MANDALA:
Jurnal Ilmu Hubungan Internasional

Vol. 5 No.2
Juli-Desember
2022

Received:16-10-2022
Accepted:23-10-2022
Published: 31-12-2022

National Cyber Defense Of The Indonesian Government In Protecting The Society

Imam Budiman
Lecturer of International Relations, Universitas Pasundan
Email: Imam.budiman@unpas.ac.id

Abstract

Technological advances in the era of globalization are now unavoidable. All countries in the world are competing in developing technology to facilitate human life. This technological advancement is inseparable from the threats that lurk in every activity. Of course, the role of the state as an actor must protect its citizens from every threat, including technological threats. This makes cyber security required by all countries, including Indonesia. With various challenges faced, as well as several policies implemented, Indonesia is still a country that is vulnerable to attacks in cyberspace. By using a qualitative research method that focuses on describing phenomena through the literature read, this study concludes that optimizing the role of national cyber defense policy can overcome problems that arise due to the advancement of technology in the present time

Keywords: Cybersecurity; Cyberspace; Technology.

Abstrak

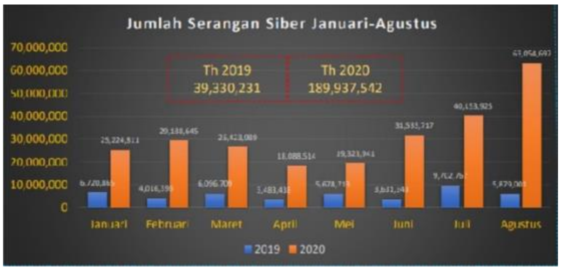
Kemajuan teknologi di era-Globalisasi sekarang tidak dapat dihindarkan. Semua negara di Dunia berlomba lomba dalam mengembangkan teknologi guna mempemudah kehidupan manusia. Kemajuan teknologi ini pun tidak terlepas dari ancaman yang mengintai di setiap aktifitas nya. Tentu peran negara sebagai aktor yang harus melindungi warga negaranya dari setiap ancaman termasuk ancaman teknologi. Hal tersebut membuat keamanan siber diperlukan oleh seluruh negara, termasuk Indonesia. Dengan berbagai tantangan yang dihadapi, serta beberapa kebijakan yang diimplementasi, Indonesia masih menjadi negara yang rentan untuk diserang diruang siber. Dengan menggunakan metode penelitian kualitatif di mana berfokus dengan mendeskripsikan fenomena melalui literatur-literatur yang dibaca, penelitian ini menyimpulkan bahwa Optimlisasi peran dari kebijakan pertahanan siber nasional dapat mengatasi masalah masala yang muncul diakibatkan maju nya teknologi dimasa sekarang ini.

Kata Kunci: Keamanan Siber; Ruang Siber; Teknologi.

Introduction

Over time, information technology has become one of the most significant tools used in helping humans live their daily lives. According to William (2005, in Kidi, 2018), information technology is a universal form that describes any technology that helps create, manipulate, store, connect, and/or convey information. The tool that was born thanks to the flow of globalization has many benefits, both in the fields of health, education, economy, and others for a country.

In the era of revolution 4.0 where almost all aspects of human life cannot be separated from technology, the activities and processes of various sectors undergo digital transformation. In this digitalization effort, Artificial Intelligence (AI) and Internet of Things (IoT) innovations were born that make it easier for every device to be connected to a computer network, such as the internet. According to data from the International Telecommunication Union (ITU) quoted by the World Bank, there were 49% of the world's population used the internet in 2017 – accounting for the jump since 2000 which was only around 6.7%. Not only that, but Internet World Stats also estimates that in 2021, this number will reach 64.2%.



Data Jumlah Serangan Siber Januari - Agustus 2019/2020(Pusat Operasi Keamanan Siber Nasional)

The number of internet users indirectly backfires because it also increases threats in cyberspace. Cyber security is one of the solutions offered. The International Organization for Standardization (ISO) defines cyber security as measures taken to maintain the confidentiality, integrity, and availability of information in cyberspace. Meanwhile, according to CISCO, cybersecurity is an effort to protect networks, systems, and programs from digital threats. The threats in question are usually varied, such as accessing, changing, or destroying sensitive information, extorting user property, or hindering a business's operation. Therefore, Permatasari (2021) concludes that cyber security is a preventive measure to protect the system from illegal accessibility.

