Measuring Legal Readiness on Determination of Cyber Security Threats on Electronic System in Indonesia

Arlina Permanasari
{arlina.p@trisakti.ac.id}

Universitas Trisakti, Jakarta, Indonesia

Abstract. The number of cyber-attacks in Indonesia which has doubled since 2019 and reached 495,337,202 in 2020 needs to be followed up comprehensively, including the preparation of legal instruments. The Law No. 11 of 2008 on Information and Electronic Transactions and Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions are the basis documents for regulating cyber security and defence systems that still requires strategic and effective control, coordination and supervision. This paper discusses the readiness of legal instruments, which refers to the cyber security system as part of cyber defence. The discussion refers to the content analysis of national regulations on the cyber security.

Keywords: Cyber security; electronic system; Indonesia

1 Introduction

Since 2014, the internet technology has resulted in cyber-attacks,[1, p. 973] and still continue until now.[2] Today, cyber-attacks are still a debatable issue whether recognized as part of the use of armed force, and can provide support for military operations. A very phenomenal cyber-attack was cyber-attacks on November 20 and 23, 2010 in Iran. The Iranian military officially stated that the Stuxnet worm managed to cause a dangerous explosion at the uranium centre and damage Iran's nuclear facility at Natanz.[3, p. 376] These events have a real, significant impact and break the notion that cyber-attacks cannot have a physical impact.

However, cyber-attacks occurred before the incident can also have a significant impact even though it does not result in a physical impact. A classic example is the cyber-attacks that took place in Georgia, Lithuania and Kyrgyzstan.[4, p. 237] At that time there were cyber-attacks in the form of DDoS and SQL injections causing harm on hundreds of websites. The situations behind the cyber-attacks in the three countries more or less make the intensity of cyber-attacks a threat that leads to cyber war.[5, p. 5] Moreover, the attack leads to areas that are very important for the state such as government, banking, health, security and national defence. This needs to be watched out for, among others, by preparing various legal instruments to anticipate cyber-attacks. This raises the main question that will be discussed in this paper, namely how is the readiness of Indonesian legal instruments in responding to the increasing number of cyber-attacks, which can pose a threat to the occurrence of cyber wars.

LePALISSHE 2021, August 03, Malang, Indonesia

DOI 10.4108/eai.3-8-2021.2315053

2 Measuring the Impact of Cyber-attacks for Organization

One example of how efforts must be made to start measuring the impact of cyber-attacks, is to formulate a taxonomy of cyber-harms. The increase of cyber-attacks in the form cyber-based incidents reports, cybercrimes, hacks and various other cyber-attacks, has caused Agrafiotis, Nurse, Goldsmith, Creese and Upton[6] to conduct a survey of the impact received by an organization, by presenting a taxonomy of cyber harm. Based on their in-depth analysis, they identify various kinds of harms due to cyber-attacks. These harms are categorized into five main categories: physical or digital harm; economic harm; psychological harm; reputational harm; and social and societal harms. Each of these major categories will consist of several impacts.[6] For example, the physical or digital cyber harms can be formed into an unavailability of data in victim's computer, theft, infected data, etc.

According to Ioannis et.al., the taxonomy of cyber-harms mentioned above can be developed for various models within an organization based on different parameters; for example an asset-oriented taxonomy. Starting from this argument, the taxonomy of cyber-harms model can also be developed for various sectors in a government. The next thing to do is to determine the level of impact caused by cyber-attack activities.

3 Cyber-attacks in Indonesia

Presidential Regulation No. 53 of 2017 has determined that the function of the Indonesia Security Incident Response Team of Internet Infrastructure Centre (ID-SIRTI/CC) is carried out by the National Cyber and Crypto Agency (BSSN). The duties of ID-SIRTI include conducting early monitoring, early detection, early warning of threats to telecommunications networks from within and outside the country. In this case, ID-SIRTI coordinates with the National Cyber Security Operations Centre in planning and implementing national cyber security monitoring, cyber contact centres, information security management and infrastructure within the national cyber security operations centre.

Based on recent data released by BSSN, data on cyber-attacks that occurred in Indonesia has shown an alarming number and is increasing from year to year. Among these cyber-attacks, the Trojan, which became the anomaly with the highest number, was accompanied by other similar malware such as AllAple, ZeroAccess, WillExec, Glupteba and CobaltStrike.[7] These attacks resulted in several classifications of impacts, such as the occurrence of Denial of Service (DOS) on the victim's computer system, damage to certain systems, and loss of data from the victim's computer system.

Of at least 35 cyber-attacks, the top ten list cyber-attacks complaint during 2020 issued by the BSSN are shown below:[7]

Table 1. Top-10 Cyber Attack Complaint according to BSSN, 2020

No	Types of Attack	Government	National Critical Information Infrastructure	Digital Economy	Total
1	Cross Site Scripting (XSS)	189	56	219	464
2	SQL Injection (SQLi)	256	79	116	481
3	Malware	19	20	0	39
4	Phising	3	4	17	24

No	Types of Attack	Government	National Critical Information Infrastructure	Digital Economy	Total
5	Web Defacement	12	6	0	23
6	Clickjacking	9	4	4	17
7	Sensitive Data Exposure	8	0	6	14
8	XMLRPC	9	4	0	13
9	Weak Password	12	0	0	12
10	Bypass Admin	10	0	0	10

Based on these cyber-attacks, the level of vulnerability and exposure to information security of a particular unit or organization can be determined from high to critical.[7]

4 Assessing the readiness of Indonesian legal instruments on cyber attacks

For the first time, Indonesia has a law relating to activities in cyberspace with the formulation of Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE). This law was later amended by Law no. 19 of 2016. In addition, there is also Government Regulation no. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions. Initially, these two regulations, namely the ITE Law and the Government Regulation, were the basis for building cybersecurity and national cyber defence in Indonesia.

