An Overview of the Development Indonesia National Cyber Security

Farisya Setiadi
Program of Information System
STMIK Indonesia
Depok, Indonesia
farisyamail@yahoo.com

Yudho Giri Sucahyo and Zainal A. Hasibuan
Faculty of Computer Science
University of Indonesia
Jakarta, Indonesia
{yudho & zhasibua}@cs.ui.ac.id

Abstract *:*

Currently, the threat for the countries will be come from cyber threats. Cyber threats potentially attack national assets and interests. Furthermore, every country needs to develop national cyber security strategies to anticipate the cyber threats. Indonesia as a country that is growing rapidly in the ICT sector has make efforts to address cyber threats. This paper describes the state of the art national cyber security in Indonesia, which is consist of five aspects, such as (1) Legal Measures, (2) Technical and Procedural Measures, (3) Organizational Structures, (4) Capacity Building and (5) International Cooperation. This paper also proposed national cyber security principles and strategies for implementation and development national cyber security in Indonesia.

Keywords-component; *NCS;National Cyber Security;Indonesia;*

I. Introduction

Information and Communication Technology (ICT) has proved positively contribute to the economic growth in every country. Positive economic growth occurs because ICT solutions as enabler of a process. It has proved that the proper infrastructure, ICT can be an enabler for socioeconomic development [1]. Examples from the developed world where significant ICT investments had major impacts include increasing the United States gross domestic product (GDP) by 7.8%, 8.0% in the UK, 8.3% in Singapore and 8.4% in Australia; all such developments were linked with improved productivity, competitiveness and citizen engagement [2].

Indonesia as a developing country, trying to develop economic country's by increasing investment in the ICT sector. Data from the Ministry of Finance of Republic of Indonesia shows an increase of approximately 18.24% or equivalent to USD 219 million in the realization of Central Government ICT Expenditure in the period Fiscal Year 2009-2010[3]. ICT growth is also felt by Indonesia people. This is shown by a high number of mobile phone users, which is about 180 million [3]. Indonesia also includes to the biggest users of social media in the worlds, facebook user third biggest in the world and the fifth for twitter users. Statistical data showed that Indonesia run into a rapid growth of ICT sector .

A rapid development in the ICT sector, gives a positive impact on economic growth and also a big threat for cyber security in Indonesia. The current threat for every country is not only come from physical threat, but also from cyber threat, because the cyber threat potentially destroying the economy and destabilize the country's security. To anticipate the threats that come from cyberspace, the government needs to develop a defense and security system and strategy.

This paper describes the current condition of system and strategy of security cyberspace in Indonesia. Explanation of national cyber security condition is consist of five pillars, i.e. (1) Legal Measures, (2) Technical and Procedural Measures, (3) Organizational Structures, (4) Capacity Building and (5) International Cooperation as categorized by the Global Security Agenda (GCA) from International telecommunication Union (ITU) [4]..

II. CONDITIONS OF CYBERSPACE AND CYBER THREATS IN INDONESIA

a. Population of Cyberspace: Mobile Phone Subscribers and Internet Users in Indonesia

Since the Telecommunications Act was adopted in 1999, telecommunications sector in Indonesia entered a new phase. The telecommunications industry is growing rapidly. Currently there are ten telecommunications operator with 180 mobile phone users. High number of mobile phone subscribers also following by internet. The growth of internet penetration in Indonesia is 12.5% or by 30 million users in 2010[3].This growth rate was lower among other Asian countries, but in terms of number, that number ranked the top in Southeast Asia Region, or the highest ranked five in Asia Region. The Indonesian government needs to work harder to increase internet users, due at the World Summit for Information Society or the World Summit Information Society (WSIS) in 2003 had declared that at least half of the world's population has internet access in 2015.

