

Cyber Warfare: Exploring New Dimensions in the History of Modern Warfare in Indonesia

Lusiana Dwiyanti, Ayu Agung, Joni Widjayanto, Robby MT, Mowafg Abraham Masuwd

Universitas Pertahanan Republik Indonesia, Indonesia

University of Zawia, Libya

dr.lusianadwiyanti@gmail.com, ayuagung2108@gmail.com

joni.wijayanto6@gmail.com

195.dikreglx@gmail.com, masuwd@zu.edu.ly ²

Corresponding Author: dr.lusianadwiyanti@gmail.com

Article Info

Received: 06-07-2025

Revised: 15-09-2025

Accepted: 09-10-2025

Keywords:

Cyber Warfare, History of
Modern Warfare, Digital
Defence, Cyber Defence
Structure, Defence
Doctrine

Abstract

Cyber warfare has become a significant threat in the current digital era, with an increasing number of cyberattacks targeting critical infrastructure and national defence systems. As cyberattacks continue to evolve and impact various sectors, this study aims to explore a new dimension of modern warfare that has not been extensively documented in Indonesia's official war history. The primary focus of this study is to document and analyse cyber conflicts as a form of new warfare history, which is becoming increasingly relevant in the digital world. A comparison between physical warfare and cyber warfare is conducted to examine the differences in impact, actors, and strategies employed in both forms of conflict. In addition, the study also examines the weaknesses in Indonesia's cyber defence structure over the past decade and provides recommendations for developing a stronger and more adaptive cyber defence doctrine. Through a historiographical approach and critical analysis, this study is expected to contribute to the development of Indonesia's digital defence foundations and the formulation of a more adaptive cyber defence doctrine to enhance Indonesia's preparedness in facing future cyber threats.

I. Introduction

Cyber warfare has become a significant threat in this digital era, creating a new paradigm in national defence strategy. As information technology advances, cyberattacks have become one of the most complex threats to national stability, affecting political, economic, and social sectors. In Indonesia, the growing dependence on digital technology, especially in the public and private sectors, increases vulnerability to attacks that could jeopardise national resilience. This underscores the need for an in-depth analysis of cyber warfare within the context of Indonesia's national defence and exploring solutions to strengthen the existing cyber defence systems.

As the most populous country in Southeast Asia, with a government increasingly reliant on digital technology, Indonesia faces significant challenges in cybersecurity. The country has established several policies to address cyber threats, such as Law No. 11 of 2008 on Electronic Information and Transactions (ITE), as well as the establishment of the National Cyber and Encryption Agency (BSSN) in 2017 to manage cybersecurity at the national level. Despite these measures, the escalating cyberattacks on critical sectors, including government, finance, and other critical infrastructures, demonstrate that Indonesia still faces substantial gaps in its digital preparedness and resilience.

The new dimension of modern warfare involving cyber strengthens the argument that cyber warfare is not just a technical threat but also a strategic issue that must be viewed within the broader context of national defence. Cyber warfare has changed how nations confront threats; previously, the reliance was on traditional armed forces, but now cyber capabilities must be integrated as part of the defence strategy. In this context, Indonesia must reassess its cyber defence structure and policies to better prepare for increasingly sophisticated attacks. One of the main challenges is the uncertainty regarding the form and scale of incoming threats. Unlike physical warfare, which involves direct and predictable conflict, cyberattacks often occur without warning, can be covert, and have the potential to damage a nation's infrastructure in a short time.

In June 2024, Indonesia faced a large-scale ransomware attack targeting the National Data Center (PDNS) in Surabaya. The attack caused significant disruption to government services, including immigration processing at airports and online student registrations. The attackers, believed to be the 'LockBit' hacker group, demanded a ransom of 8 million USD. The Indonesian government refused to pay the ransom, and

an audit of the national data infrastructure revealed that much of the compromised data lacked adequate backups. Reports from BSSN and other cybersecurity agencies indicate

a significant increase in the number of cyber attacks in Indonesia in 2024-2025. These attacks have affected various sectors, including government, finance, and critical infrastructure. While specific data is not always published, this trend highlights the growing complexity and pervasiveness of cyber threats across multiple sectors. This highlights the pressing need to enhance cyber defence policies by adopting more modern and data-driven approaches. In many cases, these cyberattacks can undermine public trust in existing digital systems, potentially reducing the effectiveness of both governmental and economic systems.

