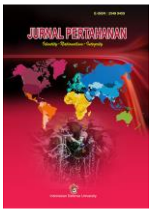
Jurnal Pertahanan

Media Informasi tentang Kajian dan Strategi Pertahanan
yang Mengedepankan *Identity*, *Nationalism* dan *Integrity*
e-ISSN: 2549-9459
http://jurnal.idu.ac.id/index.php/DefenseJournal



INDONESIA FACING THE THREAT OF CYBER WARFARE: A STRATEGY ANALYSIS

Ahmad Candra[1], Suhardi[2], Pratama Dahlian Persadha[3]
State Intelligence Academy (STIN)
Sumur Batu, Babakan Madang, Bogor, West Java 16810
ahmad.candra076@gmail.com[1], suhardi@stei.itb.ac.id[2], pratama@cissrec.org[3]

Article Info

Article history:
Received : October 10, 2021
Revised : November 30, 2021
Accepted : December 26, 2021

Keywords:
BSSN,
Cyber Security,
Cyber Warfare,
National Security,
National Threat,
Strategy

DOI:
http://dx.doi.org/10.33172/jp.v7i3.1424

Abstract

The threat of cyber warfare may disturb Indonesia's national interests. For this reason, efforts to create cyber defense forces are essential in dealing with the threat of cyberwar in this technological age. An effective strategy is needed to be carried out by the Government of Indonesia. This article analyzes the strategies implemented by the Government of Indonesia in dealing with the threat of cyber warfare. This study represents the use qualitative approach with an analytical descriptive design. The results of this study explain that the threat of cyber warfare in the future may have an impact that could shake the stability of national security. Through the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara,* BSSN) as the leading sector in handling national cyber problems, the Indonesian Government has taken strategic steps to safeguard the national interests and goals of the Indonesian nation and other state institutions stakeholders involved in the management of cyber security and defense. However, in practice, 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.

© 2021 Published by Indonesia Defense University

INTRODUCTION

The current condition of the COVID-19 pandemic requires Indonesian people to work from home to avoid direct physical contact to avoid the spread of the disease. This condition has implications to increase the need for internet connectivity and to encourage the acceleration of digital technology transformation. The acceleration of digital transformation creates an era where all forms of activity turn to digital technology, or it can be said that we are currently in the era of the Internet of Things, such as doing meetings through virtual conferences, buying and selling transactions through e-commerce applications, financial transactions, teaching and learning systems in education, as well as health services. All of these things have now switched to using digital technology systems.

Based on the latest report released by Hootsuite & We Are Social, Indonesian internet users reached 202.6 million as of

January 2021, or around 73.7% of Indonesia's population of 274.9 million people have used the internet. This number has increased by 15.5 % or more than 27 million people compared to 2020 (Riyanto, 2020). Of course, this situation will increase the threat of cyber attacks that can infiltrate these activities and even be affected in cyber warfare that causes paralysis of activities and causes huge losses for Indonesia.

The development of the use of the internet and the advancement of science and technology have a complex impact on human life and relations between countries, not only having a positive impact in providing convenience in every activity but also having a negative impact such as the emergence of the threat of cyber attacks that can trigger cyber warfare in cyberspace. The utilization of information and communication technology in cyberspace that does not recognize national borders. This can trigger activities that may harm other parties that state actors and non-state actors can carry out. Such as the theft of various information activities, attacks on information systems in various fields, namely banking, military networks, and essential national infrastructure (Smith, 2015).

Cyberwarfare is very different from conventional wars in various parts of the world involving weapons and military personnel. Cyberwarfare only uses the current technological system and attacks breaking into the opponent's information technology system to be paralyzed. Cyberwarfare is also defined as an action or attack aimed at targeting any aspect of an opposing cyber system, such as communications, logistics, or intelligence (Athanassouli, 2018). These cyber-threats have been experienced by several countries, such as in 2007, the Estonian Government was the victim of a large-scale cyberattack, which resulted in disruption of the functioning of state services (McGuinness. Damien, 2017). In addition, the Government of Georgia has also become a victim of attacks, with hacks blocking the takeoff of military aircraft and causing problems in the accessibility of official media sites, ministries, and public entities (BBC, 2019).

