WHAT ARE INFORMATION WARFARE AND ITS SIGNIFICANCE FOR INDONESIAN DEFENSE AND SECURITY?

Bagus Jatmiko
Candidate for Information Science in the Naval Postgraduate School
Gusmiko4701@gmail.com

ABSTRACT

In the modern era, information has become a powerful tool for political and military gain, and the use of information as a weapon presents significant challenges to Indonesia's national security. This article explores the concept of information warfare and its implications for Indonesia's defense and security. By providing a comprehensive overview of information warfare, this article highlights the importance of understanding this phenomenon in order to develop effective strategies for mitigating its impact. Additionally, the article examines the specific challenges and opportunities that information warfare presents for Indonesia and offers recommendations for addressing this growing threat. Ultimately, this article aims to raise awareness of the significance of information warfare and how Indonesia can safeguard its defense and security in an increasingly interconnected world.

Keywords: *Information warfare, Indonesia's defense, and security, national and regional strategic environment.*

As we navigate through an era of unparalleled technological advancement, the threat of information warfare looms more prominent than ever before. The use of information as a weapon has become a powerful tool for political and military gain, and the impact of these attacks can be devastating. In Southeast Asia, Indonesia stands at the forefront of this rapidly evolving strategic environment, and the stakes have never been higher. To protect ourselves and our region from the dangers of information warfare, we must first understand what it is and how it works. Only then can we begin to develop effective strategies to mitigate its effects. In this article, we will delve into the world of information warfare and explore its significance for Indonesia and Southeast Asia. Let us take a closer look at this urgent issue and the steps we can take to safeguard ourselves from this growing threat.

A. INTRODUCTION

1. Definition of Information Warfare

Looking for definitions of information warfare (IW) in many publications, the author comes up with several findings from open-access publications referred to as seminal work on IW. The first one comes from the US congressional report. While there is no formal definition of information warfare (IW) by the US government, those who practice it generally view it as a means of leveraging information to gain a competitive edge with offensive and defensive capabilities. In this context, strategy refers to the planning process for achieving national objectives, with operations bridging the gap between strategic goals and tactics. In the case of IW, this link is represented by information operations (IO). (Congressional Research Service, 2022).

The second definition comes from (Lewis, 2022), which defines Information warfare (IW) as a concept of utilization and control of information and communication technology (ICT) to achieve a competitive edge against an adversary. This definition encompasses a range of tactics, including gathering intelligence, ensuring the accuracy of one's information, disseminating propaganda or false information to weaken the enemy and influence public opinion, degrading the quality of the opposing force's information, and preventing the enemy from acquiring information. In addition, (Burns, 1999) defines information warfare as *a class of techniques, including collection, transport, protection, denial, disturbance, and degradation of information, by which one maintains an advantage over one's adversaries.* The third definition comes from Borden (1999), which defines IW as "any action to Deny, Exploit, Corrupt or Destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our own military information functions. In addition to that, the fourth definition by Dahm (2021), written in USNI proceedings, states that IW is the offensive and defensive actions in physical and virtual space that enable and protect the friendly force's ability to access, process, and communicate information that also deny, exploit, corrupt or destroy an adversary force's ability to use information.

However, Libicki (1995) contends that there is no single, discrete technique known as information warfare; instead, there are various distinct types of information warfare, each claiming to fall under the broader concept. According to Libicki, there are seven distinct forms of information warfare, namely command-and-control warfare, intelligence-based warfare, electronic warfare, psychological warfare, hacker warfare (which involves attacking the enemy's computer systems), economic information warfare (which pertains to controlling information to achieve economic dominance), and cyber warfare.

The elaborations on information warfare presented in the sources offer a comprehensive understanding of the concept and its various forms. Drawing from these insights, this article presents a compelling definition of information warfare. Specifically, the author defines information warfare as the strategic use of information and communication technologies (ICTs) to achieve desired outcomes. This involves collecting, analyzing, disseminating, and manipulating information to shape individuals, organizations, or governments' opinions, perceptions, and decisions. Information warfare can take multiple forms, including disinformation campaigns, cyberattacks, propaganda, psychological operations, and media manipulation. Its potential uses are wide-ranging, from gaining political advantage to destabilizing an adversary or protecting one's interests. Through this definition, it is evident that information warfare plays a crucial role in contemporary security and strategic environments, making it an essential topic for policymakers, defense strategists, and security experts alike.