In response to the rising cyber threats, President Joko Widodo ordered the formation of the Indonesian Cyber Force as the fourth branch of the Indonesian National Armed Forces (TNI) in September 2024. This initiative aims to strengthen national cyber defense capabilities and improve Indonesia's preparedness against increasingly sophisticated cyberattacks

Previous studies indicate that many countries have developed integrated cyber defence strategies aligned with their national security policies. Countries such as the United States, Russia, and China have seriously built their cyber defence capabilities, establishing dedicated agencies focused on digital threats and integrating cyber capabilities into their military defence strategies. For example, the United States has the Cybersecurity National Action Plan (CNAP) designed to strengthen the country's cyber resilience, including integrating both the public and private sectors in efforts to protect against digital threats. Indonesia, although having measures such as the formation of BSSN and the implementation of the ITE Law, still faces numerous gaps, particularly related to inter-agency coordination, human resource capacity, and existing technological infrastructure.

As cyberattacks continue to evolve and impact various sectors, their potential to disrupt national stability and security has become increasingly significant. The rise of cyber warfare represents a new dimension in modern warfare that has not been widely documented in Indonesia's official war history. Unlike traditional physical warfare, cyber warfare is defined by its complexity, anonymity, and rapid escalation, posing unique challenges to national defence systems. This study aims to explore the growing relevance of cyber conflicts as a form of modern warfare, shedding light on its emerging role in Indonesia's national security landscape.

The primary focus of this research is to document and analyse cyber conflicts within the context of Indonesia's evolving digital security environment. By comparing

physical warfare and cyber warfare, the study will examine the differences in impact, actors, and strategies employed in both forms of conflict. Through this analysis, the study seeks to contribute to the development of more effective cyber defence strategies that can address the growing and multifaceted threats posed by cyber warfare. The author will also analyse the role of existing cyber defence policies, identify gaps in their implementation, and provide recommendations for strengthening these policies. The research is expected to make a significant contribution to the development of a more comprehensive and adaptive cyber defence strategy in Indonesia, serving as a reference for enhancing national digital resilience. As the most populous country in Southeast Asia with rapid technological advancements, Indonesia must be prepared to face cyber threats with more integrated and sustainable policies.

2. Research Method

- a. This study adopts an exploratory and descriptive approach to examine the role of cyber warfare in Indonesia's national defence strategy. A qualitative methodology, using case studies and content analysis, is employed to explore key cyber conflicts impacting critical infrastructure, such as government and financial systems. The research compares cyber warfare with physical warfare, focusing on differences in impact, actors, and strategies used in both types of conflict.
- b. This study use a qualitative approach with a case study design and content analysis to explore cyber defence issues in Indonesia. The qualitative approach is chosen to facilitate a deeper investigation into perceptions, experiences, and challenges in the implementation of cyber defence policies, as well as to understand the social, political, and technical dynamics that shape these policies.

3. Results and Discussion

a. Cyber warfare comparing to physical warfare, in Indonesia's Cyber Defence Structure

Physical warfare traditionally involves direct confrontation between military forces, cyber warfare is characterised by its ability to target critical infrastructure, exploit vulnerabilities in digital systems, and undermine the economic, political, and social stability of a nation. This comparison will provide deeper insight into the changing nature of warfare and the strategies required to safeguard Indonesia's digital assets in an increasingly interconnected world.

The impact of physical warfare has historically been direct and visible, involving large-scale destruction of infrastructure, loss of lives, and significant economic

disruptions. In contrast, the impact of cyber warfare is often more subtle but can be equally, if not more, devastating. Cyberattacks can cripple critical infrastructure without the immediate destruction of physical assets. For instance, ransomware attacks can paralyse government systems, banks, and hospitals, leading to operational halts and long-term financial losses without causing any physical damage. Moreover, the psychological impact of cyber warfare can be profound, as citizens lose trust in digital services, leading to social unrest and erosion of confidence in governance.

In physical warfare, actors are primarily state and non-state military forces, engaging in direct combat or proxy wars. Cyber warfare, however, sees a broader spectrum of actors. While state-sponsored groups are still significant players, a growing number of non-state actors, including cybercriminals, hacktivists, and even private sector entities, now participate in cyber conflicts. This has expanded the scope of cyber warfare, making it less predictable and harder to attribute. As seen in the June 2024 ransomware attack on Indonesia's National Data Center (PDNS), the perpetrators were believed to be the 'LockBit' hacker group, highlighting the role of non-state actors in modern cyber warfare.

The strategies employed in cyber warfare differ drastically from those in physical warfare. Physical warfare often relies on military might, territorial control, and direct engagement. In contrast, cyber warfare leverages advanced technical skills, exploiting vulnerabilities in digital systems to disrupt, steal, or destroy data. Cyberattacks are typically non-traditional, relying on subversive tactics like phishing, DDoS attacks, and ransomware to achieve strategic objectives. These attacks are often covert and can be launched from anywhere in the world, making them more difficult to detect and prevent.

While military forces in physical warfare aim for strategic advantage through direct combat, cyber warfare seeks to achieve influence by exploiting the weaknesses in an adversary's digital infrastructure. For instance, the United States' Cybersecurity National Action Plan (CNAP) integrates both government and private sectors into national cyber defence strategies, employing proactive measures like threat intelligence sharing, which contrasts with the more militaristic approaches seen in physical warfare.

These differences demonstrate that cyber warfare is not merely a technical challenge but a complex and evolving threat requiring new strategies, policies, and

international cooperation. Unlike physical warfare, which is constrained by geographic and legal boundaries, cyber warfare transcends national borders and demands a unified, global response. Indonesia's approach to cyber warfare, integrating both military and civilian sectors through the establishment of the Indonesian Cyber Force in 2024, represents a necessary shift towards a more integrated and adaptive cyber defence strategy.

Cyberattacks have impact various sectors, yet have not been extensively documented in Indonesia's official war history. Indonesia has faced several significant cyberattacks that have impacted both the public and private sectors. Here are some key incidents:

1. LockBit 3.0 Ransomware Attack on National Data Centres (PDN)
In June 2024, over 40 Indonesian government agencies, including the Ministry of Immigration, were targeted in a ransomware attack affecting data centres in Surabaya. This attack caused disruptions to immigration services and airport operations for several days. The hackers, using LockBit 3.0 ransomware, demanded a ransom of \$8 million, which the government refused to pay.
2. Civil Servant Data Leak
In August 2024, the hacking group TopiAx leaked sensitive data of 4.7 million Indonesian civil servants onto the dark web. The leaked data included identification numbers, addresses, and employment details, highlighting vulnerabilities in the government's data security systems.
3. Bjorka's Data Breach of Taxpayer Data
In September 2024, the hacker group Bjorka breached and leaked the personal data of 6.6 million Indonesian taxpayers, including their Taxpayer Identification Numbers (NPWP) and other personal information. The data was sold on the Breach Forums for around IDR 150 million, underscoring the importance of tighter data management practices.
4. DDoS Attack on Suara.com
In April 2025, the Indonesian news website Suara.com was hit by almost 285 million Distributed Denial-of-Service (DDoS) attacks in just 1.5 hours. The attack was carried out using bots with IP addresses from several countries in Europe and Indonesia, highlighting the potential threats to digital infrastructure in the media sector.
5. Stormous Hacking of PT Kereta Api Indonesia (KAI) Website
In 2024, the hacking group Stormous attacked the official website of PT Kereta

Api Indonesia (KAI), stealing tens of thousands of employee data. This attack emphasised the need for stronger data protection for both private companies and public sector organisations.