Unpredictable future threats require the readiness of world countries to anticipate emerging threats, including the threat of cyber warfare in cyberspace. Therefore, several countries have developed their defense and security capabilities in countering the threat of cyber attacks, like the United States, which has increased its focus on cyber warfare in 2010 by establishing the U.S. Cyber Command and receiving a sizeable budget allocation (Rofii, 2018). Moreover, several other countries such as Britain, Russia, and China have formed cyber security units in their countries to anticipate potential cyber-attacks carried out by state and non-state actors from within and outside the country.

Since the development of digital transformation has far-reaching consequences and creates cyber vulnerabilities and national security threats in cyberspace, the governments of every country as policymakers are aware of starting looking for ways to secure critical national infrastructure, including in Indonesia. Indonesia has established a National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*, BSSN), a government agency responsible for national cyber security and coordinator for all government organizations with the same role in national cyber security. Cyber security is one of the most critical instruments in today's digital era in maintaining information security and protecting information systems from cyber threats that can occur at any time. The latest data related to cybersecurity in Indonesia, the National Cybersecurity Operations Center BSSN, issued an annual report on Indonesian cybersecurity in 2020 and explained that there had been 495 million identified cyberattacks throughout 2020 (Badan Siber dan Sandi Negara, 2020). With the high number of cyberattacks in

Indonesia, this country is certainly vulnerable to becoming a victim. It may even have a significant impact in the event of a cyberwar, especially against countries that have prepared their infrastructure, human resources, and technology in the face of cyber warfare.

With digital transformation taking place, which is rapidly changing all activities of society, economy, and Government, it is crucial to increase awareness of cyber threats so that it is possible to create an environment that is relatively safe against significant disruptions such as the threat of cyber warfare in the future. Therefore, this study aims to analyze the strategies implemented by Indonesia in dealing with the threat of cyberwar and the main requirements in preparing a solid national cyber system if the threat of cyberwar occurs in Indonesia.

METHODS

This research article uses a qualitative descriptive-analytical approach to describe or describe systematically, factually, and accurately the facts and the relationship between phenomena that are facts (Arikunto, 2010). Qualitative methods are also said to be research procedures that produce descriptive data in written or spoken words from people and observed behavior and are used to examine natural objects' conditions (Moleong, 2018). Data collection techniques are carried out by triangulation, and data analysis is inductive and emphasizes meaning rather than generalization. This article uses data sources derived from literature studies related to the research study following the object and subject of this research from government institutions that manage national cyber security.

RESULT AND DISCUSSION

Cyber Warfare

Many literature reviews have defined the understanding of cyber warfare, but there is no common international understanding yet of what is cyber warfare meant. Ideas such as cyber espionage, cyber attacks, cyber warfare, and even cyber crime are often combined. The current definition that is often used is the definition put forward by experts and several international organizations.

In 2014, Singer and Friedman wrote that defining cyber warfare should not be complicated. They consider that cyber warfare is similar to war in other domains because there is always a purpose behind it, a political mode, and or an element of violence. They refer to the position of the United States government on the use of force in a cyberattack that results in significant death, injury, or destruction, without further exploring the problem definition (Singer & Friedman, 2014). There is an opinion that cyber-attacks are not the same as cyber wars. Thomas Rid thinks that it must first be clear whether cyberattacks can be characterized as acts of war. To qualify as an act of war, a cyber-attack or cyber-offensive, according to him, must meet three specific criteria, namely:

1) Must be potentially lethal;
2) Must be instrumental; and
3) It must be political.