2. Importance of Information Warfare for Indonesia's Defense and Security

Given the current dynamic and uncertain strategic environment, Indonesia, as a leading country in the region, must prioritize the development of a robust Information Warfare (IW) capability to enhance its defense and security. Indonesia's strategic location in the region makes it vulnerable to a wide range of security threats, such as terrorism, piracy, territorial disputes, and cyberattacks. Thus, having an advanced IW capability is essential for Indonesia to mitigate these threats. However, there is a challenge in balancing traditional military capabilities with modern technologies to respond to growing trends toward cyberattacks and information operations. With the proliferation of social media platforms and digital communication, hostile actors can quickly spread disinformation and propaganda, which can be used to manipulate public opinion and undermine Indonesia's national security interests. Therefore, a robust IW capability is needed to detect and counter these threats. In addition, Indonesia's strategic location in the region makes it a crucial player in its security dynamics. By developing a strong IW capability, Indonesia can actively shape the region's security environment and promote regional stability and security. Having a strong IW capability is crucial, and Indonesia must invest in developing its capability to defend against emerging threats and actively promote regional stability and security.

Furthermore, Indonesia's rapidly developing economy and growing geopolitical influence mean it has become a prime target for foreign intelligence services seeking access to valuable information. Such information could include classified military documents, sensitive economic data, or critical infrastructure plans. A lack of effective IW capabilities would leave Indonesia vulnerable to these types of threats, potentially undermining the country's national security and economic interests.

Moreover, Indonesia has had several high-profile cyberattacks in recent years, including attacks on government institutions, financial institutions, and critical infrastructure. These incidents highlight the urgent need for Indonesia to develop a comprehensive and advanced IW capability to detect and respond to cyber threats effectively.

In addition, Indonesia's location as an archipelago nation means it has a complex security environment requiring a unique approach to IW. Indonesia's IW strategy should consider its maritime borders and the challenges of securing its extensive coastline against piracy and smuggling. This requires the development of advanced IW capabilities for monitoring and protecting Indonesia's maritime domain.

Indonesia's strategic environment requires a comprehensive and advanced IW capability to ensure the country's defense and security. Indonesia's location, growing economic influence, and complex security environment make it vulnerable to various security threats, including cyberattacks, disinformation campaigns, and traditional military threats. By investing in a robust IW capability, Indonesia can better safeguard its citizens, defend its national interests, and play a more active role in shaping the region's security environment.

B. UNDERSTANDING INFORMATION WARFARE

1. The Nature of Information Warfare

Information warfare (IW) is a rapidly evolving field of growing interest for defense planners and policymakers. It represents a strategy for using and managing information to pursue a competitive advantage, including offensive and defensive operations (Congressional Research Service, 2022). One can find that the nature of information warfare is complex and dynamic. It involves using information and communication technologies to achieve strategic objectives, including influencing individuals, organizations, or governments' opinions, perceptions, and decisions. It can be used for offensive and defensive purposes, such as gaining political advantage, destabilizing an adversary, or protecting one's interests.

The use of information warfare is often covert and can be challenging to detect, making it a potent tool for those who possess the capability to use it effectively. As technology continues to evolve, the nature of information warfare is likely to become even more complex, making it essential for nations to stay ahead of emerging threats in this domain.

2. Types of Information Warfare

a. Cyber-Attacks

In the context of information warfare, cyber-attacks can be used to support conventional warfare efforts by sabotaging government computer systems. Such attacks can block official government communications, contaminate digital systems, enable the theft of vital intelligence, and threaten national security (Imperva, 2023). There are several types of cyber-attacks that can be used in information warfare. These include espionage, sabotage, denial-of-service (DoS) attacks, electrical power grid attacks, propaganda attacks, economic disruption, and surprise attacks. Furthermore, Politi & Boudreaux (2022) define cyber attacks more widely as involving the actions of a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

The goal of a cyber-attack is typically to steal sensitive information, cause damage to systems, disrupt services, or gain unauthorized access to networks or devices. Individuals can launch cyber-attacks, criminal organizations, nation-states, or other entities, and they can have severe consequences for individuals, businesses, and governments. As our society increasingly relies on technology, the risk and impact of cyber-attacks continue to grow.

b. Propaganda and Disinformation Campaign

Propaganda and disinformation campaigns are a common form of information warfare that seeks to manipulate public opinion, sow confusion, and undermine the credibility of the targeted government or institution. Propaganda can be defined as the use of information to influence public opinion, often through biased or misleading information designed to shape people's perceptions and beliefs. Disinformation is a

specific type of propaganda involving the spread of intentionally false or misleading information, often intending to cause harm or disrupt social order.