Indonesia is one of the countries with the most internet access. Quoted from DataIndonesia.id, there are as many as 205 million internet users in Indonesia. Based on these data, it means that there are as many as 73.7% of the total population of

Indonesian people. With this significant number, Indonesia is also vulnerable to being the target of cyber threats. Even in 2019, CNN has paid attention to cybersecurity vulnerabilities in Indonesia. According to David Chinn, Senior Partner and Global Leader of Cybersecurity Practice, there are at least 4 (four) reasons why Indonesia is a cyber-vulnerable country, namely 1) limited planning for response in case of cybersecurity-related incidents; 2) the need to improve cyber security policies; 3) cyber risk that is seen as a technology issue, not a business one; and 4) low public awareness of cyber issues so that they are often not vigilant in sending or opening dangerous links.

Technological advances in the era of globalization are now unavoidable. All countries in the world are competing in developing technology to facilitate human life. This technological advancement is inseparable from the threats that lurk everywhere. data and account breaches, these are things that must be watched out for together considering that this crime does not discriminate.

Cybercrime is any illegal activity used by criminals using computer network information system technology that directly attacks the victim's information system technology. But more broadly cyber crime can also be interpreted as all illegal acts that are supported by computer technology activities. Of course, the role of the state as an actor must protect its citizens from every threat, including technological threats. This makes cyber security required by all countries, including Indonesia. With various challenges faced, as well as several policies implemented, Indonesia is still a country that is vulnerable to attacks in cyberspace. By using a qualitative research method that focuses on describing phenomena through the literature read, this study concludes that optimizing the role of national cyber defense policy can overcome problems that arise due to the advancement of technology in the present time

THEORETICAL FRAMEWORK

Securitization

Securitization is understood as the process of a political problem that was previously not a military problem to be resolved into a security problem by looking at the problem from a security point of view so that it becomes a country's national agenda or even a global agenda. Security studies are not only about the state and the military, but also several other fields, namely economic, political, social, and environmental (Buzan et.al, 1998). Cybersecurity belongs to the social, but can also include the political realm. Securitization here is used to determine the transition of focus where at first cyber did not get attention in security, but digitalization began to become one of the aspects that could threaten a country.

Non-traditional Security After the concept of Traditional Security began to develop, Barry Buzan also expanded his definition with a statement that reads that security does not only cover the military field with state actors but also includes non-military and non-state elements. In brief, Buzan (1998) concludes that Nontraditional Security focuses on the issue of non-military threats and the roles played by non-state actors. Buzan's previous statement later gave birth to a stance from the United Nations in the 1990s regarding the meaning of the concept of security. In its stance, the United Nations changed the definition to "The concept of security must move from an exclusive emphasis on national security" and then formalized the identity of Non-traditional Security as one of the concepts used by thinkers of International Relations.

Cybersecurity

Cyberspace is an electronic medium and computer network where communication occurs online. Dewi Triwahyuni said that the concept of cyber security no longer only touched the realm of technology, but had become a threat to national security. Cybersecurity addresses the issue of information security for governments, organizations, and individual affairs related to ICT technology, and in particular to Internet technology.

National Cyber Defense

Indonesia has started to fight cybercrime because it is considered a threat that has very high potential in the current era of high technology. It is proven that Indonesia made a design or agency that regulates cyber security, which was named National cyber defense. It should be grateful, at this time Indonesia has begun to direct its cannons toward cyber battles. The Ministry of Defense responds to this cyber war by actively holding seminars and workshops involving Ministries/LPNKs, Universities, Experts, and other parties to formulate an integrated information technology system in dealing with information technology wars through cyberspace packaged in the concept of the Cyber Defense System. Cyber Defense). So that on October 23, 2012, the Minister of Defense formed a Cyber Defense Working Team, which is chaired by the Director General of Pothan Kemhan and consists of related units in the Ministry of Defense Work Unit as well as Resource