Indonesia's population is estimated approximately 255 million in 2015. In 2011 internet users in Indonesian reached 55 millions, it means government should be able to provide internet access to 70 million people. So, Indonesian government should be more aware, because the high number of internet users and internet utilization for life will increase the frequency of cyber crime. The following section will explain the threats and crimes that occurred in Indonesia.

b. Case of Cyber Threats and Cyber Crimes in Indonesia

Cyberspace crimes or known as cybercrime include identity theft and data (information resources), piracy accounts (email, IM, social networks), the spread of malware and malicious code, fraud, industrial espionage, hostage-critical information resources and cyber warfare or war in cyberspace. Convention of Cybercrime has been split into several sections, or called by typology of cybercrime [4], such as:

1) *Offences against the confidentiality, integrity and availability of computer data and systems*
2) *Computer-related offences*
3) *Content-related offences*
4) *Offences related to infringements of copyright and related rights*
5) *Ancillary liability*

The cyber crime that is attack national assets and disrupts national interest, it is called cyber terrorism, or cyber warfare. As said by Colarik cyber terrorism means premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets and definition of cyber warfare is Information warfare is defined as a planned attack by nations or their agents against information and computer systems, computer programs, and data that result in enemy losses [5]. Both cybercrime and cyber warfare have occurred in Indonesia, the cases of cybercrime and cyber warfare that possible occurred in Indonesia are Data Theft) Release of Private Data), Copyright Violation, Defacing and Patriotic Hacking.

Theft of confidential and sensitive information data via portable media such as external storage, CD/DVD, memory card is often the case in Indonesia. Theft occurs because the data is not stored with good security, or the negligence of the owner. The sample for this case is the release of private video artists in 2010, which scandalize public.

Piracy rates in Indonesia are still high, because of lack of law enforcement. Indonesia became the highest state in the rate of software piracy. This is a serious issue for the government that needs to be resolved for improving the content and software industries in Indonesia.

Geographically, Indonesia is very large and bordered with another country. This issue could be a potential conflict, because usually disputes in cyberspace begin with the ownership claims between the two countries. Claims ownership of cultural and territory and also labor issues spread to the conflict in cyberspace. Cyber conflict begins from threads in a cyber forum that blamed each other and continued by attacking the others government websites.

Above cases are the samples of cybercrime that occurs in Indonesia and there are still many other cases of cybercrime. Cybercrime cases in Indonesia are processed by the Police of the Republic of Indonesia under Special Cybercrime Unit. To handle crimes and threats in cyberspace, it is needed the efforts from the government. These efforts may include policy, strategy, system, etc that related to cyber security. The following section is an explanation of cyber security in Indonesia.

III. DIMENSIONS OF NATIONAL CYBER SECURITY IN INDONESIA

According to the ITU Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets[4]. From this definition, cyber security means a mix of components to protect the environment and assets, the components such as policy, technology, etc. ITU also categorized national cyber security into five dimensions. This section explains dimensions of cyber security in Indonesia based on cyber security agenda for development country by ITU. Dimensions were assessed from the aspects (1) Legal Measures, (2) Technical and Procedural Measures, (3) Organizational Structures, (4) Capacity Building and (5) International Cooperation.

a. Legal Measures

Government of Indonesia has conducted a series of efforts to protect cyberspace from the threat of cybercrime. One of the Government's efforts in protecting the security of information in cyberspace is by

publishing the policies and regulations. Telecommunication Act (UU Telekomunikasi No. 36/1999) and Information and Electronic Transaction Act (UU ITE No. 11/2008) are two acts that directly related to ICT security. Those acts become the basic foundation for formulating regulations and policies related to information security.

The numbers of related policies and regulation on ICT security are still very limited to protect the rapid growth of ICT sector in Indonesia. Indonesia has only two acts that describe security in the ICT sector. Compared with another countries, Indonesia lagged behind in ICT security policy and regulation, such as Malaysia that has already had computer crime act (1997), digital signature act (1997), telemedicine act (1997), communication and multimedia act (1998), payment system act (2003), personal data act (2010), etc, even other country like Slovenia have PDP act (2004) and E-commerce & E-signature act (2004) while Estonia have Estonia-Digital Signature Act (2000) and Electronic Communication Act (2004) [6].

Because of the limitations of act, criminal cases related to cyber crime in Indonesia could also be punished with criminal procedural law codex (UU KUHAP), Pornography Act (UU Antipornografi No. 44/2008), Copyright Act (UU Hak Cipta No. 19/2002), and Consumer Protection Act (UU Perlindungan Konsumen No. 8/1999). Another Cyber law that is still in the formulation stage between the government and legislative is the Information Technology Crime Act (RUU Tindak Pidana TI/TIPITI) and Multimedia Convergence Act (RUU Konvergensi Multimedia).