In the context of information warfare, propaganda and disinformation campaigns are often used as part of a broader strategy to achieve strategic objectives. These tactics may be used to create confusion, demoralize the enemy, or shape the political and social landscape of a targeted country or region. Propaganda and disinformation campaigns can take many forms, including social media posts, fake news stories, manipulated images and videos, and the use of bots and automated accounts to amplify messages.

According to Arquilla and Ronfeldt (1996), propaganda and disinformation are among the most potent weapons in the information warfare arsenal. They can be used to demoralize an enemy, damage their reputation, and undermine their legitimacy. In addition, propaganda and disinformation can be used to influence the decision-making of a targeted audience, such as voters, policymakers, or military commanders.

It is important to note that propaganda and disinformation are not limited to state actors. Non-state actors, such as terrorist groups and criminal organizations, have also been known to use these tactics to achieve their goals. Therefore, it is critical for governments and other organizations to have the ability to detect and counter propaganda and disinformation campaigns as part of their broader information warfare strategy.

Overall, propaganda and disinformation campaigns are significant in information warfare and can have far-reaching consequences for individuals, organizations, and nations. As such, it is essential for governments and other actors to be aware of the nature and tactics of these campaigns and can respond effectively.

c. Social Media Manipulation

Social media manipulation refers to using social media platforms to spread false or misleading information to manipulate public opinion or behavior. Social media manipulation can take many forms, including using bots, fake accounts, and paid influencers to amplify certain messages or drown out opposing viewpoints.

Research has shown that social media manipulation can significantly impact public opinion and decision-making. For example, a study by the University of Oxford found

that social media manipulation was used in at least 70 countries to spread false information and propaganda during elections and other political events (Woolley & Howard, 2016)

Social media manipulation can also have severe consequences for national security. For example, during the 2016 U.S. presidential election, Russian operatives used social media manipulation to sow division and influence the outcome of the election (Mueller III, 2019)

To combat social media manipulation, a robust information warfare capability must be needed to detect and counter false information and propaganda. This can include developing advanced algorithms to detect fake accounts and bots and training individuals to be more discerning consumers of information.

C. IMPLICATIONS OF INFORMATION WARFARE FOR INDONESIA

1. Challenges of Information Warfare for Indonesian Defense and Security

Threats from cyber warfare that could interfere with Indonesia's national interests are information warfare issues for Indonesian defense and security. In order to combat this threat in this technological age, efforts must be made to establish cyber defense units (Candra et al., 2021). An effective strategy needed to be carried out by the Government of Indonesia. The National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*, BSSN) is the leading sector in handling national cyber problems. However, there are still several obstacles, such as the unreadiness of regulation, quality, and quantity of human resources and technology infrastructure owned by Indonesia in dealing with any threats that can occur at any time (Inkiriwang, 2021).

The challenges faced in Indonesia regarding cybersecurity and cyber resilience can be divided into three main pillars: regulation, technology, and human capital (Loviana & Karim, 2022). From the regulation point of view, no single law still regulates cybersecurity in Indonesia. The draft bill for cybersecurity and cyber resilience, *"Rancangan Undang-Undang Keamanan dan Ketahanan Siber,*" was canceled due to protests towards its burdening conditions for business entities (Anjani, 2021). Hence, to this day, the issue still moves under a few 'umbrella' regulations regarding cyberspace, such as Law No. 19 /2016 on Electronic Information and Transaction, Law No. 36 / 1999 on Telecommunication, and Ministry of ICT

Regulation No. 5 / 2017 on Internet Protocol-Based Telecommunication Network Security (Shafira, 2021).