Persons from the Ministry / LPNK, Universities, Experts and the cyber community, Team This work outlines the formulation of the National Strategy Roadmap for national defense relating to cyber threats and building the defense of national cyber organizations

Information, Communication, and Technologies (ICT)

ICT is Information and Communication Technologies and refers to technology that provides access to communication, where by using this ICT people can communicate in real-time with people in other countries using instant messaging, Volp (voice over internet protocol), and video conferencing. The phenomenon of the rise of ICT creates a new era called the information age. In the study of International Relations with the mastery of ICT, a country's way to spread power and influence to other countries becomes easier. Unfortunately, there is a disparity in ownership of capabilities in the ICT sector between one country and another or between a group of developed countries and developing and underdeveloped countries (Putri, 2015).

RESEARCH METHODS

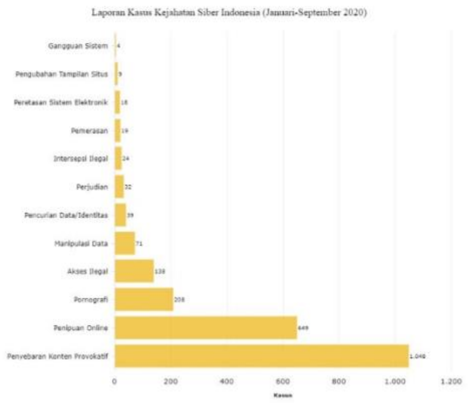
In researching this problem, the researcher uses qualitative research methods. According to Brady (2015), the qualitative research method is a method that provides tools to understand the substance of definitions related to complex phenomena and processes in the practice of social life. In addition, in 2013, Hilal and Alabri argued that this method attempts to explain an incident based on the informant's perspective, based on varied realities, and develop a holistic understanding of a particular context regarding the incident. Finally, Bertens (1987, in Eddles-Hirsch, 2015), argues that the qualitative research method analyzes and describes an individual's phenomenon in his daily life.

The data collection technique that the researcher uses is to use a literature study based on several sources, such as reference documents, articles, journals, and books, both in print and online, which are related to the title being researched, namely "Cyber Space: Challenges and Government Efforts to Protect Cybersecurity in Indonesia”.

RESULT

Cyber Security Challenge

In implementing effective cybersecurity, there are many challenges considering the supporting tools are also starting to vary. Although cybersecurity support infrastructure is strengthened, it does not mean eliminating potential exponential threats.



Sumber: Databook

The urgency of this cyber security requires serious action in building a reliable, competent, competent information and data bank design and making operational standardization in managing information and data. Cybersecurity does not only attack directly, but also in cyberspaces that are so wide. Based on the implementation operations, the following are the types of cyber threats:

a) Cybercrime

In this threat, the perpetrators usually consist of those who have expertise in hacking. Hacked information and data are usually stolen by them to commit fraud or account break-ins. espionage, and the like.

b) Cyber Warfare

This threat is a form of warfare that occurs in cyberspace or cyberspace. The main media that are attacked by this threat are cyber objects that are owned or controlled by a country.

c) Cyber Terrorism

This threat is usually carried out by terrorists who use cyberspace to spread their terror through cyberspace. Some examples of cyber terrorism are attacks on official government websites, awareness of political communications, theft of electronic data, and so on. Also, in carrying out cyber attacks, there are several methods used by the perpetrators, namely:

a. Malware

1) Viruses 2) Trojans 3) Spyware 4) Ransomware 5) Adware 6) Botnets. Social Engineering

c. SQL Injection

d. Email Spam & Pishing

e. Domain Name

1) Cybersquatting

2) Typosquatting

f. Denial of Service (DoS)

Of course, cyberspace has many benefits in facilitating almost all human activities. However, reflecting on the potential challenges that exist, cyberspace is also one of the focuses of the state to maintain its national security, including Indonesia.

Cyber Security in Indonesia

In his journal, Ardiyanti (2016) states that Indonesia is currently in a state of urgency for cybersecurity because the level of cybercrime or cyber crime in Indonesia has reached an alarming stage. Data compiled by the CIA states that the losses caused by cybercrimes in Indonesia have reached

1.20% of the losses due to cybercrime that occurred worldwide.