b. Technical and Procedural Measures

Applying the standard is an important step to protect the security of information in cyberspace. Those standards will become reference for each sector to enhance the capabilities in the field of information security. Indonesian government has been aware of it by adopting international standards on security management (ISO 27001). Indonesia National standards for security management called SNI ISO/IEC 27001:2009, which will be explained in the following sections together with existing government and community programs and activities. The following is an explanation technical and procedural measures that developed by governments and communities in Indonesia:

i. *Indonesia National Standard (SNI ISO/IEC 27001:2009:* Information Security Management System): Government of Indonesia in this regard the National Standardization Agency (BSN) has established an identical adoption of ISO 27001 become SNI ISO/IEC 27001. This standard covers all types of organizations such as commercial enterprises, government, and nonprofit organization. This standard specifies requirements for establishing, implementing, operating, monitoring, assessment, improving and maintenance of Information Security Management System (ISMS) is documented in the context of the overall organization's business risks. This standard specifies requirements for the application of security controls customized to the needs of each organization or the organization. ISMS is designed to ensure the selection of security controls are adequate and proportionate to protect information assets and give confidence to interested parties. [7]

ii. *Health and Safe Internet Program:* To optimize information security in cyberspace, Ministry of Communication and Information Technology (MCIT) has made government program called health and safe internet program. This program contains educational and public awareness about the importance of

information security. It is hoped that through this program, community in ICT sector participate in maintaining security in cyberspace.

iii. *Trust+:* Trust Positive (Trust+) is negative content filtering technology based which is developed by models and the workings of this system is to perform filtering of the top level domain, URL and Content, Keyword, Expression. Implementation Trust+ is performed in MCIT, telecommunications operators and ISPs.

iv. *Internet devices Health & Safe for Children Indonesia (Perisai):* Perisai is Open Source software designed to provide protection and education for the children of Indonesia. This software is as the result of cooperation of MCIT, Ministry of Research and Technology, IGOS Center and PC LINUX. Perisai distributed freely and easily to use by children, because the government very aware that the protection of negative content should be done early as possible.

v. *Nawala Project:* DNS filtering protection that protects internet connection from negative content such as pornography, gambling, phishing, malware, or anything harmful. This service can be used with free of charge, just by configuring DNS address in accordance with predetermined. This Project is developed by the ICT community in Indonesia to help the government enforce the laws, values and social norms.

c. Organizational Structures

Currently there are several organizations, institutions, agencies or teams involved in information security in Indonesia. Organizations established by the government or agency set up by the community. As shown in Figure 1, at the national level, MCIT has the authority in preparing the organization that handles information security sector

There are three government organizations involved in information security in Indonesia, Information Security Coordination Team, Directorate of Information Security, and Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). Comparison of the three government organizations can be seen in Table 1.

TABLE I. GOVERNMENT ORGANIZATION STRUCTURE RELATED TO ICT SECURITY IN INDONESIA [8][9][10]

	Information Security Coordination Team	**Directorate of Information Security**	**Indonesia Security Incident Response Team on Internet Infrastructure**
Legal Basis	Decree of the Minister of MCIT Number: 133/KEP/M/KOMINFO/04/2010	Regulation of the Minister of MCIT Number:17/PER/M.KOMINFO /10/2010	Regulation of the Minister of MCIT Number: 26/PER/M.KOMINFO/5/2007
Tasks and Functions	To coordinate, develop policy, develop technical guidelines, conducting awareness campaigns, and conduct monitoring and submit reports on the implementation of information security in Indonesia.	To formulate and implement policies, preparation of norms, standards, procedures and criteria, providing technical guidance and evaluation in the field of information security.	Internet traffic monitoring for incident handling purposes;Managing log files to support law enforcement;Educating public for security awareness;Assisting institutions in managing security;Providing training to constituency and stakeholders;Running laboratory for simulation practices;Establishing external and international

			collaborations.

ID-SIRTII is the first institution established by the government to handle security on internet infrastructure. The function of this organization is really crucial in ensuring the conducive environment on Internet to overcome such negative impact brought by the tremendous development of Internet into communities especially that involve intellectual property right and Internet content [10].