From a technical point of view, Indonesia has yet to have any patents on information technology products (Loviana & Karim, 2022). The dependency of Indonesia on foreign technology is worrisome to some degree, and the security of our national big data is not within our national capabilities to control it. This is where the concept of digital sovereignty emerged. This concept refers to a nation's ability to control its own digital infrastructure, data, and technology. It is an important issue because it touches everyone, even those who do not have a mobile phone or have never used an online service. The fight for digital sovereignty is an epochal struggle as the preoccupation of many nations, with variable alliances changing according to interests and opportunities. The most visible clash is between companies and states, which is asymmetric (Floridi, 2020). This concept is an interesting concept that worthy of elaborate discussion for itself.

Nevertheless, this disadvantage leaves Indonesia susceptible to any digital threats, especially when the level of digital awareness and security is very low in the country, with 86% of developers not viewing application security as a priority (Warrior, 2022). This phenomenon goes in the government itself. The development of the Electronic-Based Government System (*Sistem Pemerintahan Berbasis Elektronik* - SPBE) that is supposed to be the pinnacle of government digital administration transformation is, in fact, not seen as sustainable, overlapping with each other and contradicts the primary purpose of their development, that is to ease the previously complicated bureaucracy system (Loviana & Karim, 2022). This further puts Indonesia's information security and cyber resilience in peril that should get the utmost attention from the government. These flaws in Indonesia's cybersecurity and resilience urgently need to be resolved, which leads to the next and most crucial pillar: human capital.

Human capital is the most crucial factor in enhancing and bolstering Indonesia's cyber resilience and information security. Individuals frequently report data breaches and the illegal sharing of personal information. However, most of these "data breaches" are not actually "breaches" because people unknowingly post their personal information online in a dangerous manner. This example is one among many of the poor levels of understanding of security in using technology. People, including authorities, frequently adopt modern technological innovations without first learning about them because of a fear of missing out

(FOMO). Everyone in Indonesia must therefore receive education and socialization for awareness-building cybersecurity in order to keep up with the country's rapid technological development. Integrity is frequently omitted from the CIA (Confidentiality, Integrity, Availability) triad. Since data is the new oil that people are willing to pay a premium for, most examples of data breaches tend to involve internal factors (Sutcliffe, 2017). Other times, these incidents are inadvertent, emphasizing the need for everyone to understand cybersecurity and enhance work ethics and SOPs to stop internal cyberattacks.

2. Opportunities of Information Warfare for Indonesia

Despite the difficulties, the scenario offers Indonesia the opportunity to increase its cybersecurity and cyber resilience. To begin with, people are becoming more conscious of the problem. In the government domain, Peraturan Presiden No. 28 Tahun 2021 regarding BSSN Reorganization offers optimism for improving cybersecurity by giving BSSN room to operate more successfully, effectively, and precisely (Presidential Regulation, 2021). Besides that, the private sector is beginning to prioritize security with the government or international organizations' support, such as Kemkominfo and Google (Loviana & Karim, 2022). This should also be a momentum for the defense and security stakeholders encompassing the Defense Ministry, the Armed Forces, the National Police, and other agencies with BSSN as the leading sector to incorporate the IW capability within their strategic planning. In this digitally-connected world, IW capability seems inevitable to be owned for reasons elaborated above.

On the regulation side, Indonesia has not yet been equipped with sufficient regulations to tackle several crucial information security issues, such as personal data protection and the protection of national big data, under the scrutiny of national agencies such as BSSN. Moreover, the regulations to protect information infrastructure are still under drafting, which is vital in ensuring that the government maintains the security of vital infrastructure in times of crisis. Based on Article 99 of Government Regulation number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, it is stated that eight sectors fall into strategic categories, including government administration, energy and mineral resources, transportation, finance, health, food, information technology and telecommunications, and defense (Salmawan, 2021). The failure to protect any of these strategic sectors may lead to national crises.

Taking the lessons from the world-class tech giants and their struggle to strengthen their information security and cyber resilience, such as Google and Microsoft in the US with Google and Huawei in China, Indonesia should also be aware of technology's critical role in cybersecurity resilience capacity building. Taking technological development seriously would be the first step to enhancing our national capabilities in building IW capacity, information security, and cyber resilience toward digital sovereignty. Focusing on strengthening the regulations and mastering the technologies, besides empowering the human resources to support the IW capabilities and cyber security, are the right thing to do. Nevertheless, developing and implementing good data governance is a prerequisite to having robust information, digital security, and sovereignty. At the lower level, similar steps should be taken by the defense and security domain, particularly the defense ministry and the armed forces, in managing their big data before building the IW capabilities for tackling any cyber attack and security challenges.

