Defense Security Development: Cyber Security Capital and Gap in Indonesia

Dini Prilia Gamarlin, Humaizi[a], Opim Salim Sitompul[b] and Muryanto Amin[c]
Doctoral Program of Development Studies, Faculty of Social Science and Political Science,
Universitas Sumatera Utara, Jl. Prof. Dr. A. Sofyan No. 1 Kampus USU, Medan, Indonesia

Keywords: Cyber, Information Security, Policy

Abstract: Today's human dependence on information technology directly presents its own challenges and threats. Attacks on cyberspace are a consequence of the rapid development of information. Information technology is also a central point that has the potential to cause massive damage to various sectors related to cyberspace. Cyberspace can be said to be a complex sector because it relates to other sectors. This relation is a challenge in countering threats in cyberspace. The potential threat of cyber security has encouraged other countries to compete in structuring policies in this field. Indonesia itself until now there is no policy in the cyber sector that is integrative, therefore there must be a seriousness of the government to immediately issue a policy to protect the public from all the onslaught of cyber threats that occur in Indonesia. Discussing about cybersecurity threats means discussing information in cyberspace. Information, data, is a valuable asset that must be protected. Not to mention the growing development of misleading information or hoaxes that have been circulating in the community caused by misuse of information. Information as a very valuable asset for an organization or institution is a strategic resource. Protection of information or information security is an absolute thing that must be seriously considered by all levels of owners, management or employees of the organization or institution concerned. Information security includes policies, procedures, processes, and activities to protect information from various types of threats to it so that it can cause losses for the survival of the organization or institution. Information security assurance can basically be achieved through the activity of implementing a number of appropriate controls. The intended control is the implementation of certain policies, procedures, structures, practices, and functions. The overall control must be implemented by the organization or institution so that all the intended security objectives can be achieved. Therefore, this paper wants to examine the extent of Indonesia's cyber security defense capital, the gap between capital and the facts of the threats that occur, as well as whether existing regulations are sufficient to protect Indonesia from cyber threat attacks, or vice versa. So that cyberspace can be said to be safe from potential cyber threats and crimes. This research is qualitative research with a descriptive method that emphasizes efforts to find the right answer so that it is expected to improve the quality of the implementation of a better cyber defense.

1 INTRODUCTION

Advances in information technology, communication, knowledge, sweeping across the world make borders between countries non-existent, almost all events that occur on earth can be quickly known in other parts of the world. The Internet as a product of information technology creates a world information infrastructure. Many people say that all information can be obtained with just a fingertip and a variety of information appears. This also gives rise to various crimes that appear. For example, decode computer system passwords and transfer some money. Crimes like this can continue to grow considering that there is no integrated surveillance and security system to deal with crimes like this. This crime is born and exists in cyberspace, where millions of computers are connected.

[a] https://orcid.org/0000-0001-8520-9724
[b] https://orcid.org/0000-0001-6069-1841
[c] https://orcid.org/0000-0002-9982-4477

Gamarlin, D., Humaizi, ., Sitompul, O. and Amin, M.
Defense Security Development: Cyber Security Capital and Gap in Indonesia.
DOI: 10.5220/0011563300003460
In *Proceedings of the 4th International Conference on Social and Political Development (ICOSOP 2022) - Human Security and Agile Government*, pages 167-173
ISBN: 978-989-758-618-7; ISSN: 2975-8300

The industrial revolution 4.0 brought changes in the field of technology. These dynamics have an influence on the life of the nation and state. The development of technology connects physical and non-physical infrastructure, the interconnection between these two infrastructures is what we know as cyberspace. Cyberspace is formed because of the existence of an electronic system that is connected to the internet, and most importantly, has an interest in cyberspace, including the government sector, infrastructure and internet users.

The word cyber comes from cybernetic which comes from Greek which means skilled adjective. The term cyber is used to describe existing entities or events that occur in cyberspace. This is realized through a commuter network, which is digital and represented in bits, which in the development of information technology has created a new artificial space (Munir, 2017), as well as giving influence to society and even state sovereignty. The public is not only a consumer of news, but also has a role as a producer of the news itself.