Indonesia began to address cyber security through the establishment of the Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) in 2007. The Ministry of Communication and Information (Kemkominfo) assigned the team to conduct internet protocol-based network security surveillance. Some of the duties of ID-SIRTII include monitoring, early detection, early warning of threats and disturbances to the network, coordinating with relevant parties, both at home and abroad, in carrying out the task of securing internetprotocol-based telecommunications networks, operating, maintaining, and develop the IDSIRTII system database system by compiling catalogs and syllabus related to the process of securing network utilization, providing information services on threats and security disturbances in securing the utilization of telecommunication networks based on internet protocols, becoming a contact point with related institutions regarding the security of securing the utilization of telecommunication networks based on internet protocols as well as compiling work programs to carry out work related to security and security of utilization of telecommunication networks based on internet protocols.

In 2018, the National Cyber Security Index released data stating that Indonesia was ranked 83 out of 100 countries related to the most vulnerable countries to be hacked with 19.48 points. This figure is quite high when compared to Indonesia's digital development index which touched 50.22 points (Krisnaduta, 2019).

Cybersecurity Policy and Challenges in Indonesia:

a. Legality

The establishment of ID-SIRTII in 2007 became Indonesia's starting point in shaping policies regarding cyber security in Indonesia. The legal basis for cyber security is currently built based on the Information and Electronic Transaction Law no. 11 of 2008, Government Regulation on the Implementation of Electronic Systems and Transactions no. 82 of 2012, as well as ministerial circulars and ministerial regulations. However, the legality of crime prevention in the cyber world is still weak. This is because, even though some laws and regulations prohibit any form of attack or destruction of electronic systems in the Electronic Information and Transaction Law No. 11 of 2008, there is still no legislation that specifically regulates cyber attacks and their handling, making it difficult for law enforcement officials to process. In terms of legality, developing cyber security is about having a document security policy document as a standard that is used as a reference in the implementation of all processes related to information security. The development and strengthening of Indonesia's cyber security policies must be integrated with the national strategy to build a national cyber security ecosystem prepared by the government.

b. Technical & Procedural

In general, Gautama explained several problems related to cyber security development efforts, namely:

1. Weak understanding of countries related to the cyber world that requires restrictions on the use of services whose servers are located abroad and the use of a secured system is required.
2. The legality of handling attacks in cyberspace.
3. The pattern of incidents of cybercrime is so fast that it is difficult to handle.
4. National cyber-security institutional governance.
5. Low awareness or awareness of international cyber-attack threats that can paralyze a country's vital infrastructure.
6. Indonesia's industry is still weak in producing and developing hardware or hardware related to information technology which is a gap that can strengthen or weaken defenses in the cyber world.

The handling of cyber crimes is still partial and scattered, and there is no standard coordination in cyber security issues. Regarding cyber security policies in Indonesia, it is necessary to make policies that regulate various elements related to cyber security in different ways. The main element of cyber security that must be met during the availability of information infrastructure is the media which plays a role in the continuity of information operations, including hardware and software. Next, in cybersecurity, from a technical point of view, is the improvement of devices connected to computers

Personnel, infrastructure, applications, services, telecommunications systems, and the totality of information transmitted and/or stored in cyberspace.

c. Organizational structure

Another challenge is that the handling of cyber security in national defense is still sectoral and uncoordinated and not integrated. One alternative policy to combat cybercrime which has reached an alarming level is to place cybersecurity in the context of defense. An organization related to cyber security must adapt to the organization's use of information technology systems by focusing on four main things, namely: 1) information systems; 2) organizational competition; 3) information systems and decision-making in the organization (information systems and decision making in the organization), and 4) organizing the use of information systems (organizational use of information systems). Various concepts and steps related to improving the organization and management of institutions engaged in security are applied to achieve and maintain the security nature of organizations and users against relevant requirements, both at the institutional level and at the national level, in reducing cybersecurity risks.

d. Capacity Building

The cyber security skills training and development program is carried out in coordination with the Cyber Defense Operation Center task force. In addition, it is necessary to develop human resources about the importance of cyber security to increase awareness of preventive measures to prevent all cyber crimes. Given the rapid development of technology, the management of cybersecurity resources must be positioned as a business management process. This is necessary because dealing with cybersecurity is not a cheap and fast-growing business. Infrastructure capacity development can reduce the potential costs or expenses associated with technology development by positioning it as a business management process. By managing Human Resources (HR) who are proficient in cybersecurity with business management, it is expected to accelerate the need for HR who understand cybersecurity.