D. STRATEGIES FOR ADDRESSING INFORMATION WARFARE IN INDONESIA

1. Enhancing Cybersecurity Measures

Enhancing cybersecurity measures as part of national information awareness and security requires a multifaceted approach that includes regulatory reforms, technological advancements, workforce development, and public awareness efforts. With the implementation of these measures, Indonesia can develop a robust cybersecurity infrastructure capable of withstanding the growing threats of cyber-attacks.

a. **Strengthen the Regulatory Framework**: The government of Indonesia should create a comprehensive legal framework that can provide a solid foundation for cybersecurity regulations. According to Loviana and Karim (2022), Indonesia needs to establish clear regulations that prioritize cybersecurity to help counteract the growing number of cyber threats. The legal framework should cover all aspects of cybersecurity, including data protection, privacy, and cybercrime.

b. **Improve the Technological Infrastructure**: To enhance cybersecurity measures in Indonesia, the country needs to improve its technological infrastructure. Loviana and Karim (2022) suggest that Indonesia needs to develop an indigenous technological capability to counteract cyber threats. This requires investment in research and development to create

effective cybersecurity solutions. Additionally, the country must adopt cutting-edge cybersecurity technologies that can help protect its digital assets.

c. **Develop a Skilled Workforce**: Indonesia needs to develop a skilled workforce that can respond to cyber threats that require training programs for cybersecurity professionals, including law enforcement officials and IT professionals. One way is to create a talent pool through programs such as the Gladiator Cybersecurity Indonesia program, which aims to increase cybersecurity skills among ten thousand candidates1. Another way is to provide technical guidance for information security for government bodies (Shafira, 2021).

d. **Raise Public Awareness**: Indonesia should invest in public awareness programs to help citizens understand cybersecurity's importance. Education and socialization efforts can help individuals, businesses, and government agencies recognize potential cyber threats and take appropriate measures to protect themselves. According to Sutcliffe (2017), raising public awareness is essential in building a culture of cybersecurity where all individuals are responsible for protecting themselves and their digital assets.

In the defense and security domain, similar steps at the lower level can be taken based on the assessment of strategic planning and the requirement to build a national IW capability.

2. Developing Policies to Address the Information Warfare capabilities

In developing policies that address the necessity to build national IW capabilities, taking a multi-stakeholder approach involving the government, private sector, civil society, and academic institutions is essential. The following are some ways to develop policies to address the necessity of IW capabilities:

a. **Comprehensive Cybersecurity and Information Warfare Strategy**: Indonesia needs a comprehensive cybersecurity and information warfare strategy considering the three pillars of cybersecurity challenges: regulation, technology, and human capital. The strategy should be developed in collaboration with key stakeholders and cover all critical sectors, including government, financial institutions, healthcare, and energy.

b. **Legal and Regulatory Framework**: Indonesia needs to develop a legal and regulatory framework that addresses using the information as a weapon. The framework should clearly define what constitutes information warfare and outline the legal consequences for those who

engage in such activities. Moreover, there needs to be a law that regulates cybersecurity in Indonesia that covers all critical infrastructure.

c. **Cyber Defense Forces**: Efforts to create cyber defense forces are essential in dealing with cyber threats in this technological age. The National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*, BSSN) is the leading sector in handling national cyber problems. However, Indonesia must invest more in cybersecurity research and development to improve its cyber defense capabilities.

d. **Capacity Building**: Indonesia must invest in capacity building for its cybersecurity professionals and the wider public. The government should create programs to raise awareness about cybersecurity and information warfare and provide training for professionals to enhance their skills and knowledge.

e. **International Cooperation**: Indonesia should work with other countries to address the necessity of developing IW capabilities. International cooperation could include information sharing, IW joint training exercises, and IW cooperation on research and development.

Overall, developing policies with multifaceted approaches and stakeholders is critical for protecting national security, maintaining economic stability, and protecting the privacy and safety of citizens. Moreover, developing effective policies informed by research, stakeholder feedback, and international best practices is essential.