These incidents demonstrate the critical need for Indonesia to enhance its cybersecurity systems across all sectors to protect sensitive data and critical infrastructure from the growing and evolving cyber threats. Based on the findings of this study, several innovative and constructive recommendations are put forward to enhance Indonesia's cyber defence capabilities and address the emerging cyber threats more effectively:

1. Creation of a Cyber Resilience Index (CRI) for Critical Infrastructure.
It is recommended that Indonesia establish a Cyber Resilience Index (CRI), a national benchmarking tool that assesses the cyber resilience of critical infrastructure in real-time. The concept of a Cyber Resilience Index (CRI) was first introduced by the World Economic Forum (WEF) as part of their efforts to assess and strengthen global cyber resilience. This index could be updated regularly, providing a transparent and objective evaluation of infrastructure security across various sectors, such as energy, banking, transportation, and healthcare. The CRI could be used to identify vulnerabilities, track improvements over time, and help decision-makers allocate resources more effectively. By integrating data-driven insights, this initiative would empower both the public and private sectors to strengthen their security posture.
2. Public-Private Cyber Threat Intelligence Sharing Platform.
To overcome the persistent gap in coordination, Indonesia could create a public-private cyber threat intelligence sharing platform. This platform would allow businesses and government agencies to share threat data, intelligence reports, and best practices in real time. A secure, government-backed platform could be established to anonymise sensitive data, ensuring trust and fostering collaboration. The platform should be supported by regular joint workshops and training sessions between government agencies, the private sector, and academia to continuously enhance the country's collective cybersecurity knowledge.
3. Cybersecurity Mental Health and Resilience Programs for the Workforce.
The increasing frequency and severity of cyberattacks can have a psychological toll on cybersecurity professionals, who are on the front lines of defending

against these threats. Establishing mental health and resilience programs within the cybersecurity workforce is vital to ensure that these professionals

are well-equipped to handle the stress and high pressure associated with their roles. By prioritising mental well-being, Indonesia can ensure a more resilient workforce capable of responding effectively to high-stakes cyber incidents. This would also improve employee retention and foster long-term expertise within the cyber defence sector.

4. **Mandatory Cybersecurity Framework for Indonesian SMEs.** Small and Medium Enterprises (SMEs) represent a significant part of Indonesia's economy, yet many remain vulnerable to cyber threats due to a lack of cybersecurity awareness and resources. A mandatory cybersecurity framework for SMEs should be introduced, offering clear guidelines on minimum security standards that are affordable and achievable. This initiative could be paired with government-subsidised training programs, and tax incentives for businesses that implement cybersecurity measures. By empowering SMEs with the tools and knowledge to defend themselves, Indonesia would create a more resilient digital economy.

These recommendations are designed to create a holistic and forward-thinking approach to cybersecurity, addressing both technical and social aspects while fostering a collaborative national and regional framework. They aim to build a more secure, resilient, and adaptable cyber defence system that can keep pace with the evolving digital threat landscape.

b. Cyber defence policies, and Shortage of Human Resources (HR) in Cybersecurity

Indonesia's cyber defence structure continues to face several challenges that affect its overall effectiveness. One of the key challenges is the need for stronger coordination between government agencies and the private sector. While the National Cyber and Encryption Agency (BSSN) plays a vital role in coordinating cybersecurity policies, there are still areas where improved collaboration between different sectors could lead to more efficient responses to cyber threats. For instance, ransomware attacks targeting critical systems, such as banking and government institutions, are sometimes only identified after significant damage has occurred, rather than at earlier stages of detection and mitigation. This highlights the importance of enhancing monitoring mechanisms and ensuring a more timely response to potential cyber threats.

Countries with more advanced cyber defence systems generally benefit from well-coordinated structures, integrating various agencies within a unified framework to address cyber threats directly. Nations like the United States have implemented a

whole-of-government approach that links agencies like CISA (Cybersecurity and Infrastructure Security Agency) with the private sector for seamless communication. Indonesia has made efforts to strengthen BSSN, but challenges persist, particularly in bridging the communication gaps between the private and public sectors. Improved communication and information sharing between these sectors can help bridge gaps in preparedness and response to cyber threats, ensuring a more cohesive and efficient approach to tackling potential vulnerabilities.

The private sector, particularly technology companies and the banking sector, plays an essential role in securing digital infrastructure. However, these sectors face challenges in implementing comprehensive and effective security policies. Many organisations, despite managing valuable data and systems, may not fully recognise the extent of existing cyber threats or the urgency of securing their systems in a holistic manner. This challenge can be further influenced by reliance on external technology vendors, whose security solutions might not always align perfectly with national frameworks.