Today many people use the internet as a new medium in life. Like trade transactions, now there are many online shops that make it easier for us to buy everything. Then in the field of telecommunications, telephone, conference, it can be done using multimedia on the internet. In the past, correspondents used direct mail, now it is known as e-mail or electronic mail which makes it easier because it is more practical and faster. Companies also use the internet a lot as a marketing medium. It is different with the field of science and technology, which uses internet media to exchange information and transfer data. The entertainment sector uses it to make products known and economically distributed throughout the world. Mass media uses internet media through online news so there is no need for printing and distribution, because they can directly buy and download from online media. Everyone is trying to use the internet media and trying to get profit from it.

Indonesia is vulnerable to cyberattacks, coupled with the widespread issue of fake and misleading news circulating through social media. In addition, the political realm is also colored by the spectrum of information through cyber that competes with each other at the time of strategic momentum for the country. This is clearly seen during the momentum of elections and local elections, where parties or combinations of parties, candidates or competing figures use cyber for political communication and campaigning. This shows that cyber has strategic meaning for politics and social, therefore this cyber control should not be trapped in the interests of a group.

The National Cyber and Crypto Agency (BSSN) detected more than 495 million cyberattacks throughout 2020. Cyberattacks themselves are divided into two, namely technical attacks and social attacks. Technical attacks are usually in the form of malware, SQL injection that targets security holes to DDOS. The second attack is a social one. This is no less dangerous than attacks that threaten the computer directly. Social attacks basically have a social networking target, or it can be said, an attempt to influence humans through cyberspace or cyberspace. Attacks on the social sphere are related to political warfare, propaganda, human psychology/psychology, and information attacks. This attack actually endangers the unity of the country.

2 THEORETICAL FRAMEWORKS

2.1 Security Concept

Security according to Patrick J. Garrity means “closely tied to a state's defense of sovereign interest by military means. At its most fundamental level, the term security has meant the effort to protect a population and territory against organized force while advancing state interest through competitive behavior”. Security comes from the word safe, which basically means protected from danger, free, safe, in no-dangerous condition, while security means calm, tranquility, and a safe atmosphere. There are many definitions of security that have emerged. As according to Awaloedin Djamin, security is a condition or condition that is free from physical and psychological disturbances, the protection of life safety and the guarantee of property from all kinds of threats and dangers. The concept of security itself is divided into four categories, namely, international security, national (state) security, public security (and order), and human security.

Broadly speaking, national security is a concept where the government in this case the executive together with the legislature must and must protect the country and its citizens against various national crises through various power projections such as political power, diplomacy, economic strength, military capability, cyber, and others (Amaritasari, 2015).

Basically, the concept of national security has existed since the end of the cold war, many new things have emerged and then the concept of national security is affected. Each country has a different concept of the concept of national security; therefore the concept of national security is called flexible because it cannot be defined with certainty. The point is that each country translates the concept of national security and adapts to a very dynamic security situation and condition.

Security by Barry Buzan is "Security, in any objective sense, measures the absence of threat to acquired values, in a subjective sense, the absence of fear that such values will be attacked" (Buzan, 1983), so that it can be used as a basis for establishing for determining the direction of Indonesia's defense policy. The former Indonesian Minister of Defense, Ryamizard Ryacudu, stated that there were eight manifestations of non-military (asymmetric) threats in the context of defending the country, including; terrorism, natural disasters, border violations, separatism, infectious diseases, cyberattacks, drugs and cultural infiltration. In addition, the 2015 Indonesian Defense White Paper explained the three divisions of current threats, namely, military, non-military and hybrid threats. The impacts that can be caused by this threat include various aspects such as political, economic, social, cultural, ideological, as well as defense and security. By looking at the current world security situation and condition, the Indonesian government can analyze and absorb the dynamics that occur at the international level, then take it to the national level, of course, adjusted to the domestic situation and conditions.

2.2 Cyber Attack Concept

Cyberattack or cybercrime is a term that is widely used to describe criminal acts using computer or internet media (Murti, 2005), while according to Gregory (2015) cyber-attacks are a form of virtual crime by utilizing computer media that is connected via the internet and can exploit another computer connected to the internet. Based on the actions and motives carried out by someone who carried out a cyber-attack, it is divided into five parts (Hius, et al, 2014) :

2.2.1 Cybercrime as a Pure Crime

Deliberate crime, where the person intentionally and planned to do damage, theft, anarchic actions against an information system or computer system.

2.2.2 Cybercrime as a Gray Crime

This crime is not clear whether it is a criminal crime or not because he broke into but did not damage, steal or commit anarchic acts against the information system or computer system.

2.2.3 Cybercrime That Attacks Individuals

Crimes committed against other people with a motive of revenge or fad with the aim of destroying one's good name, trying or playing tricks on someone to get personal satisfaction. Example, pornography, cyberstalking.

2.2.4 Cybercrime That Attacks Copyright or Property Rights

Crimes committed against someone's work with the motive of duplicating, marketing, altering, aiming for personal or public interest or for material or non-material purposes.

The linespace must be of exactly 11-point with 9-point of font size and the font style set to italic.

2.2.5 Cybercrime That Attacks the Government

Crimes committed against the government as an object by terrorizing, hijacking or damaging the security of a government with the aim of disrupting the government system or destroying a country.

2.3 Development Concept

Development can be interpreted as a measure of changes in the level of welfare in a measurable and natural way. Indonesia's development paradigm has developed starting from the growth paradigm, then shifted to the welfare paradigm or also referred to in another sense as the basic need paradigm, and finally the people-centered development paradigm. (Bastian, 2006).

Development planning must be adapted to certain development sectors whose approach is based on what is needed by citizens and becomes a development priority based on the country's capabilities. There are four sectoral areas which later became the development planning sector, namely the economic, political, social and defense and security sectors (Wrihatnolo and Nugroho, 2006).

First, the economic sector is the development sector which is divided into economic development groups including agriculture, mining, manufacturing, electricity, gas, clean water, buildings, trade, restaurants and hotels, transportation and transportation, communications, institutional services. financial services, corporate services, general government services, social services, and other services.

Second, the political sector which consists of the sectors of democracy, human rights, law enforcement, regional autonomy, domestic politics and foreign relations.

Third, the social sector which is the development sector which is divided into groups of development of education, health, government administration, facilitation of religious life and its derivatives such as health insurance, social security, education insurance, clean water supply, hygiene and sanitation facilities, management waste, facilitation of religious worship, document services such as birth certificates, population identity documents and so on.

Fourth, the defense sector is the development sector which is divided into the armed forces development group which includes the police force and the armed forces. Development planning in this field is based on the history that the security of all citizens is the responsibility of the state as the holder of the people's mandate. National development planning consists of development plans compiled centrally by Ministries/Agencies and development planning by Regional Governments in accordance with their respective authorities. The results of the planning are the Long-Term Development Plan (RPJP), the Medium-Term Development Plan (RPJM), and the Annual Development Plan.

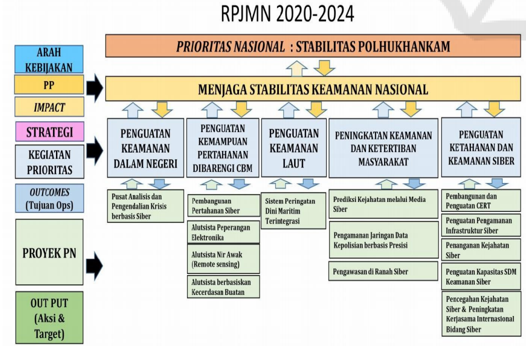
RPJMN 2020-2024
PRIORITAS NASIONAL : STABILITAS POLHUKHANKAM
ARAH KEBIJAKAN
PP
IMPACT
STRATEGI
KEGIATAN PRIORITAS
OUTCOMES (Tujuan Ops)
PROYEK PN
OUT PUT (Aksi & Target)
MENJAGA STABILITAS KEAMANAN NASIONAL
PENGUATAN KEAMANAN DALAM NEGERI
PENGUATAN KEMAMPUAN PERTAHANAN DIBARENGI CBM
PENGUATAN KEAMANAN LAUT
PENINGKATAN KEAMANAN DAN KETERTIBAN MASYARAKAT
PENGUATAN KETAHANAN DAN KEAMANAN SIBER
Pusat Analisis dan Pengendalian Krisis berbasis Siber
Pembangunan Pertahanan Siber
Alutsista Peperangan Elektronika
Alutsista Nir Awak (Remote sensing)
Alutsista berbasiskan Kecerdasan Buatan
Sistem Peringatan Dini Maritim Terintegrasi
Prediksi Kejahatan melalui Media Siber
Pengamanan Jaringan Data Kepolisian berbasis Presisi
Pengawasan di Ranah Siber
Pembangunan dan Penguatan CERT
Penguatan Pengamanan Infrastruktur Siber
Penanganan Kejahatan Siber
Penguatan Kapasitas SDM Keamanan Siber
Pencegahan Kejahatan Siber & Peningkatan Kerjasama Internasional Bidang Siber