According to Rid (2012), there has been no cyber attack that meets these three criteria, and therefore he concludes that no cyber warfare has ever occurred. However, Rid's opinion is still under scientific debate to this day. In addition to Rid's opinion, there are other views on the definition of cyber warfare and are still acceptable and relevant in this article, and these views are derived from Martin Libicki's opinion, he defines cyberattacks can be full-scale cyber warfare which is described as a deliberate attack on a network to disable it (Libicki, 2009). For simplicity, Libicki distinguishes between strategic and operational cyber warfare. Strategic cyberwarfare consists of cyberattacks launched by a single entity against a country and its people, but not exclusively to influence the behavior of the target country. Meanwhile, in his opinion, operational cyber warfare has a more limited scope and is defined as the use of computer networks to support physical military operations (Libicki, 2009).

The Threat of Cyber Warfare in Indonesia

The development of information and communication technology today in the Industrial Revolution 4.0 era and the start of Society 5.0 significantly influenced the development of information and communication technology. This influence also has an impact on shifting future war strategies, where a country no longer uses conventional war methods. or in other words, in the future, the data on the threat of war will no longer be in the form of the deployment of military forces in the form of weapons and mobilization of troops to an area. However, they will carry out attacks into the enemy's cyberinfrastructure through computer networks and the internet so that the development of information technology creates new threats that have an impact on the stability of a country's sovereignty.

The shift in future warfare strategies where the battlefield is cyberspace will make it more difficult to determine the perpetrators of cyber attacks and will not be easy to prove that an action in a cyber attack is an act by a state or can be carried out by non-state actors. Anderson said that cyber threats could also be dominated by non-state actors such as individuals or groups of hackers, non-government organizations, organized crime groups, and the private sector to threaten defense and security (Anderson, 2007).

Information and Communication Technology can be said to have become the backbone of any current situation, such as financial transactions, health services, and government communication systems. Advances in information and communication technology have led to interdependence and connectivity in cyberspace. However, today's digital transformation may have hazardous side effects such as cyberattacks that can lead to cyber-war in cyberspace that can impact all critical national infrastructure of those countries in conflict. With the rapid digital transformation that is changing all activities of people's and country's lives today, it is crucial to increase awareness of cyber threats, one of which is Indonesia, which experiences an increase in internet users every year.

The COVID-19 pandemic has had an impact on the acceleration of digital transformation in Indonesia, based on the results of the latest research released by Hootsuite and We Are Social explaining that until January 2021, the number of internet users in Indonesia reached 202.6 million, and this number increased by 15, 5 percent compared to 2020 (Anggraeni, 2021). Based on the number of internet users, Indonesia cannot escape from the various potential threats of cyber attacks today.

Cyber attacks are perpetrators attacking an object controlled by a country to carry out government activities in cyberspace. Data from the National Cyber and Crypto Agency (BSSN) revealed that there had been 290.3 million cyber attacks targeting Indonesia in 2019, and in 2020 there was a significant increase of 495.3 million identified cyberattacks (Badan Siber dan Sandi Negara, 2020). Most attacks are malware that can damage a system or steal data from the number of identified attacks. Currently, cyberattacks targeting Indonesia are dominated by malware attacks. Indonesia occupies the highest position as a country experiencing malware attacks in the Asia Pacific region in 2019 (Setyowati, 2020). Furthermore, it is predicted that the highest number of cyber attacks targeting Indonesia comes from malware attacks.

In today's digital era, when all activities have utilized technology, there are so many unlimited digital world users. However, not all accessors are good people because every security gap can be exploited for profit, from data theft to system destruction. The number of cyberattacks targeting cyberspace in Indonesia has various impacts according to the type of attack used by the attacker. Attacks in cyberspace are attack activities that take advantage of computer networks and the internet in cyberspace. The attackers use this technology to compete and dominate, interfere, stop communication, and even change the flow of information and content and various other actions that can harm and destroy other parties. Seeing the number of cases of cyber attacks in Indonesia as shown in Figure 1 which explains that every year there is always an increase, even during the pandemic, there is a drastic increase in cyber attacks targeting Indonesia, so it can be said that Indonesia is a country that often becomes a victim of cyberattacks.