Additionally, some companies, especially those outside major tech sectors, may have limited resources to develop advanced cybersecurity systems or to provide extensive internal training for staff on handling cyber threats. Companies affected by ransomware attacks often face difficulties due to insufficient protection and recovery processes.

To improve coordination between government agencies and the private sector, this study suggests establishing a more integrated mechanism, with enhanced information-sharing systems between the public and private sectors. The government could introduce policies that encourage transparency and collaboration, establishing security standards that all critical digital infrastructure stakeholders must follow. Furthermore, the private sector could be supported in increasing investments in security technologies and training, as well as strengthening their internal cybersecurity measures, particularly regarding data protection and risk management.

BSSN can play a key role in facilitating this collaboration by providing regular training and ensuring that all sectors involved have a shared understanding of the threats and the necessary responses. Partnering with higher education institutions to cultivate more cybersecurity experts and develop more secure infrastructure would be essential in addressing these threats in a comprehensive manner.

Moreover, more adaptive policies need to be developed to ensure that responses to cyber threats can be faster and more efficient. Updates to existing cybersecurity regulations, such as the Electronic Information and Transactions Law (ITE Law), should include stricter personal data protection, increased transparency in data management, and incentives for the private sector to adopt stronger security technologies. These measures will strengthen national cyber resilience and raise awareness across all sectors regarding the importance of mitigating cyber risks.

Recent updates in cyber policy have highlighted the importance of collaboration and integration between public and private entities to create a more effective cyber defence system. As seen in countries with advanced cyber frameworks, a unified response to cyber threats allows for quicker mitigation, which is essential as Indonesia continues to face an evolving threat landscape.

Based on these findings, emphasises the need for a cultural shift in the private sector to adopt stricter security policies, alongside introducing more significant investments in relevant technologies and training. If these sectors can overcome their internal challenges and implement effective security policies, the threats to Indonesia's digital infrastructure can be significantly reduced, enabling a more resilient digital ecosystem.

In addition to challenges in inter-agency coordination, this study also highlights that the shortage of skilled human resources in the field of cybersecurity is a major obstacle in strengthening Indonesia's cyber defence. While efforts are underway, there is still a gap in the availability of trained experts who can identify, prevent, and respond to increasingly complex cyberattacks. For instance, many companies and government institutions do not have enough internal staff adequately trained to face rapidly evolving digital threats. This can impact the overall of resilience in responding to attacks targeting sensitive data or critical systems.

As a solution, this study proposes enhancing cybersecurity training through collaboration between the government, the private sector, and higher education institutions. The establishment of a national training centre capable of producing competent and ready-to-deploy cybersecurity professionals is urgently needed. Additionally, government institutions should be more proactive in implementing certification programmes to improve the competency of HR in this field.

Indonesia has adopted several relevant policies, such as Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and Government Regulation No. 71 of 2019 on Electronic Systems and Transactions. However, despite these

foundational policies, this study finds that the regulations are still inadequate in addressing increasingly sophisticated cyber threats. Many attacks exploit weaknesses not covered by the existing policies, such as ransomware-based attacks and attacks on critical infrastructure that go undetected by current defence systems.

As a recommendation, updating the ITE Law to include stricter personal data protection measures and to mandate the private sector to improve data and infrastructure security. More dynamic and adaptive regulatory adjustments are necessary for Indonesia to respond more effectively to cyber threats.

International cooperation is a critical component in addressing global cyber threats. Although Indonesia has joined several international forums on cybersecurity, stronger collaboration with developed countries in this field is still highly needed. Countries such as the United States and European nations possess more advanced experience and technology in cyber defence, so international cooperation in information exchange and technology development would be highly beneficial for Indonesia.

As a recommendation, Indonesia should increase its participation in international organisations discussing cybersecurity and strengthen information and technology exchanges with more advanced nations in this domain. There are several strategic actions to strengthen Indonesia's cyber defence:

1. Enhancing Coordination and Collaboration Among Agencies, by establishing a more integrated body or committee between the government, private sector, and educational institutions to ensure Indonesia's cyber defence is more solid.
2. Enhancing HR capacity by conducting more intensive training and certification programmes for government employees, the private sector, and students to prepare them for cyber threats.
3. Updating cybersecurity regulations by revising the ITE Law and other regulations to include more detailed provisions on personal data protection and critical systems.
4. International cooperation by intensifying cooperation with countries more advanced in cybersecurity and participating more actively in international forums addressing cyber threats.