Figure 1: 2020-2024 National Medium-Term Development Plan (RPJMN 2020-2024).

3 RESEARCH METHODS

This research is a type of qualitative research, to examine social problems researchers will report on the results of research based on data reports and data analysis obtained in the field, then described in a descriptive method research report that emphasizes efforts to find the right answer so that it is expected to improve better quality of cyber defense implementation. With descriptive, the description of the problem will be seen more clearly by describing the situation or phenomenon accurately and systematically. Primary data obtained from observations, in- depth interviews on the opinions of informants related to cyber management experience.

Observations in this study are observations on the handling of cyber security in related agencies or agencies. In this case, the observation of the main tasks and regulations related to cyber security. in-depth interview, in order to find information and data related to cyber security, supporting and inhibiting factors, initiatives of policy makers, and agencies in charge of cyber security.

4 RESULTS AND DISCUSSION

Indonesia is a country with the highest cybercrime vulnerability in Asia. With a very large number of cellular phone users, with a very large area, mastery of the internet is a mandatory thing that must be owned by the government to unite the entire territory of Indonesia. With a very large number of internet users, cyber threats and attacks can cause paralysis in various sectors, including banking, government service agencies and even the national defense and security system. Therefore, the risk of a large cyber-attack threat requires all sectors to have adequate cyber security in order to protect information technology systems from all forms of cybercrime.

The more users in cyberspace, the more threats that are present, here are some emerging threats (Indrajit, 2016):

1. The first threat is the desire of a number or group of people or parties who want to take various assets or valuables that are exchanged or transacted on the internet. For example, digital money, debit card value, number of bank accounts, to bank account password data, user confidential information, and so on.

2. The second threat is the intention of the group of people to make the internet not function normally, or try to make the internet malfunction. The goal is to disrupt the process of trade transactions, government administrative procedures, and so on. This is because more and more aspects of human life are dependent on the internet. If the internet is disrupted it can lead to chaos.

3. The third threat, attempts to modify data or information on the internet for bad purposes, such as

misleading, pitting, destroying images, deceiving, and so on. The above methods occur in the daily life of internet users.

4. The fourth threat, the will of a person to spread things that are not true to the entire population of the world. For example, spreading misleading ideas, pornographic media, information that supports terrorism, gambling activities, and other hidden crimes.

5. The fifth threat, the spread and planting of malicious programs to computers connected to the internet with the aim of destroying. For example, deleting the contents of the hard disk, retrieving user data, spying on user activity, unwanted viewing, and so on.

The World Economic Forum (WEF) lists “cyber dependence” in the top five risk trends facing society. Therefore, it is important for the government to design regulations, develop cyber capabilities, and, most importantly, apply digital properly so that the public can minimize information security risks, and other risks. Cyber security issues are now an important issue, and were reinforced when President Joko Widodo's state speech in 2019 reminded the importance of sovereignty, including maintaining data security from attacks by mush and hackers, as well as protecting user privacy data, because data is a new and strategic asset of the Indonesian nation that is must be protected from attacks by hackers and enemies.

Indonesia as one of the countries with the largest internet users in the world is very vulnerable to cyberattacks. An example of a case that has occurred is the hacking of the KPU website in the simultaneous regional elections in 2018, resulting in the server being paralyzed and having an impact on public access to all information from election organizers. Next came cyberattacks that paralyzed computer systems in several hospitals and large companies in Jakarta as well as thousands of other IP addresses. There is also the misuse of the internet by terrorist networks to spread propaganda, radicalism, hacking, and others to raise funds and recruit members. From this, it can be seen that threats that occur in cyberspace are dominated by non-state actors but have a direct impact on state security. Threats to state security are not only to attack the government through agencies, but also threaten all aspects of human life.

Today's human dependence on information technology directly presents its own challenges and threats. Attacks on cyberspace are a consequence of the rapid development of information. Information technology is also a central point that has the potential to cause massive damage to various sectors related to cyberspace (Brenner, 2013). Cyberspace can be said to be a complex sector because it relates to other sectors. This relation is a challenge in countering threats in cyberspace. The potential threat of cyber security has prompted other countries to compete in structuring policies in this field. In Indonesia until now there is no policy in the cyber sector that is integrative, therefore there must be a seriousness of the government to immediately issue a policy to protect the public from all the onslaught of cyber threats that occur in Indonesia.

The Ministry of Defense and the Indonesian National Armed Forces have two interests in cyber defense. First to secure all electronic systems and information networks in their environment. Second, support the coordination of cyber security in other sectors as needed. By considering these two interests, it is necessary to anticipate the need for cyber defense which consists of the following aspects (Minister of Defense Regulations number 82/2014):

1. Policy. Policies that become a reference for all cyber defense activities including development, operation and coordination are very important to be formulated and determined. These policies cover aspects of institutional development, preparation of infrastructure and technology, preparation of human resources and determination of roles, functions and authorities in cyber defense within the Ministry of Defense. This need needs to be realized in the form of regulations, guidelines, technical instructions and other forms of policies that can ensure cyber defense activities can run as they should.

2. Institutional. Strong and effective institutions are needed in carrying out cyber defense tasks and activities with reference to established policies. This includes organizational structure, division of tasks and authorities, and work and supervisory mechanisms. This institution needs to be realized through a study of institutional development in all work units of the Ministry of Defense followed by preparatory steps, and the formation, adjustment and/or strengthening of institutions so that effective institutions are available to support cyber defense.

3. Technology and supporting infrastructure. Complete technology and supporting infrastructure are needed as facilities and equipment for cyber defense activities that are carried out, so that cyber defense can be carried out effectively and efficiently. Supporting technology and infrastructure needs to be realized through a development study followed by preparatory steps, and the formation, adjustment and/or strengthening of technology and infrastructure that can be utilized optimally in meeting cyber defense needs.

4. Human resources. Human resources are one of the most important elements in ensuring the implementation of cyber defense in accordance with established policies. Cyber defense special knowledge and skills must be owned and maintained in accordance with the development of cyber defense needs. Human resources are realized in the form of recruitment, coaching and separation programs that refer to applicable regulations.

When viewed from the population, hundreds of millions of Indonesians use the internet and the number continues to grow. The number of cyber-attacks in Indonesia shows the weakness of this country's security system. For example, several government institutions such as the General Election Commission, the Indonesian Child Protection Commission, and even the Ministry of Defense have been victims of hacking targeting government websites. In the corporate sector, for example, the telecommunications company Telkomsel, which was hacked in 2017, and there are many other examples. What concerns espionage is when the Australian government allegedly tapped the cellphones of former President Susilo Bambang Yudhoyono and his wife, as well as several other senior officials between 2007 and 2009. And what was widely reported was when a massive cyberattack occurred in 2017 that infected about 200,000 computers in 150 countries with attackers demanding ransom. In Indonesia, about twelve institutions were attacked, including plantation companies, manufactures, and universities. Therefore, it is important to map emerging threats in order to make policy solutions that are right on target.

In 2008, the Information and Electronic Transactions (ITE) Law was issued, Number 11 of 2008 has been revised in 2016 namely the ITE Law Number 19 of 2016. This law regulates rules regarding several violations, such as distributing illegal content, unauthorized access permission to computer systems to obtain information, data protection violations, takeovers or illegal wiretapping and do not have permission to other computer or electronic systems. Indeed, if the contents of electronic systems and electronic transactions are protected by the ITE Law, on the other hand this Law does not cover important parts of cyber security, such as information and network infrastructure, as well as human resources with expertise in cyber security.