In addition to the threats that have occurred and have been mentioned previously, Indonesia needs to be aware of various threats that come from cyber power that has been owned by state actors and non-state actors at this time. Cyber power is defined as using cyberspace to create profit and influence in all operational environments and across power tools (Kuehl, 2009). Collin Gray (2013) also defines cyber power as the ability to do something strategically useful in cyberspace.

Three cyber power activities need to be anticipated by Indonesia because attacker actors can do something harmful to Indonesia's cyberspace. These three wrongs doing are namely subversion, espionage, and sabotage (Rid, 2012). Rid defines sabotage as a deliberate attempt to weaken or destroy a government or military system; espionage is defined as an attempt to penetrate a hostile system to extract sensitive or protected information; and subversion is defined as a deliberate attempt to undermine the authority, integrity, and constitution of the authority (Rid, 2012).

One of the significant cases related to sabotage in cyberspace was in 2015. There was sabotage carried out by Russia against public services in Ukraine, which left around 230,000 people in the middle of winter in Ukraine without electricity for several hours (Electricity Information Sharing and Analysis Center, 2016). Espionage is also a threat that the Indonesian government needs to be aware of. One of the most prominent espionage cases is China's efforts against the United States. Namely, a case of theft of sensitive military information, including technical documentation for the F-35 Lightning II

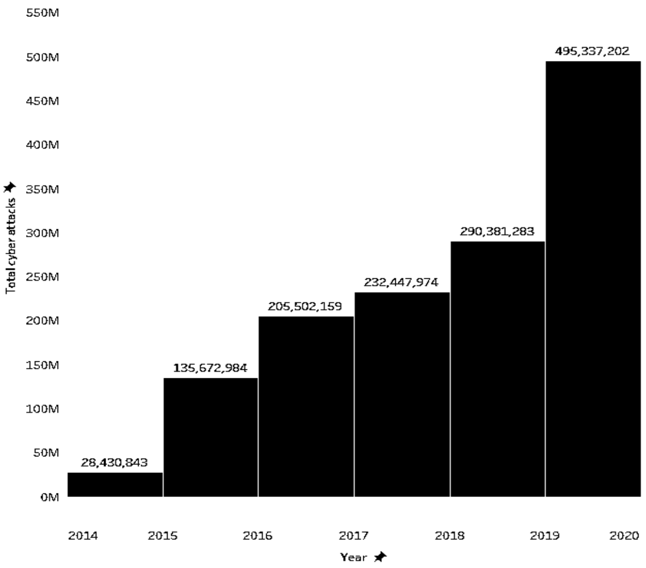


Figure 1. Number of Cyber Attacks in Indonesia in 2015-2020
Source: ID-SRTII Annual Report BSSN and reprocessed by the Authors, 2021

multirole fighter jet and the F-22 Raptor tactical fighter jet (The United States Department of Justice, 2016). Lastly, the threat from the opposing cyber power that needs to be watched out for is the power of subversion, the main characteristic of subversion activities is to target the collective political cohesion, their trust and mutual trust in general, and among the subversive means, propaganda is the most popular means (Rid, 2012). Some of the subversive activities that have shown the dangers of subversive means, such as propaganda, are riots in Libya, Egypt, and several other countries. The purpose of these subversive powers is to reduce the Government's freedom of action and influence a country's policies directly (Brown, Guskin, & Mitchell, 2012).

These attacks mainly target the installation of computer networks belonging to the government or state institutions and public services. Therefore the Indonesian Government needs to anticipate the possibility of cyberattacks that can paralyze critical national infrastructure.

Cyber Attack Cases in Indonesia

A cyber attack impacts the target of the cyber attack may feel. The impact experienced can take the form of:

1) Functional disorders;
2) Remote control of the system;
3) Misuse of information;
4) Riot, fear, violence, conflict chaos;
5) As well as other conditions that are very detrimental, it is possible to cause destruction. (Kementerian Pertahanan Republik Indonesia, 2014)

The number of cyberattacks targeting Indonesian cyberspace has various impacts according to the type of attack used by the attacker. Indonesia often experiences cyber security incidents that have a small or significant impact on national security and can even interfere with the sovereignty of the Indonesian state, as in 2013 the wiretapping scandal revealed by the Australian Intelligence Agency and the United States against high government officials in Indonesia at that time. This case impacts the national security situation because intelligence officers know state secret information through private communications of state leaders of other countries.

