RESEARCH ARTICLE

Cybersecurity Policy and Its Implementation in Indonesia

Anggoro Yulianto
Information and Communication Technology Awareness Community Movement (*Gerakan Masyarakat Sadar Teknologi Informasi dan Komunikasi*, GEMASTIK)
✉ puttroanggoro@gmail.com

OPEN ACCESS

Citation: Yulianto, A. (2021). Cybersecurity Policy and Its Implementation in Indonesia. *Law Research Review Quarterly, 7*(1), 69-82. https://doi.org/10.15294/lrrq.v7i1.43191

Submitted : September 3, 2020
Revised : November 3, 2020
Accepted : January 10, 2021

ISSN **2716-3415**
Law Research Review Quarterly published by Faculty of Law, Universitas Negeri Semarang, Indonesia. Published quarterly on February, May, August, and November.

Abstract

The aim of national defense is to protect and save the integrity of the Unitary State of the Republic of Indonesia, the sovereignty of the state, and its security from all kinds of threats, both military and non-military. One of the non-military threats that could potentially threaten the sovereignty and security of the nation-state is the misuse of technology and information in cyberspace. This paper is intended to analyze the cybersecurity policy in Indonesian and its challenges. This paper highlighted that the threat of irresponsible cyber attacks can be initiated by state and non-state actors. The actor may be an individual, a group of people, a faction, an organization, or even a country. Therefore, the government needs to anticipate cyber threats by formulating a cyber security strategy and determining comprehensive steps to defend against cyber attacks; type and scale of retaliation, and drafting the rule of law.

Keywords: *Cybersecurity; Cybercrime; Law Enforcement; Policy*

1. INTRODUCTION

In the era of globalization, cyberspace has become the staple of human life, and connects people regardless of distance. Cyberspace is a new world brought by the internet (Mahzar, 1999: 9). Paul Wagner (2010) argues that cyberspace is outside every computer system that is connected by wire. Cyberspace also includes:

1) isolated networks (private, military companies);
2) laptops and other personal PCs connected several times (wireless, modem);
3) industrial control machines, including programmable logic controllers (PLCs);

4) industrial robots (connected to a PLC or directly to a computer);
5) home control equipment (household appliances and control units);
6) mobile devices (smartphones, PDAs); and
7) USB and other storage devices.

The virtual world displays reality, even though it is not the real one. This is a virtual world, virtual reality, a world without borders. This is what is meant by a world without borders in a way that cyberspace does not recognize national boundaries, and it removes the dimensions of space, time, and place (Purbo, 2000: 50; Islami, 2018). It enables its citizens to connect with anyone anywhere as Bruce Sterling (1992) argues: *While not exactly "real," "cyberspace" is a real place.* Everything that happens there has very genuine consequences. This "place" is not "real," but it is serious, earnest. Tens of thousands of people have dedicated their lives to it, to the public service of wire and electronic communications.

The concept of cybernation sparked hopes to bring people endless comfort, happiness, and opportunities. However, it comes with a price. Cyber security is a real and urgent need because its impact has the potential to damage or disrupt the lives of people, countries, and even the whole world (Piliang, 1999: 14-15).

The urgency of cybersecurity is all the more pressing because the internet has a certain dark side, for example it is widely perceived to provide access almost exclusively to pornography. A recently published survey showed that more than 80% of the images on the internet are pornographic. Although the survey results themselves turn out to be completely false, the observation that the internet can and does contain illegal, inappropriate or completely illegal material is perfectly legitimate. It also supports fraudulent traffickers, terrorist information exchanges, software pirates, computer hackers, and more (Barrett, 1997: 21; Rizal & Yani, 2016; Jurriëns & Tapsell, 2017).

The world has long been worried about cybercrime. In fact, one of the topics discussed at the 10th UN Congress on the Prevention of Crime and the Treatment of Offenders in Vienna, Austria, 2000 was Crime Related to Computer Networks. However, not every country has cybercrime laws, and not all of them are very worried about this

problem (only developed countries and some developing countries). This depends on how well the country develops laws and how much to do with technological advances. This was revealed at the UN Congress in Vienna:

Reasons for the lack of attention to cybercrime may include relatively low participation rates in international electronic communications, low levels of law enforcement experience and low estimates of expected public harm from e-crime (United Nations Office on Drugs and Crime, 2000).

As a developing country, Indonesia is a little behind in following the development of information technology (Nur, 1998: 34; Chasanah & Candiwan, 2020; Setyawan & Sumari, 2016), as a result of an inappropriate technology development strategy that ignores scientific and technological research. As a result, the transfer of technology from advanced industrial countries was not followed by the mastery of technology itself which turned Indonesia into a non-technology-based country. As an alternative, as Nur (1998: 5-6) said, Indonesia is a new pseudo-industrialized country.

2. METHOD

The fact that Indonesia is still lagging behind in information technology raises questions about the conditions for implementing cyber security policies in Indonesia. Therefore, this study seeks to address this issue. The object of this research is cyber security in the context of law and national defence. Aspects of this discussion include law, national defence, and an international relations perspective. We will use the theory of realism as an analytical knife to see how Indonesia reacts to this international phenomenon. Realism is a school of thought in which states compete for power in international. The study of relationships, power is one of the most widely used concepts (the main concept) as well as the most controversial and difficult to define (Perwita & Yani, 2006: 13).

3. RESULT AND DISCUSSION

A. Cyber Threat Forms and Attack

Cybercrime is a cross-border crime. Because it crosses borders and involves many countries, cybercrime is considered an extraordinary crime. As such, it is important to have multilateral agreements to address them, both at the

regional and international levels. The use of military force should be a last resort. This is because a country cannot simply use military force to carry out attacks or initiate battles. There are many things to consider such as costs and budget. The country must build cyber defence based on digital technology immediately. Some forms of cyber threats today are as follows (Ministry of Defence of the Republic of Indonesia, 2013: 25):

1) Advanced persistent threats (APT), denial-of-service (DoS), and distributed denial-of-service (DDoS) attacks are typically carried out by straining system capacity and preventing authorized users from accessing and using targeted systems or resources. These attacks represent dangerous threats to organizations that rely almost entirely on the ability of the Internet to carry out their activities;
2) The vandalism attack is carried out by replacing the victim's web page with a fake page, where the type of content depends on the criminal motive (it can be pornographic or political);
3) A malware attack is a malicious program or code that can be used to interfere with the normal operation of a computer system. Typically, malware programs are designed for financial gain or other benefits;
4) Cyber infiltration can attack a system through identification.

Authorized user and connection parameters such as password. These attacks are carried out by exploiting vulnerabilities that exist in the system. The main methods used to gain access to the system are:

1) Guess very clear passwords, such as a person's username, the name of someone's spouse or child, date of birth or anything important and related to someone or their family, so that they are easy to guess and find out;
2) Take advantage of an unprotected account. Users can also make mistakes, by not entering their password or giving their password to someone else;
3) Fraud and social engineering. For example, the perpetrator could claim and act as administrator and ask for a password for several technical reasons;

4) Listening to data communication traffic. An eavesdropper will listen to unencrypted data sent over the network via a communication protocol;
5) Trojan horses, certain spying programs and spyware are very dangerous. It can secretly record the parameters used to connect to a remote system.
6) Testing all possible permutations that can be the key to cracking a password, if a cracker knows the cipher algorithm; and
7) Espionage, this is done by recording their connection parameters using software, spyware, or multimedia devices, such as video cameras and microphones, to capture confidential information, such as passwords for accessing protected systems.

Apart from the cyber threats above, there are other types of cyberattacks. These cyberattacks can be categorized into (Carr, 2009):

1) Hardware threat, this threat is caused by the installation of certain equipment that functions to perform certain activities in a system. Therefore, the equipment is a disruption to network systems and other hardware. For example, jamming and network disruption.
2) Software threats, this threat is caused by software whose function is to steal information, to destroy information / systems, manipulate information (Corruption Information) in a system, and others.
3) Data/information threats, this threat is caused by the dissemination of certain data / information for certain motives. What is done in information warfare is considered propaganda.

B. The Role of Cyber Security in National Security

Weak cyber defences can create tensions between countries and destabilize security, create social, economic, and environmental impacts, and disrupt relations between countries (Ghernaouti-Hélie, 2009: 24; Nugraha & Putri, 2016). Cyber security has two keywords: cyber and security. Talking about cyber means talking about information, connections (telecommunications, networks), gateways (computers, devices, users), space, or space, and it is about engaging, using, or relating to computers, networks, and the internet. Meanwhile, security is usually related to assets and asset protection. Security protects assets, protects

computers, networks, programs, and data from unwanted or unauthorized access, alteration or destruction,

Computer security, cyber security, or IT security is information security applied to a computer or network. Computer security aims to help users prevent fraud or detect any fraudulent attempts in information-based systems. Information itself is non-physical. Cyber security is an effort to protect information from cyberattacks. Cyberattack in information operations means any deliberate act to compromise the confidentiality, integrity, and availability of information. This action can be in the form of physical disruption or disruption of the logical flow of the information system. Cyberattacks are attempts to disrupt information that focuses on the logical flow of information systems. National Cyber Security is a term used for cyber security related to the assets / resources of a country (Boisot, 1998: 18; Saputra, et.al, 2019; Arianto & Anggraini, 2019).

The purpose of national cyber security is the protection, domination and control of data and information. National cyber security is closely related to information operations, which involve various parties such as the military, government, state-owned companies, academics, the private sector, individuals, and the international world (Siagian, Budiarto, & Simatupang, 2018). The continuity of information operation does not only depend on cyber security itself, it also depends on physical security, which is related to all physical elements such as data center buildings, disaster recovery systems, and transmission media.

C. Cyber Security Policy in Indonesia

In terms of cyber security, Indonesia already has cyber security systems and strategies implemented by government agencies as well as official communities. Cyber security policy is coordinated by the Ministry of Communication and Information (MCI). There are three government organizations involved in cyber security in Indonesia, which are the Information Security Coordination Team, the Directorate of Information Security, and the Indonesian Security Incident Response Team on the Internet Infrastructure (ID-SIRTII) (Nugroho, Abdullah, Wulandari, & Hanafi, 2019; Saudi, 2018; Zaleski, 1999).

The Information Security Coordinating Team was formed in April 2010 to coordinate cyber security, with a focus on expertise and practice in the information and technology fields. The Information Security Directorate has the task of policy formulation and implementation, training, monitoring, evaluation and reporting in the field of information security governance. Finally, ID-SIRTII was established by the government based on the Government Regulation of the Minister of Communication and Information Technology No. 8 of 2012 to deal with security in internet infrastructure.

Meanwhile, there are two community organizations involved in cyber security in Indonesia. Acting as a support agency, the Indonesian Communications Emergency Response Team (ID-CERT) is an organization that works with the government on special cases to support the development of cyber security in Indonesia. In addition, ID-CERT also functions as a support institution for government organizations (Setiadi, Sucahyo, & Hasibuan, 2012: 111; Perwita & Yani, 2006; Slouka, 1999), such as ID-SIRTII. Another community organization is the Indonesian Academic Computer Security Incident Response Team (ID-ACAD-CSIRT), an organization for universities wishing to focus on developing security in Indonesia. ID-ACAD-CSIRT currently has 40 academic CSIRT university members.

D. Laws and Regulations Related to World Security in Indonesia

The Indonesian government has made a policy regarding the application of cyber security in its law based on Law no. 11 of 2008 concerning Information and Electronic Transactions (ITE). There are several other laws that are indirectly related to policy, but are related to this information, such as Law No. 36 of 1999 concerning Telecommunications, and Law No. 14 of 2008 concerning Freedom of Information.

In addition, the following are laws that support the implementation of cyber security:

1) Law Number 8 of 1999 concerning Consumer Protection,
2) Law Number 2 of 2002 concerning the National Police of the Republic of Indonesia,
3) Law Number 3 of 2002 concerning State Defence,

4) Law Number 15 of 2003 concerning the Enforcement of Government Regulations in lieu of Law Number 1 of 2002 concerning Terrorism and the Eradication of Crime as Law,
5) Law Number 34 of 2004, concerning the Indonesian National Army, and
6) Law Number 25 of 2009 concerning Public Services.

Until now, government regulations as law enforcers, which support the implementation of the national information security policy, are still being processed by MCI. However, several presidential regulations have become a reference in implementing national information security policies. Some of the rules are:

1) Presidential Instruction Number 3 of 2003 concerning National Policy for E-Government Development,
2) Presidential Regulation No. 20 of 2006 concerning the National Agency for Information and Communication Technology (ICT), and
3) Presidential Regulation No. 41 of 2010 concerning the General Policy on National Defence in 2010 - 2014.