e. International Cooperation

Indonesia's cooperation in fighting cyber crime includes being a member of the ASEAN Network Security Action Council, becoming a member of the International Telecommunication Union (ITU), and becoming a steering committee for the Asia-Pacific Computer Emergency Response Team (APCERT). member of the Forum of Incident Response and Security (FIRST), as well as conducting bilateral cooperation in the field of cyber security with Japan, the UK, and several other countries. The problem is that until now there is no binding international agreement on cyber security, so Indonesia needs to take the initiative as a country to seek a binding collective agreement on cyber security at the international level.

Increased cooperation in the field of information technology and cyber security is expected to open up opportunities for the development of new IT-related media industries in Indonesia as part of strategic sector development. Regarding the development of international cooperation in the context of cyber security development, Indonesia needs to increase its active role in encouraging various collective agreements negotiated at the ILO, which is the leading organization in creating safe cyberspace for the state, and government. society and the business world.

However, it is very unfortunate, with the efforts that have been made, there are still some gaps so it is not uncommon for Indonesia to be one of the countries that are attacked by hackers to steal data, both public data and state data. Indirectly, this is expected to be able to make the government aware that cyber security is also one of the things that must be considered to maintain the national security of the Indonesian nation.

As a developing country, Indonesia can be said to be quite behind in terms of information technology (Nur, 1998). This consequence is felt by Indonesia due to several systematic things, namely Indonesia's lack of sensitivity to research and discourse around technology. The lack of technological modernity in Indonesia results in a lack of knowledge about cybersecurity itself. Among the G20 countries themselves, Indonesia occupies a poor position in cybersecurity issues, which is at level 3 from the bottom with a score of 38.96 (Annur, 2022).

The problems faced by Indonesia in dealing with cyber security issues need to be reviewed from the status of its international relations as a developing country. In this case, several crucial problems that have resulted in the lack of handling of cyber security in Indonesia include (1) economic conditions that are not yet possible to improve cyber quality, (2) political conditions that still tug of war between authoritarianism, democracy, and other issues. populist, and (3) the government's lack of effectiveness in responding to cyber issues resulting in slow change (Paterson, 2019).

In terms of role and functionalization, discourse related to Indonesian cyber security does seem to have to be directed at the basis of government policies and efforts, because broadly speaking, the role of the Indonesian people themselves is lacking in literacy about cyber security in Indonesia (Rai, Heryadi, & Kamaluddin, 2022). Therefore, the government is expected not to ignore the basic rights of the people to access the internet and information must be upheld while ensuring security for its citizens to access freely and responsibly.

Indonesia needs policies that can regulate or protect all elements related to cyber security (Rizal & Yani, 2016). Before taking a policy, the government must take serious steps to be able to comprehensively understand what is meant by cybersecurity and what the threats are. The problems that occur in Indonesia are related to the way the government works as well as the private sector. Indonesia as a sovereign country is expected to realize its capacity and function, namely to protect all citizens from threats, including cyber threats. Public-private cooperation is one such effort.

In this era of globalization, Indonesia is expected to be able to meet international cybersecurity standards. Therefore, Indonesia needs to develop itself domestically and strengthen international and regional cooperation. The reason why Indonesia must strengthen domestic and international aspects lies in Herryanto's conclusion that the policy on cyber security carried out by the Indonesian Ministry of Defense through the MoD policy is still sectoral, and not comprehensive as a single system (Herryanto, 2012).

CONCLUSION

Based on what has been explained, it can be concluded that globalization has given birth to cyberspace with various positive and negative impacts. The negative threats that have the potential to be present are varied, so several strategies or efforts are needed to overcome them. Indonesia, as one of the countries with the most technology users and internet access in the world, of course also has many vulnerabilities in protecting cyberspace. This is the main urgency for the existence of cyber security in Indonesia.