In addition to this case, there is also a disinformation war in cyberspace between the Indonesian Government and the OPM or *Organisasi Papua Merdeka* (Free Papua Organization). The OPM often uses propaganda methods against the Indonesian Government in cyberspace. This, of course, impacts the security situation in Papua, which can lead to conflicts that will not end if they are not handled quickly and appropriately in countering the issues issued by the OPM in cyberspace.

In addition to the large impact caused and causing conflict and threatening the country's sovereignty, there are cyber attacks that occurred in Indonesia and had a moderate impact on the Indonesian state, such as the theft of information data through malware attacks that occurred on e-commerce platforms in Indonesia, including Tokopedia, Bukalapak, Lazada, Bhinneka. Not only e-commerce platforms are often victims of information data theft, but this is also experienced by Indonesian government institutions such as the General Elections Commission (*Komisi Pemilihan Umum*, KPU). On May 22, 2020, KPU hackers claim to have broken into 2.3 million Indonesian citizens' personal data which contains their names, address, identity number, and date of birth (CNN Indonesia, 2020). In addition, there was also the hacking of the COVID-19 patient database in Indonesia. The leakage of information data is the misuse of information that can harm individuals or the Indonesian people.

Cyber attacks also have a small impact, namely frequent attacks on Government and private cyberinfrastructure, cyber-attacks such as web defacement websites owned by the Government or private parties, such as cases of hacking websites of the Ministry of Home Affairs; the House of Representatives of the Republic of Indonesia or *Dewan Perwakilan Rakyat Republik Indonesia* (DPR RI); the Indonesian Child Protection Commission or *Komisi Perlindungan Anak Indonesia* (KPAI); Meteorology, Climatology, and Geophysical Agency or *Badan Meteorologi, Klimatologi, dan Geofisika* (BMKG); Criminal Investigation Agency of the Indonesian National Police or *Badan Reserse Kriminal Kepolisian Negara Republik Indonesia* (Bareskrim Polri); and The General Election Supervisory Agency or *Badan Pengawas Pemilu* (Bawaslu) (Pusat Operasi Keamanan Siber Nasional, 2019). The hacking has an impact on the functional disruption of public services in government institutions in Indonesia.

Indonesian Government Strategy

The trend of cyberattack threats will continue to increase along with information and communication technology development. Therefore, studies are needed to overcome various cyber defense techniques, tactics, and strategies that will continue to develop. The impact of the development of the cyber world is the widespread escalation of threats in cyberspace that can threaten state sovereignty, territorial integrity, and national safety.

To carry out early anticipation related to possible cyber warfare threat situations that can occur in Indonesia, it is necessary to have a strategy be implemented by the Government of Indonesia in dealing with all threats of cyber attacks that can lead to cyber warfare involving Indonesia's cyberspace. The explanation related to the Indonesian Government's strategy uses the strategy theory initiated by B.H Liddell Hart's which defines that strategy as "the art of distributing and applying military means to fulfill policy ends" (Hart, 1967). The meaning of this understanding explains that strategy is the art of determining goals (ends), formulating ways to be taken (ways), and determining the means (means) used to achieve goals.

As one of the countries with the most significant number of internet users in Southeast Asia, Indonesia must protect the country from various threats of attacks in cyberspace. This is based on the national goal of the Indonesian people, namely protecting the entire Indonesian nation and the entire homeland of Indonesia, advancing public welfare, educating the nation's life, and participating in carrying out world order based on independence, eternal peace, and social justice. To achieve this goal, it is necessary to reduce it to the national interest as stated in Law Number 3 of 2002 concerning National Defense, which states that the national interest of the Indonesian nation is to maintain the establishment of the Unitary State of the Republic of Indonesia based on the 1945 Constitution and Pancasila and to ensure the smooth running of national development to realize a national goal.