4. Conclusion

The conclusions of this study are as follows:

- a. This study highlights the critical importance of understanding and adapting to the evolving nature of cyber warfare in Indonesia's national defence strategy. Indonesia has made significant strides in addressing cyber threats through initiatives such as the establishment the Indonesian Cyber Force (ICF). The comparison of cyber warfare with traditional physical warfare underscores the unique challenges posed by cyber threats, which involve different actors, strategies, and impacts. The study stresses the need for a more holistic approach to cybersecurity, incorporating both technical measures and broader societal awareness. Strengthening international cooperation, increasing public-private collaboration, and adopting innovative solutions like a Cyber Resilience Index (CRI) can help Indonesia improve its preparedness and response to future cyber threats. By addressing these challenges and adopting comprehensive strategies, Indonesia can build a more secure and resilient digital environment in the face of evolving cyber warfare.
- b. To strengthen Indonesia's cyber defence, updates to its cybersecurity policies are necessary, incorporating several strategic solutions that can be implemented. Some solutions that should be considered include enhancing the capacity of human resources in cybersecurity, strengthening more secure information technology infrastructure, and updating regulations to accommodate changes in cyberattack trends. Additionally, closer international cooperation is needed to address increasingly global and cross-border cyber threats. Countries with more experience in cybersecurity, such as the United States and European nations, can serve as strategic partners for Indonesia in strengthening its cyber resilience. The development of research and education in cybersecurity in Indonesia is crucial to creating a generation ready to face future cyber challenges. Indonesia must strengthen training programmes focused on digital security and increase collaboration between the government, private sector, and universities in addressing increasingly complex threats. Formulating more adaptive policies in response to technological developments and emerging threats should be a top priority in strengthening Indonesia's cyber defence.

References

Regulation

- BSSN. (2025). *Indonesian Cyber Security Strategy*.
BSSN. (2025). *Collaboration is the key to Indonesia cyber resilience*.
BSSN. (2024). *Peraturan BSSN Nomor 4 Tahun 2023 tentang Perubahan atas Peraturan BSSN Nomor 6 Tahun 2021*.
BSSN. (2024). *Peraturan BSSN Nomor 8 Tahun 2024 tentang Audit Keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE)*.
Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law)
Presidential Regulation No. 95 of 2018 on Electronic-Based Government Systems

Books and Journal

- Chertoff, M. E. (2017). *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Oxford University Press.
CYFIRMA. (2025). *Executive Threat Landscape Report Indonesia*.
Hogan Lovells. (2024). *Highlight: Amendment of Indonesia's Electronic Information and Transactions Law*.
IndoSec Summit. (2025). *The Escalating Cyber Threat in Indonesia: A Wake-Up Call for Digital Security*.
International Comparative Legal Guides. (2024). *Cybersecurity Laws and Regulations Report 2025 Indonesia*.
Kaspersky. (2021). *Global Cybersecurity Index*. Kaspersky Lab.
Libicki, M. C. (2009). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
Makarim & Taira S. (2024). *Second Amendment to Indonesia's ITE Law: What's Changed*.
Mazzucato, M. (2020). *The Value of Everything: Making and Taking in the Global Economy*. Penguin Press.
Moore, J. (2019). *Building Cyber Resilience: Strategy and Action for a Secure Future*. Wiley.
National Cybersecurity Connect 2025. (2025). *Strategic Platform for Cybersecurity Collaboration*.
Renda, A. (2018). *Cybersecurity in Europe: Policy and Regulatory Framework*. Springer.
Reuters. (2024). *Cyber attack compromised Indonesia data centre, ransom sought*.
Rid, T. (2013). *Cyber War Will Not Take Place*. Oxford University Press.
Sari, I., & Suryanto, E. (2021). Analisis kelemahan struktur pertahanan siber Indonesia. *Jurnal Teknologi dan Keamanan Informasi*, 4(2), 120-135.
The White House. (2018). *Cybersecurity National Action Plan*.