Meanwhile, MCI as an ICT regulator has released several regulations as implementation guidelines, such as:

1) Regulation of the Minister of Communication and Information Technology No. 29 of 2006 concerning Certification of Authority Implementation Guidelines,
2) Regulation of the Minister of Communication and Information Technology No. 28 of 2006 concerning the Use of the go.id Domain Name for All Central and Local Government Officials on the Website,
3) Regulation of the Minister of Communication and Information Technology No. 30 of 2006 concerning the Supervisory Committee of the Certification Authority,
4) Regulation of the Minister of Communication and Information Technology No. 41 of 2007 concerning General Guidelines for National ICT Governance,
5) Decree of the Minister of Communication and Information Technology No. 57 of 2003 concerning Guidelines for Making the Institution's E-Government Development Master Plan.

To optimize implementation efforts, the regulations issued require additional material and elaboration on implementation strategies, cooperation models, and organizations. In addition, the implementation of national

cyber defence requires coordination between institutions (Ministry of Defence of the Republic of Indonesia, 2013: 35).

E. Current Cyber Security Policies in Indonesia

Indonesia's cyber security policy began in 2007, after the issuance of the Minister of Communication and Information Technology Regulation No. 26 PER/M.Kominfo/5/2007 concerning Security of Use of Internet Protocol-Based Telecommunication Networks, which was later replaced by Ministerial Regulation of Communication and Information Technology No. 16 /PER/M.Kominfo/10/2010. This was later updated with Ministerial Regulation of Communication and Information Technology NO.29/PER/M.Kominfo/12/2010. An important aspect in regulation is the establishment of ID-SIRTII. The Minister of Communication and Information Technology has assigned a team to help control the security of internet protocol-based telecommunications networks.

The function and task of ID-SIRTII is to monitor and detect early and warn when there is interference on the network. The team also coordinates with relevant parties at home and abroad when it is necessary to secure the network. The team also provides information when threats and disturbances arise. Finally, ID-SIRTII is also working to compile a work plan (Article 9 of the Minister of Communication and Informatics Regulation No. 29/PER/ M.Kominfo/12/2010). According to Hasyim Gautama, the cybersecurity legal framework in Indonesia is based on Law No. 11 of 2008 concerning Information and Electronic Transactions, Government Regulation No. 82 of 2012 concerning the Application of Electronic Systems and Transactions, as well as ministerial circulation letters and ministerial regulations (Ardiyanti, 2014).

Apart from the initiation of laws related to cyber security, to ensure legal certainty in the development of cyber security, the government enforces a national cyber security framework. However, the legal framework for dealing with cybercrime is still weak. Although there are laws that prohibit any form of attack or tampering with electronic systems, no law that specifically regulates and contains cybercrime is available. Meanwhile, cybercrime is evolving and progressing rapidly, making it difficult for law enforcement to handle it (Sterling, 1992; Sudarsono, 1992).

F. Implementation of Cyber Security in Indonesia

The way of handling cyber security in the framework of state defence is still sectoral, not well coordinated or not yet integrated. As stated by the Secretary General of the Ministry of National Education Eris Herryanto (2011), the cyber defence concept applied by the MoD and the Indonesian National Army is still sectoral, not comprehensive as a unit (Herryanto, 2012; Adrdiyanti, 2016).

Therefore, the Ministry of Defence formed a cyber defence operations center team to deal with cybercrime as well as to secure and protect countries in cyberspace. The establishment of the Cyber Defence Operations Center in the national cyber security policy is intended to build a universal defence system, which involves all citizens, territories, and other national resources, and to uphold state sovereignty, as well as to protect the territory. integrity and security of the entire nation from cyber threats.

One of the alternative policies is to place cyber security in the context of defence. Several policies that have been implemented are also in the context of defence. The Cyber Defence Operations Center, as described above, is one of them. The center has a working team formed in 2010 that draws up plans to form an information security incident management team (Alwajih, 2014; Nur, 1998).

4. CONCLUSION

Indonesia already has several policies that regulate cyber security; however, the nature of the policy is general in nature (*lex generalis*, and therefore not specific (*lex specialis*). As a result, the implementation of cyber security has not been effective. To be effective, the government needs to make it specific. and, together with all stakeholders, continue to socialize it. Therefore, the government needs to take the implementation of cyber security more seriously to anticipate cyberattacks Singapore and Malaysia, among ASEAN members, already have specific cyber security policies, and this is in line with the potential threats. Indonesia, on the other hand, does not have a special agency with full authority to manage and handle cyber security, yet. However, even without a special institution, the government must still be able to establish one of its structures or institutions to become the leading sector. This

shows us that the implementation of cyber security is diffuse and that the role of government in cyber defence is small. There are individuals who try to violate norms and laws, break rules and regulations, or take control of the security of information and physical assets for material or non-material benefits. Therefore, the government needs to make some serious efforts to anticipate cyber threats and attacks and save Indonesia's cyber defence from being targeted by irresponsible parties.

5. DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no potential conflict of interest in the research, authorship, and/or publication of this article.

6. FUNDING

None

7. ACKNOWLEDGEMENT

None

8. REFERENCES

Alwajih, A. (2014). Dilema E-Democracy di Indonesia: Menganalisis Relasi Internet, Negara, dan Masyarakat. *Jurnal Komunikasi*, *8*(2), 139-152.

Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, *5*(1), 95-110. https://doi.org/10.22212/jp.v5i1.336.

Arianto, A. R., & Anggraini, G. (2019). Membangun Pertahanan Dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). *Jurnal Pertahanan & Bela Negara*, *9*(1), 13-30. http://dx.doi.org/10.33172/jpbh.v9i1.497.

Chasanah, B. R., & Candiwan, C. (2020). Analysis of College Students' Cybersecurity Awareness in Indonesia. *SISFORMA*, *7*(2), 49-57. https://doi.org/10.24167/sisforma.v7i2.2706.

Islami, M. J. (2018). Tantangan dalam implementasi strategi keamanan siber nasional indonesia ditinjau dari penilaian global cybersecurity index. *Masyarakat*

Telematika Dan Informasi: Jurnal Penelitian Teknologi Informasi dan Komunikasi, *8*(2), 137-144. http://dx.doi.org/10.17933/mti.v8i2.108.

Jacob, T. (1993). *Manusia, Ilmu dan Teknolog.* Yogyakarta: PT Tiara Wacana.

Jurriëns, E., & Tapsell, R. (Eds.). (2017). *Digital Indonesia: Connectivity and Divergence*. Singapore: ISEAS-Yusof Ishak Institute.

Nugraha, L. K., & Putri, D. A. (2016). *Mapping the Cyber Policy Landscape: Indonesia*. London: Global Partners Digital.

Nugroho, F. P., Abdullah, R. W., Wulandari, S., & Hanafi, H. (2019). Keamanan Big Data di Era Digital di Indonesia. *Jurnal Informa*, *5*(1), 28-34. https://doi.org/10.46808/informa.v5i1.65.

Nur, M. (1998, August). Dilema Pengembangan Infrastruktur Informasi Indonesia. *Info Komputer*, *XII* (8), 27-39.

Perwita, A.A., & Yani, Y. M. (2006). *Pengantar Ilmu Hubungan Internasional.* Bandung: PT Remaja Rosdakarya.

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

Saputra, P. N., Sudirman, A., Sinaga, O., Wardhana, W., & Hayana, N. (2019). Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP). *Central European Journal of International & Security Studies*, *13*(4), 104-120.

Saudi, A. (2018). Kejahatan Siber Transnasional dan Strategi Pertahanan Siber Indonesia. *Jurnal Demokrasi dan Otonomi Daerah*, *16*(3). 165-256.

Setyawan, D. P., & Sumari, A. D. W. (2016). Diplomasi Pertahanan Indonesia Dalam Pencapaian Cybersecurity Melalui ASEAN Regional Forum on Cybersecurity Initiatives. *Jurnal Penelitian Politik*, *13*(1), 1-20. https://doi.org/10.14203/jpp.v13i1.250.

Siagian, L., Budiarto, A., & Simatupang, S. (2018). Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. *Peperangan Asimetrik*, *4*(3), 1-18.

Slouka, M. (1999). *Ruang yang Hilang: Pandangan Humanis tentang Budaya Cyberspace yang Merisaukan.* Bandung: Mizan.

Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier.* New York: Bantam Books.

Sudarsono, J. (1992). *Ilmu, Teknologi, dan Etika Berprofesi: Pandangan Sosial Politik.* Jakarta: Masyarakat Jurnal Sosiologi, FISIP UI-Gramedia.

Zaleski, J. (1999). *Spiritualitas Cyberspace: Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagamaan Manusia*. Bandung: Mizan.

I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive. We've created life in our own image.

Stephen Hawking

ABOUT AUTHORS

Anggoro Yulianto is an activist and community empowerment activist. Currently, his activities assist the community by increasing public awareness of information technology and its impacts. Anggoro is actively advocating for various cases related to data privacy, cybersecurity, and technology.