In securing the national interest, it is necessary to have a cyber defense which is an effort to prevent and overcome cyber threats and attacks that will disrupt the implementation of national defense, and this must be a priority for all state administrators. In dealing with the threat of cyber warfare in Indonesia, some institutions are authorized to deal with these threats, namely the National Cyber and Crypto Agency (BSSN), and are the leading sector in handling cyber problems in Indonesia.

In securing cyberspace in Indonesia, BSSN must collaborate with all stakeholders in building systems and governance to implement integrated cyber security strengthening. BSSN involves four stakeholders referred to as the "Quad Helix." The Director of National Critical Information Infrastructure Protection BSSN explained that in handling cyber threats, to overcome and resolve them, BSSN involves four stakeholders called the Quad Helix (Ayu, 2021). The Quad Helix in question is a BSSN concept inviting stakeholders, including Government, business people, academics, and the community, to spread cyber security awareness to jointly realize national cyber security and national security stability (Ayu, 2021).

In improving and realizing a solid cyber security system, BSSN, through the Director of Threat Detection of BSSN, explained that the defense strategy implemented was through the development of a layered security strategy. In addition, it also develops cyber capabilities through the development of cyber intelligence, cyber defense, cybercrime, cyber diplomacy, and cyber economy in Indonesia, as well as several strengthening steps explicitly described in the BSSN Strategic Plan. (Badan Siber dan Sandi Negara, 2020), as follows:

1. Strengthening cyberinfrastructure security;
2. Development and strengthening of computer emergency response teams;
3. Prevention of cybercrime and increasing international cooperation in the cyber field;
4. Strengthening the capacity of human cybersecurity resources;
5. Settlement of cybercrime clearance rate.

Several government organizations deal with cybersecurity components, such as the BSSN, the Ministry of Communication and Information (Kominfo), the Ministry of Defense (Kemhan), the State Intelligence Agency (BIN), the Indonesian National Army, and the Indonesian National Police (Polri). Various programs related to cyber security that are prepared and implemented are still at the level of each government agency.

These various government agencies need to be synergized to fend off, ward off, and prevent cyberattacks by state and non-state actors originating from within the country and other countries. The presence of BSSN as a national cyber institution here plays a role in establishing coordination and cooperation between institutions and stakeholders in the cyber sector in Indonesia.

Cybersecurity Incident Handling

Cyber security has become a priority issue for all countries since information and communication technology is used in various aspects of life. In direct proportion to the high utilization of information and communication technology, the level of risk and threat of misuse of information and communication technology is also getting higher and more complex so that cyber security incidents often occur. A cybersecurity incident is an event that disrupts or threatens the operation of an Electronic System or Critical Information Infrastructure for public services and a violation of compliance with cybersecurity policies.

The Indonesian government, through the BSSN, already has a standard of handling in the event of a cyber attack on a strategic electronic system that can have a severe impact on the public interest, public service; smooth running of the state; or national defense and security. Cybersecurity incident handling attempts to detect, report, assess, handle, respond to, and study cybersecurity incidents. Response to cybersecurity incidents is urgently needed to mitigate, repair, and restore an Electronic System to a normal condition. There is a response cycle when a cybersecurity incident occurs, namely:

1) Preparation;
2) Detection & Analysis;
3) Containment Eradication & Recovery; and
4) Post-Incident Activity (Cichonsk, Millar, Grance, & Scarfone, 2012).

Incident response is urgently needed because cyberattacks often occur with the development of information and communication technology so that it takes the form of handling incidents quickly and systematically and minimizing losses that occur. Incident response has several functions, such as detection as quickly as possible, diagnosis as accurately as possible, control incidents as precisely as possible, control the impact to a minimum restore affected services, find the root cause, and prevent further incidents.

