

# Indonesia Cyber Security Development: The Analysis Of Infrastructure, Regulation And Institutional Building (2007-2015)

Elsa Faradilla<sup>1</sup>, Anak Agung Banyu Perwita<sup>2</sup>

<sup>1</sup> President University, School of International Relations, Faculty of Humanities  
E-mail: aabanyu.perwita@gmail.com

**Abstract**— The issue of current global cyber threats and attacks has been around taking International Relation study's attention. As the development of Information Communication and Technology advances, the issue of current global cyber threats and attacks becomes no longer state-level issue only. Individuals and almost all layers of community play part (government institution, education institution/community and business entity). At this point, the role of government takes the utmost important part. Government has choices to put effort in resolving the current global cyber threats and attacks, in the form of cyber security infrastructure development, implementation of the regulation or policy, and role of the institutional building that handling cyber security. This particular research centered upon the effort of Indonesia in resolving current global cyber threats and attacks by analyzing the cyber security infrastructure development, implementation of the regulation or policy, and role of the institutional building that handling cyber security. The time frame taken is from 2007-2015. Qualitative method will be used by this research in order to examine and explain the analysis in narrative order supported by some pictures and tables. The research seeks to conclude that how far the development of Indonesia cyber security in resolving current global cyber threats and attacks.

**Keywords**— *cyber security, regulations, infrastructure, policy, cyber attacks.*

## I. INTRODUCTION

Cyber security is one of the most important issues and is a challenge that must be dealt with seriously. The growth on the Information Communication and Technologies network sector is very fast which very possible the opportunist to take a chance in the middle of the cyber space which very vulnerable to crime and attacks.

Cyber security can be defined as “the collection of tools, policy, security concept, security protection, guidelines, risk management approach, action, training, best practices, assurance and the

technology that can be used to protect the cyber environment and the organization and user assets”.<sup>1</sup> The organization and user in cyber security assets, including the connected device computing, personnel, infrastructure, applications, services, telecommunication system and the totality of the transmitted and/or stored information in the cyber environment.<sup>2</sup>

Every country in the world must be able to develop the cyber security in order to withstand cyber threats and attacks from various parties who will do the espionage, tapping and destruction against various system or software. Since we do not have a world government, global efforts depend on national action. States are fundamental players in cyber security, because it holds the policy and regulation, economic and diplomatic tools.

Cyber threats and attacks appear along with the increasing knowledge on the use of information technology including computer network and internet. This raises cyber threats and attacks in the form of cyber terrorism, hacktivism and cyber warfare that carried out the attacks regardless of national boundaries. According to Libicki, cyber threats and attacks happened because the opening of the target system in the whole world and the weakness of the system that cause the system is able to exploited.<sup>3</sup>

Indonesia is currently in urgent circumstances cyber security, because of the fact that the level of cybercrime in Indonesia has reached the stage of concern.

<sup>1</sup> EdmonMakarim (2013). Indonesian Legal Framework for Cyber Security. Retrieved September 15, 2016. Web site: <http://www.nisc.go.jp/security-site/campaign2013/ajsympo2013/pdf/lecture2.pdf>

<sup>2</sup> Ibid.

<sup>3</sup> Martin Libicki. Cyber war as a confidence game, Strategic Studies Quarterly, Spring, 2011.

10 Riskiest Countries			
	TER		TER
1. Indonesia	23.54%	6. India	15.88%
2. China	21.26%	7. Mexico	15.66%
3. Thailand	20.78%	8. UAE	13.67%
4. Philippines	18.81%	9. Taiwan	12.66%
5. Malaysia	17.44%	10. Hong Kong	11.47%

Threat exposure rate (TER): Measured as the percentage of PCs that experienced a malware attack, whether successful or failed, over a three month period.

Source: SophosLabs

This paper aims at explaining the cyber threats as part of non-traditional threats in Indonesia and looks at the efforts of Indonesia's government in dealing with this issue. More specifically, this paper focuses on the development of infrastructure, regulation and institutional building in countering the cyber security threats in Indonesia.

## II. ANALYSIS

Anticipation efforts to minimize vulnerability to security and durability of information in cyber space is expected to be able to bring Indonesia to realize the security and durability of the information considering the development of information technology and communication that is very fast and the use and its utilization which is relatively high for both the internal needs of the government, local government with the public, and the local government with the business sector, and it requires the availability of infrastructure and application that is sufficient to ensure accessibility, affordability of services and the most important point is to guarantee the security and resilience information.