3. Strengthening Strategic Partnerships with other Countries

Following the last point in the previous section regarding international cooperation, Indonesia recognizes the importance of international cooperation in developing Information Warfare (IW) capabilities. Strengthening strategic partnerships with other countries is crucial for Indonesia's defense and security. To achieve this goal, there are several ways in which Indonesia can enhance its cooperation with other countries in the field of IW.

One approach is establishing joint training and education programs with other countries to exchange knowledge and experience in IW. These programs can provide opportunities for Indonesian military and civilian personnel to learn from their foreign counterparts and vice versa. This also may involve the civilian counterpart as it may feel more neutral than all military cooperation, which may draw an unnecessary response from certain parties.

Another way to strengthen strategic partnerships is by establishing information-sharing agreements with other countries. Sharing information on cyber threats, vulnerabilities, and attacks can help to build a better understanding of the IW landscape and improve the ability to respond to emerging threats. Such agreements can also facilitate joint investigation and prosecution of cybercriminals. The agreement is the General Security of Military Information Agreement (GSOMIA) and a Communications Interoperability and Security Memorandum of Agreement (CISMOA). These foundational agreements establish the framework for enhanced partnership, information sharing, and defense cooperation between the United States and Indonesia (US Department of State, 2023). Furthermore, this agreement can be the umbrella for further cooperation to increase Indonesia's IW and cybersecurity capabilities.

Lastly, Indonesia can also engage in joint research and development (R&D) projects with other countries to develop new IW technologies and solutions. Collaborative R&D can accelerate innovation and help address complex IW challenges. Overall, strengthening strategic partnerships with other countries is essential for Indonesia to enhance its IW capabilities with all viable approaches to help Indonesia achieve this goal.

E. CONCLUSION

1. Recap of the Significance of Information Warfare for Indonesia's Defense and Security

Information warfare strategically uses information and communication technologies (ICTs) to achieve desired outcomes. This involves collecting, analyzing, disseminating, and manipulating information to shape individuals, organizations, or governments' opinions, perceptions, and decisions. Information warfare can take multiple forms, including disinformation campaigns, cyberattacks, propaganda, psychological operations, and media manipulation. Nation-states, non-state actors, and private sector entities can all be involved in information warfare. To combat information warfare, individuals should be vigilant and critical when consuming information, organizations should invest in cybersecurity and train their employees, and governments should invest in cybersecurity and intelligence capabilities, work with technology companies, and promote media literacy. By working together, we can better prepare ourselves to defend against information warfare threats and protect our democracies and societies from manipulation and destabilization.

For Indonesia, the relevance of having IW capabilities grows even more potent every day with the world that has become more interconnected. The significance of information warfare for Indonesia's defense and security lies in its potential to threaten Indonesia's national interests. Cyber warfare is a significant challenge in the technological age, and efforts to create cyber defense forces are essential to deal with this threat. To this moment, Indonesia still faces several obstacles, such as the unreadiness of regulation, quality, and quantity of human resources, and technology infrastructure owned by Indonesia. To enhance cybersecurity measures, Indonesia needs to develop policies to address the use of information as a weapon, strengthen strategic partnerships with other countries in developing IW capabilities, and invest in human capital development. These efforts are crucial to ensure that Indonesia can protect its national interests and maintain its sovereignty in the face of information warfare threats.

2. Call to Action for Addressing the Threat of Information Warfare in Indonesia.

The increasing threat of information warfare in Indonesia poses a significant challenge to its defense and security. It is imperative for the Indonesian government to take immediate action to address this threat. This call to action involves developing a comprehensive national strategy that includes strengthening cyber defense forces, improving the quality and quantity of human resources, upgrading the technological infrastructure, and establishing regulations to govern the use of information in the country. Additionally, the government should focus on raising public awareness of the dangers of information warfare and investing in education and training to equip the population with the necessary skills and knowledge to combat the threat.

The Indonesian Armed Forces (TNI) also play a critical role in addressing the threat of information warfare. By strengthening its IW defenses, Indonesia can safeguard its national interests and maintain regional stability and security. The military should prioritize the development of IW capabilities by investing in training, technology, and infrastructure. Additionally, the military should work closely with other government agencies, such as the National Cyber and Crypto Agency, to coordinate efforts and share information. Collaboration with other countries can also be beneficial in enhancing Indonesia's IW capabilities.

REFERENCES

Anjani, N. H. (2021). *Perlindungan Keamanan Siber di Indonesia* (0 ed.). Center for Indonesian Policy Studies. https://doi.org/10.35497/341780

Arquilla, J., & Ronfeldt, D. F. (1996). *The advent of netwar*. RAND.

Borden, C. A. (1999). What is Information Warfare? *Aerospace Power Chronicles*.

Burns, M. (1999). *Information warfare: What and how?* https://www.cs.cmu.edu/~burnsm/InfoWarfare.html

Candra, A., Suhardi, S., & Persadha, P. (2021). INDONESIA FACING THE THREAT OF CYBER WARFARE: A STRATEGY ANALYSIS. *Jurnal Pertahanan: Media Informasi Ttg Kajian & Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism & Integrity*, *7*, 441. https://doi.org/10.33172/jp.v7i3.1424

Congressional Research Service. (2022). *Defense primer: Information operations* (p. 3) [Congress]. US Congress. https://crsreports.congress.gov/product/pdf/IF/IF10771

Dahm, M. (2021, March 18). *The Reality of War Should Define Information Warfare*. U.S. Naval Institute. https://www.usni.org/magazines/proceedings/2021/march/reality-war-should-define-information-warfare

Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, *33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Imperva. (2023). What is Cyber Warfare | Types, Examples & Mitigation | Imperva. *Learning Center*. https://www.imperva.com/learn/application-security/cyber-warfare/

Inkiriwang, F. W. (2021, May 8). Recalibrating Indonesia's Defense Diplomacy for the New Normal. *The National Bureau of Asian Research (NBR)*. https://www.nbr.org/publication/recalibrating-indonesias-defense-diplomacy-for-the-new-normal/

Lewis, B. C. (2022). *Information warfare*. Information Warfare. https://irp.fas.org/eprint/snyder/infowarfare.htm

Libicki, martin C. (1995). *What is Information Warfare?* The Center for Advanced Concepts and Technology (ACT) National Defense University. https://apps.dtic.mil/sti/pdfs/ADA367662.pdf

Loviana, K., & Karim, M. P. (2022, May 10). *Cybersecurity and Cyber Resilience in Indonesia: Challenges and Opportunities : Center for Digital Society*. https://cfds.fisipol.ugm.ac.id/2022/05/10/cybersecurity-and-cyber-resilience-in-indonesia-challenges-and-opportunities/

Mueller III, R. S. (2019). *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (p. 448).

Politi, C., & Boudreaux, B. (2022). *Cyber Warfare*. https://www.rand.org/topics/cyber-warfare.html

Presidential Regulation. (2021). *PERPRES No. 28 Tahun 2021 tentang Badan Siber dan Sandi Negara [JDIH BPK RI]*. https://peraturan.bpk.go.id/Home/Details/165493/perpres-no-28-tahun-2021

Salmawan, N. A. (2021, November 29). *Infrastruktur Informasi Vital Nasional dan Ancaman Siber*. cyberthreat.id. https://cyberthreat.id/read/12955/Infrastruktur-Informasi-Vital-Nasional-dan-Ancaman-Siber

Shafira, I. (2021, July 28). *Analyzing Indonesia's National Cybersecurity Strategy: Center for Digital Society*. https://cfds.fisipol.ugm.ac.id/2021/07/28/analyzing-indonesias-national-cybersecurity-strategy/

Sutcliffe, A. (2017, December 21). 8 Most Common Causes of Data Breach. *Sutcliffe Insurance*. https://www.sutcliffeinsurance.co.uk/news/8-most-common-causes-of-data-breach/

US Department of State. (2023). U.S. Security Cooperation With Indonesia. *United States Department of State*. https://www.state.gov/u-s-security-cooperation-with-indonesia/

Warrior, S. C. (2022, April). *Secure Code Warrior Survey Finds 86% of Developers Do Not View Application Security As a Top Priority*. Global Security Mag Online. https://www.globalsecuritymag.com/Secure-Code-Warrior-Survey-Finds,20220407,123977.html

Woolley, S. C., & Howard, P. N. (2016). *Political Communication, Computational Propaganda, and Autonomous Agents-Introduction*.