In fulfilling the response to cybersecurity incidents that often occur in Indonesia, the government, through the BSSN, has formed a Computer Security Incident Response Team (CSIRT). The Government Sector CSIRT plays an essential role in maintaining the cybersecurity of the government sector. The Government sector CSIRT consists of Government Sector CSIRT (Gov-CSIRT Indonesia) and Organizational CSIRT at Central Agencies (both Ministries and Non-Ministerial Government Agencies), Provincial and District/City Regional Governments. The Government Sector CSIRT (Gov-CSIRT Indonesia) coordinates and supervises CSIRT Organizations in the Government Sector in handling cyber incidents and distributing information related to cyber security to all members of the Government Sector CSIRT. These teams are made up of specialists who act according to procedures and policies to respond quickly and effectively to security incidents and reduce the risk of cyberattacks.

Challenges in Indonesian Cybersecurity

Handling in dealing with the threat of cyberwar and responding to any cyber security incidents has several obstacles in its implementation. Three crucial issues need attention: regulations, human resources, and owned infrastructure. Indonesia does not yet have specific regulations and policies that regulate cyber security and resilience. BSSN, as the leading sector responsible for national cyber security, does not yet have a clear framework to realize cyber security and defense strategies in Indonesia. Also, human resources who become cyber personnel still have shortcomings both in quantity and quality. In addition to regulatory problems and inadequate resources, some problems must be addressed immediately, such as the national cybersecurity infrastructure, which is still inadequate in carrying out its functions as cyberspace security. Indonesia's internet usage continues to increase. Indonesia must have a plan to build cyber weapons or cyber technology infrastructure to improve national cyber security and resilience in the face of cyber warfare threats.

National cyber security threats such as cyber warfare threats need special attention for the Government in preparing its ability to deal with each of these threats and can even take early anticipation so that these threats do not arise. Policymakers are currently faced with the challenge of very rapid technological development, and comprehensive cyber security governance is needed. It will balance national interests in cyberspace because national cyber policies are relevant to domestic affairs, defense and security policies, foreign policies, industrial and economic policies, research, education, and technology development.

It is not only the provision of government policies needed to deal with national cyber problems. There are essential elements that must be prepared in handling national cyber security threats, and this element is training on how to respond to significant cyberattacks or national crisis management exercises. The Government must carry out national crisis management with several elements, one of which can be cyber disruption exercises against critical national critical vital networks or services. A well-executed exercise will enable the preparation of contingency plans and an assessment of the readiness of the national cybersecurity structure. The exercise will also tell policymakers which priorities need to be prioritized, such as strengthening alternative means of communication, strengthening network defenses in vital areas.

CONCLUSIONS AND RECOMMENDATIONS

The increasing need for internet connectivity encourages digital transformation in Indonesia. The acceleration of this transformation has a complex impact on every side of state life, one of which is the future threat of cyber warfare. With these future threats, Indonesia must increase its awareness and create a safe national cyber environment against significant disturbances that may lead to cyber warfare. Every year Indonesia experiences a rapid increase in cyberattacks. This situation must be addressed immediately to not become a danger in the future. In addition, there are cyber power activities that Indonesia needs to anticipate too, namely subversion, espionage, and sabotage, and several threats of cyber-attacks in Indonesia that are predicted will still dominating namely the malware attacks.

The threat of cyber warfare and other cyber security threats needs to be an essential concern for the Indonesian Government to prepare its capabilities in dealing with each of these threats. Policies in governance are needed in handling national cyber problems in responding to threats when they occur in the cyberspace rapidly and to increase at the same time the national capacity through the implementation of the national crisis management by preparing the contingency plans and improving the cyber security infrastructures that need to be prioritized in the plan in dealing with each of these threats.

REFERENCES

Anderson, N. (2007). Massive DDoS Attacks Target Estonia; Russia Accused. Retrieved October 15, 2021, from Information Technology website: https://arstechnica.com/information-technology/2007/05/massive-ddos-attacks-target-estonia-russia-accused/

Anggraeni, L. (2021). Pengguna Internet Indonesia Capai 202,6 Juta Orang. Retrieved October 15, 2021, from medcom.id website: https://www.medcom.id/teknologi/news-teknologi/yNL4R3qN-pengguna-internet-indonesia-capai-202-6-juta-orang

Arikunto, S. (2010). *Prosedur Penelitian: Suatu Pendekatan Praktik*. Jakarta: Rineka Cipta.