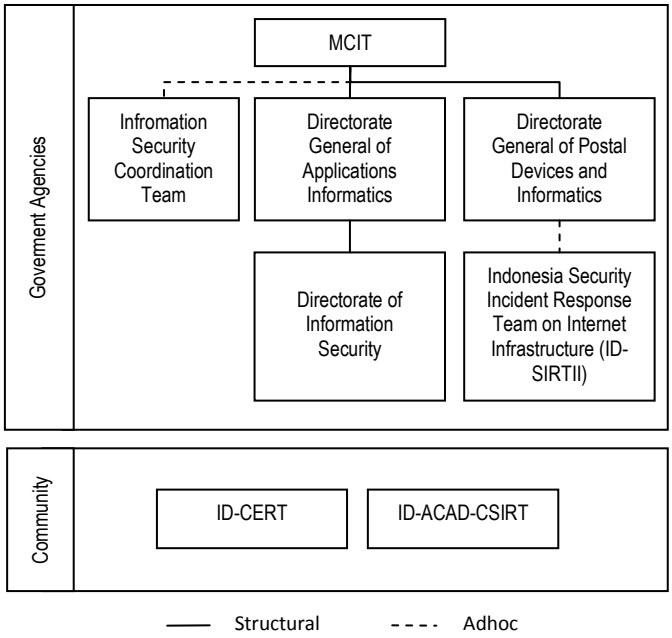

Figure 1. Organization structure related to ICT security in Indonesia

Furthermore, MCIT in April 2010 formed the coordination team of information security to accommodate the importance coordinate and collaborate in government agency. Information Security Coordination Team composed of leaders of government agencies associated with security, also experts and practitioners of information security. Still in the same year, MCIT formed of structural organization of information security called Directorate of Information Security.

Meanwhile, ID-CERT is an organization that advocates and security incident response coordination in Indonesia. ACADEMIC CSIRT (ID-ACAD-CSIRT] is an organization for the University who want to focus on the development of security in Indonesia, currently has 40 members Academic CSIRT University. ID-CERT and ID-ACAD-CSIRT even though there is no structural line with the government, those institutions continue to work with governments to support information security in Indonesia.

d. Capacity Building

Capacity building capabilities contribute in creating the information security components. The capacity can be gained through human resource development, organizational development, and institutional and legal framework development. Here are the efforts made by the government to develop capacity in the information security aspects.

i. *Indonesia's National Work Competence Standards (SKKNI) Sector Information Security:* To improve the capacity of human resources in the areas of information security, MCIT in cooperation with experts from academics, government and the private sector have developed a standard framework of competence in information security that is called SKKNI Sector of Information Security. This standard is used to provide guidance in identify and categorize the positions and certification of personnel who perform information security functions that support the organization's which implementing information security.

ii. *Information Security Index (KAMI Index):* To measure the maturity of information security in government agencies, MCIT released the program of Information Security Index (KAMI Index). KAMI Index is an annual program from Directorate Information Security MCIT that measures the Information security within government agencies as measured in five aspects, (1) Governance, (2) Risk Management, (3) Framework, (4) Asset Management, (5) Technology. The purpose of this activity to map the maturity level of information security in the public service providers in accordance with SNI 27001[11].

e. *International Cooperation*

Politically, Indonesia has free and active principle, it is stated in the preamble of the constitution. Indonesia has collaborated with international parties on the issue of cyber security. For cyber security international cooperation, Indonesia has become a Full Member of the Asia Pacific and APCERT FIRST (Forum for Incident Response and Security Team) of the world. Indonesia also has become a Full Member and founder of the OIC-CERT (Organization of the Islamic Conference-CERT).

International cooperation can also be interpreted in an effort to participate or agreed to an international agreement. Currently, Indonesia is trying to ratify European Union of Convention of Cybercrime. This Convention held on 23 November 2001 in Budapest, Hungary. The meeting intended to discuss thoroughly the threats facing the international world of cyberspace-related crimes. This convention has been agreed that the Convention on Cybercrime included in the European Treaty Series No. 185.

IV. STRATEGIES OF THE DEVELOPMENT INDONESIA NATIONAL CYBER SECURITY

The Indonesian government should develop national cyber strategy to protect national assets and cyber space environment. The strategy is created to ensure and alignment process within government agencies. The strategy must have principles:

i. *Leadership:* Complexities and challenges of cyber security in Indonesia need powerful leadership. The Leaders must recognize and responsible with the importance of cyber security in their agencies.

ii. *Shared responsibilities:* Cyber security requires a shared responsibility, because the use of ICT is related to each others. Each agencies must maintain their sensitive ICT resources.

iii. *Partnership:* To create a cyber security, it is required the cooperation and partnership from the various parties.

iv. *National Values Impact and Risk Management:* Applying a business impact analysis approach for national asset and risk management. This approach aims to prioritizes the protection of the national assets and critical ICT resources.

v. *International Cooperation:* Cyber crime is a transnational crime, therefore the government should cooperate actively with foreign parties to protect the national asset.

According to above principles, below are the strategies that should be considered by Indonesian government to improve national cyber security:

1) *Create and alignment cyber security regulations:* A Regulation is a basic foundation to protect cyber environment. A regulation also must be alignment with other laws. It must be developed and revised regularly to anticipate rapid technology development. Further is the commitment of all parties for law enforcement

vi. *Strengthen the roles, responsibilities and authorities of cyber security government organizations:* To solve the problems of cyber security in national level, it is needed cooperation and collaboration with academics, governments, business organizations and communities. Therefore, at the strategic level there must be an organization that responsible to supervise and coordinate cyber security organization. This organization must be supported by the highest authorities in the national level, politically and technically. At the operational level, the country also needs technical agencies to handle incident management in each sector. All of the cyber security organizations must have clear roles, responsibilities and authorities. It is very important part, because all of complex problem of cyber security can be solved only by powerful organization and mutual cooperation,. The cyber security organization also needs the human resources who have integrity and ability in cyber security

vii. *Improve cyber security human resources*: Training and skill development are needed to improve quality and to increase quantity. Government agencies can develop their human resources by do cooperation with universities and training institutions

viii. *Development application, systems and technologies security standard.:* The autonomy on developing application, system and technology are needed to protect the country from internal and external cyber threats. But, it must be standardize and evaluate regularly.

ix. *Improve security awareness and governance:* Introducing risks that exist in cyberspace will raise the awareness about the importance of cyber security. The efforts to develop awareness can be done through campaign, dissemination and publication program. Implementation of security governance is also important part. It can be adopted from national standard or international best practices of security governance standard.

V. CONCLUSIONS AND FUTURE WORKS

ICT growth in Indonesia gives impact on a high cyber threats. Indonesian government has tried to address that problem by issued policies and regulations, developed technical and procedures, established organization security, improved capacity building and conducted international cooperation.This paper shown that Indonesia had many efforts to anticipate and protect cyberspace. This paper also propose principles and strategies to improve national cyber security in Indonesia. Therefore, further work is to determine the ideal conditions for cyber security in Indonesia, futhermore by understanding the current conditions and the ideal conditions we can view the gaps that might be improved

REFERENCES

[1] S. Kamel, D. Rateb, and M. El-Tawil, "The Impact Of ICT InvestmentsOn Economic Development In Egypt," Electronic Journal on Information Systems in Developing Countries., vol. 36, no. 1, pp. 1-21, 2009.

[2] S. Bhatnagar, "ICT Investments in Developing Countries: An Impact Assessment Study, Information Technology in Developing Countries," Newsletter of the IFIP Working Group 9.4., vol. 15, no. 2, pp. 1-8, 2005.

[3] Pusat Teknologi Informasi dan Komunikasi BPPT, "Seri TIKOMETER Indikator Teknologi Informasi Dan Komunikasi Edisi 2011,". 2011

[4] International Telecommunication Union (ITU), "Understanding Cybercrime: A guide for Developing Countries,", 2009.

[5] A. M Colarik, and L. J. Janczewski "Cyber Warfare and Cyber Terrorism. Information Science Reference. Hersey, New York. 2008

[6] M. Lubis, F. A. Maulana, "Information and Electronic Transaction Law Effectiveness (UU-ITE) in Indonesia," Proceeding 3rd International Conference on ICT4M. 2010.

[7] Badan Standarisasi Nasional. Teknologi Informasi-Teknik Keamanan-Sistem Manajemen Keamanan Informasi-Persyaratan. SNI ISO/IEC 27001:2009

[8] Ministrial Communication and Information Technology Republic Indonesia Decree. Information Security Coordination Team. No. 133/KEP/M.KOMINFO/04/2010.

[9] Ministrial Communication and Information Technology Republic Indonesia Regulation. Information Security Coordination Team. 17/PER/M.KOMINFO/10/2010.

[10] Ministrial Communication and Information Technology Republic Indonesia Regulation. Information Security Coordination Team. 26/PER/M.KOMINFO/5/2007.

[11] Ministrial Communication and Information Technology Republic Indonesia Regulation. Information Security Index for Public Services Agencies. 2011