In addition, the Indonesian government itself has at least 5 (five) efforts to improve its cyber security, such as legality, technical and procedural, organizational structure, capacity building, and international cooperation. can be addressed by the government in maintaining the cyber security of the Indonesian nation to minimize the leakage of information or data, both public, and state property. This is because the information or data is the property of the Indonesian people and has the potential to pose a greater threat and threaten the nation's national interests.

REFERENCES

Annur, C. M. (2022). “Indonesia Keamanan Siber Indonesia Peringkat ke-3 Terendah di Antara Negara G20” dalam tautan: https://databoks.katadata.co.id/datapublish/2022/09/13/indeks-keamanan-siber-indonesia-peringkat-ke-3-terendah-di-antara-negara-g20

Brady, S.R. (2015). Utilizing and Adapting the Delphi Method for Use in Qualitative Research Dalam International Journal of Qualitative Methods, Vol.14, No.5.

Buzan, B., & Waever, Ole, & Wilde, Jaap de (1998). Security: A New Framework for Analysis. Lynne Rienner Publisher: Colorado, Amerika.

Edless-Hirsch, K. (2015). Phenomenology and Educational Research Dalam International Journal of Advanced Research, Vol.3, No.8.

Haikal, Muhammad (2018). Kebijakan Censorship Tiongkok Terhadap Perusahaan Multinasional Dalam Bidang Ict (Information Communication Technologies) (Studi Kasus Google Inc.). Skripsi daring Universitas Komputer Indonesia.

Herryanto, E. (2012, November 27). Keynote Speech. *Seminar Nasional Keamanan Infrastruktur Internet tentang Trend Ancaman Infrastruktur Internet 2012*. Bandung, Jawa Barat, Indonesia.

Hilal, A.H.; & Alabri, S.S. (2013). Using Nvivo for Data Analysis in Qualitative Research Dalam International Interdisciplinary Journal of Education, Vol.2, No.2, Hlm.181-186.

Karnadi, Alif (2022). Pengguna Internet di Indonesia Capai 205 Juta pada 2022. Artikel daring Data Indonesia.id yang diakses melalui tautan: https://dataindonesia.id/digital/detail/pengguna-internet-di-indonesia- capai-205-juta-pada-2022.

Kidi (2018). Teknologi dan Aktivitas dalam Kehidupan Manusia. Artikel daring yang diakses pada 29 September 2022 melalui tautan: https://bpsdmd.ntbprov.go.id/wp-content/uploads/2018/05/Teknologi-dan-aktivitas-dalam-kehidupan manusia.pdf

Krisnaduta, Hegar (2019). Kerjasama Indonesia-Australia di Bidang Keamanan dalam Mengatasi Cyber Crime di Indonesia melalui Program Cyber Policy Dialogue. Skripsi daring yang diakses melalui tautan: http://repository.unpas.ac.id/46253/

Nur, M. (1998). “Dilema Pengembangan Infrastruktur Informasi Indonesia”, *Info Komputer*, 12(8), hal. 34.

Permatasari, Dwiyani (2021). Tantangan Cyber Security di Era Revolusi Industri 4.0. artikel daring Kementerian Keuangan Republik Indonesia yang diakses melalui tautan: https://www.djkn.kemenkeu.go.id/kanwil-sulseltrabar/baca-artikel/14190/Tantangan-Cyber- Security-di-Era-Revolusi-Industri-40.html

Paterson, T. (2019). “Indonesian cyberspace expansion: a double-edged sword”, *Journal of Cyber Policy*, 4(2), hal. 216-234

Putri, Sylvia Octa (2015). Kebijakan E-waste Management Pada Perguruam Tinggi berbasos ICT: Suatu Tinjauan Perspektif Green Thought Dan Hukum Lingkungan (Studi Kasus Universitas Komputer Indonesia (2007-2011).

Rai, I. N. A. S., Heryadi, D., & Kamaluddin, A. (2022). “Peran Indonesia dalam Membentuk Keamanan dan Ketahanan di Ruang Siber”, *Politica*, 13(1), hal. 43-65.

Rizal, M., & Yani, Y. M. (2016). “Cybersecurity policy and its implementation in Indonesia", *Journal of ASEAN Studies*, 4(1), hal. 61-78.