Athanassouli, K. (2018). Economic Implications of the Rise of Information Warfare, Cyber-War and Cyber-Security. In N. J. Daras (Ed.), *Cyber Security and Information Warfare*. New York: Nova.

Ayu, M. G. (2021). BSSN Tangani Ancaman Siber di Indonesia Bersama Quad Helix. Retrieved March 15, 2021, from Cloud Computing website: https://www.cloudcomputing.id/berita/bssn-tangani-ancaman-bersama-quad-helix

Badan Siber dan Sandi Negara. (2020). Laporan Tahunan Hasil Monitoring Keamanan Siber Tahun 2020. Retrieved October 15, 2021, from https://cloud.bssn.go.id/s/ZSdfebRTKW7p8nW#pdfviewer

BBC. (2019). Georgia Hit by Massive Cyber-Attack. Retrieved October 15, 2021, from BBC News website: https://www.bbc.com/news/technology-50207192

Brown, H., Guskin, E., & Mitchell, A. (2012). The Role of Social Media in the Arab Uprisings. Retrieved October 15, 2021, from Journalism website: https://www.pewresearch.org/journalism/2012/11/28/role-social-media-arab-uprisings/

Cichonsk, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide* (NIST Speci). National Institute of Standards and Technology.

CNN Indonesia. (2020). Serangan Siber 2020: Data Pasien Covid-19 RI Hingga KPU. Retrieved from cnnindonesia.com website: https://www.cnnindonesia.com/tekn ologi/20201223144145-185-585740/serangan-siber-2020-data-pasien-covid-19-ri-hingga-kpu

Electricity Information Sharing and Analysis Center. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case*. Washington, DC. Retrieved from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

Gray, C. S. (2013). *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling*. Carlisle: Strategic Studies Institute. Retrieved from https://press.armywarcollege.edu/monographs

Hart, B. H. L. (1967). *Strategy: The Indirect Approach* (4th ed.). London: Faber.

Kementerian Pertahanan Republik Indonesia. (2014). *Pedoman Pertahanan Siber*. Jakarta: Kemhan RI.

Kuehl, D. T. (2009). From Cyberspace to Cyberpower. In *Cyberpower and Nation Security*. Washington, DC: National Defense University. Retrieved from https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation. Retrieved from www.rand.org

McGuinness. Damien. (2017). How A Cyber Attack Transformed Estonia. Retrieved October 15, 2021, from News website: https://www.bbc.com/news/39655415

Moleong, L. J. (2018). *Metodologi Penelitian Kualitatif*. Bandung: PT. Remaja Rosdalarya.

Pusat Operasi Keamanan Siber Nasional. (2019). *Indonesia Cyber Security Monitoring Report 2019*. Retrieved from https://cloud.bssn.go.id/s/nM3mDzCkgycRx4S#pdfviewer

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Riyanto, A. D. (2020). Hootsuite (We are Social): Indonesian Digital Report 2020. Retrieved October 15, 2021, from https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2020/

Rofii, M. S. (2018). Antisipasi Perang Siber: Postur Ketahanan Nasional Indonesia Merespon Ancaman Perang Siber. *Jurnal Kajian Stratejik Ketahanan Nasional*, *1*(2), 105–114. Retrieved from http://jurnalpkn.ui.ac.id/index.php/jkskn/article/view/10

Setyowati, D. (2020). Microsoft: Serangan Malware di Indonesia Tertinggi di Asia Pasifik. Retrieved October 16, 2021, from Digital website: https://katadata.co.id/desysetyowati/digital/5f76e3df376e1/microsoft-serangan-malware-di-indonesia-tertinggi-di-asia-pasifik

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.

Smith, M. (2015). *Research Handbook on International Law and Cyberspace*. Massachusetts: Edwar Elgar Publishing Limited.

The United States Department of Justice. (2016). Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors’ Systems to Steal Sensitive Military Information. Retrieved October 16, 2021, from News website: https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive