RFID localization in construction with IoT and security integration. In *Automation in Construction* (Vol. 159). https://doi.org/10.1016/j.autcon.2023.105249

Kurnia, S. S., Rahman, Z., Cakranegar, D. I., Abdulla, S. I., Setiawan, D. A., Agustini, P. M., & Yenrizal. (2024). Effect of Counter-Narratives and Credibility of Sources on Emotional Response: A Study of Instagram and WhatsApp Followers. *Journal of Intercultural Communication, 24*(1). https://doi.org/10.36923/jicc.v24i1.170

Liebetrau, T. (2024). Problematising EU Cybersecurity: Exploring How the Single Market Functions as a Security Practice. Journal of Common Market Studies, 62(3). https://doi.org/10.1111/jcms.13523

Li, Y., Dai, J., & Cui, L. (2020). The impact of digital technologies on economic and environmental performance in the context of industry 4.0: A moderated mediation model. International *Journal of Production Economics, 229*. https://doi.org/10.1016/j.ijpe.2020.107777

Martin, C. (2022). Climate Change and Global Security: Framing an Existential Threat. AJ*IL Unbound, 116*. https://doi.org/10.1017/aju.2022.39

Moyo, M., & Loock, M. (2021). Conceptualising a cloud business intelligence security evaluation framework for small and medium enterprises in small towns of the Limpopo Province, South Africa. *Information (Switzerland), 12*(3). https://doi.org/10.3390/info12030128

Nguyen, T. T., & Reddi, V. J. (2023). Deep Reinforcement Learning for Cyber Security. *IEEE Transactions on Neural Networks and Learning Systems, 34*(8). https://doi.org/10.1109/TNNLS.2021.3121870

Nimmy, K., Dilraj, M., Sankaran, S., & Achuthan, K. (2023). Leveraging power consumption for anomaly detection on IoT devices in smart homes. *Journal of Ambient Intelligence and Humanized Computing, 14*(10). https://doi.org/10.1007/s12652-022-04110-6

Paalo, S. A., Degraft Arthur, D., Dramani, A., & Adu-Gyamfi, S. (2024). Exploring hybrid security strategies in Ghana: State and private sector partnerships. *African Security Review, 33*(1). https://doi.org/10.1080/10246029.2023.2286225

Poornima, B. (2022). Cyber Threats and Nuclear Security in India. *Journal of Asian Security and International Affairs, 9*(2). https://doi.org/10.1177/23477970221099748

Prezelj, I., Injac, O., & Kolak, A. (2020). Democratisation of defence policies and systems in Slovenia and Montenegro: Developmental and comparative aspects. *Politics in Central Europe, 16*(3). https://doi.org/10.2478/pce-2020-0032

Qammar, A., Ding, J., & Ning, H. (2022). Federated learning attack surface: taxonomy, cyber defences, challenges, and future directions. *Artificial Intelligence Review, 55*(5). https://doi.org/10.1007/s10462-021-10098-w

Reza, Md. H. (2021). "Conservation of Environment by Military-A New Dimension of Ensuring Security in Bangladesh." Scholars *Journal of Arts, Humanities and Social Sciences, 9*(6). https://doi.org/10.36347/sjahss.2021.v09i06.012

Sadhu, P. K., Yanambaka, V. P., Abdelgawad, A., & Yelamarthi, K. (2022). Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions. In *Sensors* (Vol. 22, Issue 15). https://doi.org/10.3390/s22155517

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. In *SN Computer Science* (Vol. 2, Issue 3). https://doi.org/10.1007/s42979-021-00557-0

Shandilya, S. K., Upadhyay, S., Kumar, A., & Nagar, A. K. (2022). AI-assisted Computer Network Operations testbed for Nature-Inspired Cyber Security based adaptive defense simulation and analysis. *Future Generation Computer Systems, 127*. https://doi.org/10.1016/j.future.2021.09.018

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access, 8.* https://doi.org/10.1109/ACCESS.2020.3041951

The United States and Bahrain Sign Comprehensive Security Integration and Prosperity Agreement. (2024). *American Journal of International Law, 118*(1). https://doi.org/10.1017/ajil.2023.73

Triyana, H. J. (2022). Conscientious Objection Before the Indonesian Constitutional Court. *Constitutional Review, 8*(2). https://doi.org/10.31078/consrev825

Wieslander, A. (2022). "The Hultqvist doctrine"–Swedish security and defence policy after the Russian annexation of Crimea. *Defence Studies, 22*(1). https://doi.org/10.1080/14702436.2021.1955619

Wolfley, K. J. (2021). Military Statecraft and the Use of Multinational Exercises in World Politics. *Foreign Policy Analysis, 17*(2). https://doi.org/10.1093/fpa/oraa022

Zhang, H., Mi, Y., Fu, Y., Liu, X., Zhang, Y., Wang, J., & Tan, J. (2023). Security defense decision method based on potential differential game for complex networks. *Computers and Security, 129.* https://doi.org/10.1016/j.cose.2023.103187

Biographies of Authors

Rosi Fitria, Sensing Technology Study Program, Faculty of Defense Engineering and Technology, Universitas Pertahanan Indonesia, Bogor, West Java, 16810, Indonesia.

- Email: rosi.fitria@tp.idu.ac.id
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A

Asep Adang Supriyadi, Sensing Technology Study Program, Faculty of Defense Engineering and Technology, Universitas Pertahanan Indonesia, Bogor, West Java, 16810, Indonesia.

- Email: aadangsupriyadi@gmail.com
- ORCID: 0000-0003-1103-6669
- Web of Science ResearcherID: N/A
- Scopus Author ID: 57201546735
- Homepage: N/A