Then in 2019, the government issued a technical regulation based on the 2016 ITE Law, namely Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. There are updates regarding the implementation of cyber security in electronic systems and transactions. Basically, this regulation has stronger rules regarding the protection of personal data and information, as well as web page authentication to avoid fake or fraudulent web pages. This emphasizes the importance of the government to prevent harm to the public interest through the misuse of information and electronic transactions and what is important is the need to develop a national cyber security strategy. The weakness of this lies in the scope of cybercrimes regulated in the regulation, which is only related to electronic transactions, examples of data misuse, unauthorized electronic signatures, and the spread of viruses and links.

Basically, the existing rules have not responded well to cyber threats that continue to grow. It is important to update cyber-related policies. This is important because cyber threats are now growing rapidly in all forms, and targeting critical infrastructure such as the government, therefore it is very important for the government to immediately prepare cyber policies to protect the entire nation. The government must hasten further discussions regarding the cyber security bill by involving the private sector or public private dialogue. By involving the private sector, the government, BSSN and the private sector can exchange relevant information and experience, and produce policies that are appropriate and on target, and are expected to be implemented properly and, last but not least, supported by more stakeholders.

5 CONCLUSIONS

Discussing about cybersecurity threats means discussing information in cyberspace. Information, data, is a valuable asset that must be protected. Not to mention the growing development of misleading information or hoaxes that have been circulating in the community caused by misuse of information. Therefore, this paper wants to examine the extent of Indonesia's cyber security defense capital, the gap between capital and the facts of the threats that occur, as well as whether existing regulations are sufficient to protect Indonesia from cyber threat attacks, or vice versa. So that cyberspace can be said to be safe from potential cyber threats and crimes. For this reason, regulations, ethics, and awareness are needed from power holders or stakeholders so that cyberspace is safe and trusted by the public. In addition, this research is expected to be able to fill in the gaps or lack of references, as well as being able to provide benefits for the government and stakeholders so as to create a cyber security development that is good, conducive, and able to respond to any existing threats.

Information as a very valuable asset for an organization or institution is a strategic resource. Protection of information or information security is something that must be seriously considered by many parties. Information security includes policies, procedures, processes, and activities to protect information from various types of threats to it so that it can cause a lot of losses. Information security assurance can basically be achieved through the activity of implementing a number of appropriate controls. The intended control is the implementation of certain policies, procedures, structures, practices, and functions. All these controls must be implemented so that all the intended security objectives can be achieved.

REFERENCES

Brenner, S.W. 2013. Cyber-threats and the limits of bureaucratic control. *Minnesota Journal of Law, Science, and Technology*, Vol. 14, Issue 1, pp. 137-258. https://scholarship.law.umn.edu/mjlst/vol14/iss1/6.

Buzan, B. 1983. *People, States & Fear*, Wheatsheaf Books Ltd. Great Britain.

Castro, S. 2021. Towards the Development of a Rationalist Cyber Conflict Theory. *The Cyber Defense Review*, Vol. 6(1), pp. 35-62. https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2537125/towards-the-development-of-a-rationalist-cyber-conflict-theory/.

Flynn, M. 2019. Civilians 'Defending Forward' in Cyberspace: Aligning cyber strategy and cyber operations. *International Conference on Cyber Conflict (CyCon U.S.)*, November 18-20, Vol. 5(1), pp. 29-40. https://www.jstor.org/stable/26902661?seq=1.

Iasiello, E. 2014. Is Cyber Deterrence an Illusory Course of Action? *Journal of Strategic Security*, Vol. 7(1), pp. 54-67. http://dx.doi.org/10.5038/1944-0472.7.1.5.

Indrajit, R. E. 2016. *Keamanan Informasi dan Internet*, Preinexus. Yogyakarta.

Munir, N. 2017. *Pengantar Hukum Siber Indonesia*, Rajawali Press. Depok.