Based on the two rules above, there are important articles that need to be underlined. Article 15 of the ITE Law stipulates that the Electronic System Operator must operate its electronic system in a safe, reliable and responsible manner for the proper operation of the Electronic System. This means that all Electronic System Operators, regardless of whether the system is used for government, commercial, or personal interests, must operate the system reliably, safely and responsibly. While Government Regulation no. 82 of 2012 provides guidelines on how Electronic System Operators operate their systems reliably, safely, and responsibly as mandated by the ITE Law. A list of national regulations concerning cyber security:[8, pp. 14–27]

Table 2. Indonesia national regulations on cyber security

Regulations	Government's Role
Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions	The government's role in facilitating the use of information technology and electronic transactions, protecting the public interest from all kinds of disturbances as a result of the misuse of electronic information and electronic transactions that disrupt public order, and prevent the dissemination and use of electronic information and/or electronic documents containing prohibited contents in accordance with the provisions of laws and regulations.
Government Regulation No. 80 of 2019 on Trading through Electronic Systems	Regulates the main points of e-commerce transactions both from within and outside the country, including business actors, licensing, and payments.
Presidential Regulation No. 95 of 2018 on Electronic-Based Government System	To achieve clean, effective, transparent, and accountable governance as well as quality and reliable public service, as well as increasing the integration and effisiency of the electronic-based government system.
Presidential Regulation	Government's data management policy to produce accurate, up-to-

Regulations	Government's Role
No. 39 of 2019 on One Indonesian Data	date, integrated, and accountable data, as well as easy to access and share between central; and regional agencies.
Draft law on personal data protection.	Draft law to protect personal data as part of Human Rights and the mandate conveyed by the 1945 Constitution of the Republic of Indonesia.

Based on these legal instruments, various digital infrastructures have been prepared in order to deal with possible cyber-attacks:[8]

Table 3. Infrastructure and the Purposes

Infrastructures	Purposes
Palapa Ring	A national fibre optic cable network construction project that connects 90 regencies/cities throughout Indonesia, with 57 service regencies/cities and 33 interconnecting regencies/cities. This network consists of 12,148 kilometres of fibre optic cable consisting of land and underwater optical cables, as well as a 55 hop microwave radio network segment.
Satria Satelit	The Republic of Indonesia Satellite (SATRIA) Multifunction Satellite (SMF) project is expected to be able to connect all education services, health facilities, defence and security administration, as well as local governments throughout Indonesia. The SATRIA satellite is a solution for areas not covered by the Palapa Ring Project. With a capacity of 150 Gbps, the SATRIA Satellite uses High Throughput Satellite (HTS) technology with a Ka-Band frequency, and reaches nearly 150 thousand public service points throughout Indonesia.
Negative Content Search Engine	a proactive monitoring system and control centre system device for handling negatively charged internet content.
Root Certification Authority (CA)	the parent agency for issuing digital or electronic certificates managed by the Directorate General of Informatics Applications (Kemkominfo).
Data Storage Centre	presenting IaaS (Infrastructure as a Service) which allows government agencies or agencies to be interconnected and integrated to exchange information, share resources and facilitate coordination.
Integrated Applications	Public services applications, both state and non-state administrators.
National, Regional and Multinational Cooperation	Cooperation was carried out by the Ministry of Communication and Informatics in 2019 in various forms of activities, both in the form of meetings and discussions of a special agenda on a national, regional and multilateral scale. This chapter describes the Ministry of Communication and Informatics' national and international cooperation, including UNCITRAL, ASEAN SOMRI, RCEP, ICT Minister Forum, and ITU Telecom World.

5 Conclusion

Based on the development of Indonesia's national legal instruments that have regulated various digital infrastructure sectors, and taking into account that there is a role for the government in each of these regulations, it can be concluded that the readiness of legal instruments in cyber security has been improved. However, based on the taxonomy of cyber-harms model, it is still necessary to develop a similar taxonomy for various sectors, both government and non-government sectors.

References

[1] J. jang-J. and S. Nepal, "A Survey of Emerging Threats in Cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, p. 973, 2014, doi: https://doi.org/10.1016/j.jcss.2014.02.005.

[2] CSIS, "Significant Cyber Incidents," *Strategic Technologies Program*, 2021. .

[3] Michael N. Schmitt et.al., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2017.

[4] Andrzej Kozlowski, "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan," *Eur. Sci. J.*, vol. 3, no. 237–243, 2014.

[5] J. M. Jane Hakala, *Russia's Strategy in Cyberspace*. NATO Strategic Communications Centre of Excellence, 2021.

[6] S. C. and D. U. IoannisAgrafiotis, Jason R.C. Nurse, Michael Goldsmith, "A TAxonomy of Cyber-harms: Defining the Impacts of Cyber-Attacks and Understanding How they Propagate," *J. Cybersecurity*, vol. 0, no. 0, pp. 1–15, 2018.

[7] ID-SIRTII/CC, *Laporan Tahunan 2020. Hasil Monitoring Keamanan SIber (Annual Report 2020. Cybersecurity Monitoring Result)*, 1st ed. Jakarta: Pusat Operasi Keamanan SIber Nasional, Badan Siber dan Sandi Negara, 2020.

[8] Kominfo, *Dinamika Data Aplikasi Informatika 2019 (The Dynamics of Informatics Application Data 2019)*, 1st ed. Jakarta: Kominfo, 2019.