- The Implementation of the Regulation and Policy in Cyber Security
- The basic regulation and policy of cyber security in Indonesia:
- Electronic Information and Transactions Act No. 11/2008.
- Law No. 3 The year 2002 about the defence of the State.
- Government regulations for the organizer of the system and Electronic Transaction No. 82/2012.
- Regulation of the Defence Ministry No. 16 2010 about the organization and administration of the Defence Ministry

The emergence of those policy and regulation are to accommodate the incidents and regulate the changes which occur in the Indonesian society (to accommodate various negative behaviors and criminal acts that occurred using the Internet). Those policy and regulation are one of the efforts of the government to make the internet more regularly and controlled.

The presence of those policies and regulations were greeted positively in various circles, although there are also that opposed it. For the cons side, those policies and regulations are seen as an attempt to limit the right to freedom of expression and issued opinions and can impede creativity of someone in cyber space. For those who agree, their presences are seen as the right steps to anticipate the possibility of the misuse of the internet which is uncontrollable and can be harmful to others.

### A. The Role of Institutional Building in Handling Cyber Security

Many critics emerged from various circles, especially foreign researchers of Cyber Security related to Indonesia cyber security, such as lack of cooperation between institutions or government think-tank in the field of cyber security in their functions. Quoting the statement of Kathleen Rustici: "Indonesia faces numerous challenges in developing its cyber security capabilities, including coordinating across a large and diffuse government. Currently, the government has no coordinated strategy for cyber security..."

The strong and effective institutions are needed in carrying out the tasks and cyber security activities by referring to the specified policy. This includes the structure of the organization, the duties and responsibilities, working mechanism and monitoring. These institutions need to be realized through the study of the institutional development which followed by the steps of preparation and the formation, adjustments and/or institutional strengthening, so it provided effective institutions in support of cyber security. The institutions also must be adjusted with the needs of the implementation of cyber security, in order to make sure that the purpose of the cyber security can be achieved optimally.

### B. Coordination of Cyber Security in Indonesia

Not only with the presence of National Cyber Agency which coordinated and collaborated with National Cyber Forum. Some of the initiatives and development that have been done by the institutions or business entities in handling cyber security which can be identified until 2012 in Indonesia is as follows:

#### *Government institutions*

- The Ministry of Communication and Information has established ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure) in 2007.
- State Cryptography Agency (Lembaga Sandi Negara), State Intelligence Agency and Strategic Intelligence Agency have unit that specializes in Information Communication and Technology resources security especially related to Signal Intelligence.

- The Defence Ministry and the Indonesian National Armed Forces have the initiative to build internal cyber defence force respectively which developed continuously until this time.

*Educational institution/Community*

- Indonesia Computer Emergency Response Team (ID-CERT) was established by the community of Information Communication and Technology in Indonesia.
- Bandung Institute of Technology, University of Indonesia, Gajah Mada University, and Surabaya Institute of Technology have started to build and implement Information Communication and Technology security in academic environment respectively.

*Business entity*

- Telecommunication Industry which was pioneered by PT Telekomunikasi Indonesia (Telkom) as the owner and the management of information and communication infrastructure has been implementing the standard against network security information and communication.
- The banking industry under the construction of the Bank of Indonesia has been implementing the security system on banking information infrastructure by following Bank Indonesia Regulation guidelines and international security standards of Information Communication and Technology.
- Oil and gas industry also have implemented a security standard of Information Communication and Technology on the scope of their respective business field.

### III. CONCLUSIONS

Indonesia is currently in the urgent circumstances cyber security, because of the fact that the level of threats and attacks in the cyber space or cyber crime in Indonesia has reached the stage of concern. Indonesia establishes the first Cyber Security Center for Indonesia and establishes Disaster Recovery Center in every company, even though the implementation is still sectorial. The data network traffic in Indonesia is continuing to grow, even though not all Indonesia citizens can enjoy the high speed of internet access. Indonesian government has embracing international standard on security administration. Indonesia also has been installing of various internet security products to prevent possible, exploitation of various weakness which is owned by a system. Unfortunately, the development of technology in Indonesia can be categorized as quite slow compared to other countries in Southeast Asia; it is because of the political instability and the slow economic growth and the limited use of English in

Indonesia, as well as lack of access to telecommunication infrastructure in rural areas. Currently, Indonesia also does not have the system Internet infrastructures that centralized and have many connections to the international network. So, the development of cyber security infrastructure in Indonesia is already good enough, but still need the improvement and serious action from government.

### REFERENCES

- [1] Anak Agung Banyu Perwita (2003) Human Security dalam Konteks Global dan Relevansinya Bagi Indonesia (In analysis of CSIS XXXII/2003 No.1) Jakarta, CSIS.
- [2] Anne W. Brascomb (1986) Toward a Law of Global Communication Network, New York: Logman.
- [3] James Lee Ray (1998) Global Politics, New York: Houghton Mifflin.
- [4] Kathleen Rustici (2013) Indonesia's Cyber Security: An Opportunity for Deeper Cooperation, Center for Strategic and International Studies.
- [5] Koesnanto Anggoro (2003) Keamanan Nasional, Pertahanan Negara dan Ketertiban Umum, CSIS.
- [6] Kothari, C. R. (2004) Research Methodology: Method and Techniques (Second Revised Edition). New Delhi: New Age International Ltd
- [7] Martin Libicki (2011) Cyber war as a confidence game, Strategic Studies Quarterly, Spring.
- [8] Nazli Choucri and David Clark (2011) Cyberspace and International Relations; Toward an Integrated System, Massachusetts: MIT press.
- [9] Newton Lee (2013) Counter terrorism and Cybersecurity, Springer Science & Business Media, New York.
- [10] Saini, Hemraj. Rao, Yerra Shankar. Panda, T.C. Cyber-Crimes and Their Impacts: A Review, Ijera, Vol. 2.
- [11] The International Dimensions of Cyberspace Law: Law of Cyberspace Series, Vol.1. 2000
- [12] Tikk, Eneken (2008) Cyber Attacks Against Georgia: Legal Lessons Identified, Cooperative Cyber Defence Center of Excellence.
- [13] Troy E. Smith, Trinidad and Tobago (2012) Cyber warfare: Misrepresentation of the true cyber threat, American Intelligence Journal, Vol. 31, No. 1.

*Journals*

- [14] Ahmad Budi Setiawan. Peran Government Chief Information Officer (GCIO) Dalam Tata Kelola Keamanan Informasi Nasional, Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika Indonesia, Volume 2 No. 4, 2011.
- [15] David Putra Setyawan and Arwin Datumaya Wahyudi Sumari, Indonesia Defence Diplomacy in Achieving Cyber Security Through ASEAN Regional Forum on Cyber Security Initiatives.
- [16] Hollis, David, Cyber War Case Study: Georgia 2008, Small Wars Journal.
- [17] Sanger, David. E., 2012, Obama Order Sped Up Wave of Cyber Attacks against Iran, the New York Times: Middle East.

*Web Sites*

- [18] Agus Subagyo, Sinergi dalam Menghadapi Ancaman Cyber Warfare: <https://agussubagyo1978.files.wordpress.com/2015/08/sinergi-dalam-menghadapi-ancaman-cyber-warfare.pdf>
- [19] Arnold Wolfers, "National Security" as an Ambiguous Symbol: <http://n.ereserve.fiu.edu/010034515-1.pdf>
- [20] Australian Politics. (2013, November 20). Indonesia Demands Spying Explanation, Suspends Co-operation:

- Abbott to Respond; Shorten Invokes “Team Australia” from Australian Politics:<http://australianpolitics.com/2013/11/20/indonesia-escalates-dispute-over-spying.html>
- [21] Bachelard, M. (2013, November 18). Indonesia Recalls Ambassador to Australia Over Spying Claim from Sydney Morning Herald:<http://www.smh.com.au/federal-politics/political-news/Indonesia-recalls-ambassador-to-australia-over-spying-claim-20131118-2xr5x.html>
- [22] Brissenden, M. (2013, November 18). Australia Spied on Indonesian President Susilo Bambang Yudhoyono Leaked Edward Snowden Documents Reveal from Australian Broadcasting Corporation News (ABC News): <http://www.abc.net.au/news/2013-11-18/Australia-spied-on-indonesian-president-leaked-documents-reveal/5098860>
- [23] Citizenlab (2013) Pemaparan Infrastruktur dan Tata Kelola Internet di Indonesia: <https://citizenlab.org/>
- [24] Cyber Security Policy Making at A Turning Point, Analyzing A New Generation of Cyber Security Strategies for the Internet Economy: <https://ccdc.org/sites/default/files/documents/OECD-121116-CybersecurityPolicyMaking.pdf>
- [25] Edmon Makarim (2013). Indonesian Legal Framework for Cyber Security:<http://www.nisc.go.jp/security-site/campaign2013/ajsympo2013/pdf/lecture2.pdf>
- [26] Indonesian Defence University, Technology Perspective: National Cyber Security: [https://www.academia.edu/15208522/National\\_Cyber\\_Security\\_Technology\\_Perspective](https://www.academia.edu/15208522/National_Cyber_Security_Technology_Perspective)
- [27] Erwin Kurnia, Kebijakan Strategi Keamanan Cyber Nasional dalam Menghadapi Perang Cyber (Cyber Warfare): [http://www.academia.edu/7238257/Kebijakan\\_Strategi\\_Keamanan\\_Cyber\\_Nasional](http://www.academia.edu/7238257/Kebijakan_Strategi_Keamanan_Cyber_Nasional)
- [28] Hewlett-Packard Security Research, Profiling an Enigma: The Mystery of North Korea’s Cyber Threat Landscape. HP Security Briefing, Episode 16, August 2014. Companion report, ITU National Cyber Security Strategy Guide: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf>
- [29] Kementerian Komunikasi dan Informatika Republik Indonesia (2014) Pengguna Internet Indonesia Nomor Enam Dunia from Kementerian Komunikasi dan Informatika Republik Indonesia: [https://kominfo.go.id/content/detail/4286/pengguna-internet-indonesia-nomor-enam-dunia/0/sorotan\\_media](https://kominfo.go.id/content/detail/4286/pengguna-internet-indonesia-nomor-enam-dunia/0/sorotan_media)
- [30] Liputan6 (2014) Kecepatan Internet Indonesia Masuk Kategori Paling Lambat: <http://tekno.liputan6.com/read/2113835/kecepatan-internetindonesia-masuk-kategori-paling-lambat>
- [31] Menteri Kominfo Pada “High-Level Segment ITU Council 2008” yang Membahas Cyber Security: [http://www.postel.go.id/info\\_view\\_c\\_26\\_p\\_814.htm](http://www.postel.go.id/info_view_c_26_p_814.htm)
- [32] Mick Moore (1995) Institution Building as A Development Assistance Method: A Review of Literature and Ideas: [http://www.sida.se/contentassets/d133ef34e6244dce87574126c303ff4f/19951-institution-building-as-a-development-assistance-method---a-review-of-literature-and-ideas\\_3592.pdf](http://www.sida.se/contentassets/d133ef34e6244dce87574126c303ff4f/19951-institution-building-as-a-development-assistance-method---a-review-of-literature-and-ideas_3592.pdf)
- [33] Mike Collier, Estonia: Cyber Superpower (BusinessWeek, December 17, 2007):[http://www.businessweek.com/globalbiz/content/dec2007/gb20071217\\_535635.htm](http://www.businessweek.com/globalbiz/content/dec2007/gb20071217_535635.htm)
- [34] National Geographic Indonesia, Pusat Keamanan Dunia Maya di Indonesia: <http://nationalgeographic.co.id/berita/2013/02/pusat-keamanan-dunia-maya-pertama-indonesia>
- [35] Prof. Richardus Eko Indrajit: Enam Aspek Menjaga dan Melindungi Dunia Maya: [http://idsirtii.or.id/doc/IDSIRTII-Artikel-6\\_aspek\\_menjaga\\_dan\\_melindungi\\_dunia\\_maya.pdf](http://idsirtii.or.id/doc/IDSIRTII-Artikel-6_aspek_menjaga_dan_melindungi_dunia_maya.pdf)
- [36] Richardus Eko Indrajit. Cyber-6: Memahami Isu Keamanan dan Informasi di Ranah Maya: <http://iaii.or.id/wp-content/uploads/2015/12/Ekoji999-Edisi5-13Sep12-Cyber6.pdf>
- [37] Ronald Waas, The Deputy Governor of Bank Indonesia, presented at the Seminar of the Association of Indonesian Payment System: Prevention and handling of Crimes in electronic banking services, Jakarta 5 July 2012: [http://www.bi.go.id/id/ruang-media/pidato-dewan-gubernur/Documents/bd70f9b8109f4472a480e1ae01b5c778RW\\_050712\\_02.pdf](http://www.bi.go.id/id/ruang-media/pidato-dewan-gubernur/Documents/bd70f9b8109f4472a480e1ae01b5c778RW_050712_02.pdf)
- [38] SindoNews.com (2015) Sistem Informasi di Indonesia Tidak Aman: <http://autotekno.sindonews.com/read/967047/133/sistem-informasi-di-indonesia-tidak-aman-1424482867>
- [39] The U.S. National Security Agency (NSA) Surveillance Programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) Activities and Their Impact on EU Citizens’ Fundamental Rights: <https://fas.org/irp/eprint/eu-nsa.pdf>
- [40] Tony Burke (2013, November 20) Freeze Over Boats Disastrous, Says Tony Burke – The Australian from Melbourne Daily Star News:<http://www.melbournedailystar.com/freeze-over-boats-disastrous-says-tony-burke-the-australian/>
- [41] Zawilska-Florczuk, M. The NSA: The Impact of the Wiretapping Scandal on German-American Relations:[http://www.osw.waw.pl/sites/default/files/commentary\\_124\\_0.pdf](http://www.osw.waw.pl/sites/default/files/commentary_124_0.pdf)

