Mapping on Cyber Threats in Indonesia Related to Indonesia's Cyber Security Agenda

Y C Mahendra[1], N K D S A Pinatih[2]
[1,2]Universitas Brawijaya, Malang
[1]masmahe@ub.ac.id, [2]d.pinatih@ub.ac.id

ABSTRACT

This paper aims to give a comprehensive analysis about the mapping of cyber threats in Indonesia. Indonesia is well known as a country with millions of Internet users. This fact is combined with the rise of cyber activities, making Indonesia vulnerable to cyber threats. This is a multi-year research which tries to identify the cyber threats in Indonesia and how the government attempts to tackle it while pursuing the cyber security agenda in Indonesia. Interestingly, in International Relations Studies, cyber security is commonly discussed both in traditional security studies and non-traditional security studies, which makes the studies more dynamic and complicated.

Keywords: *Cyber Threats, Cyber Security, Security Studies*

1. INTRODUCTION

It is generally known that cyber space activities cannot be separated with the rise of the information technology. Everyday people tend to rely more on the Internet to support their activities. Talking about Internet activities is just like talking about two sides of a coin and each coin has positive and negative sides. In positive aspects, the usage of the Internet helps people to manage their business, support online transactions such as Internet banking and online stores. Moreover, Internet also helps us to communicate with people who live in another part of the world. On the other hand, cyber world is a fragile space where criminal activities like hacking, scamming and stolen identity happen. Furthermore, there is a concern about the degree of information credibility and the user privacy when it comes to Internet activities. This fact is contrary with the spirit of information transparency which is based on the cyber world which is initiated by the government.[1]

Regarding to the overview mentioned earlier, it is important for us to put more attention to cyber threats, thus the recognition and identification of the cyber threats become inevitable, both from the society and government perspectives.[2][3] Because the threats that challenge the people also considered as a national threat to the state. By considering that approach, this paper tries to describe three main aspects: First, the identification of the various kinds of cyber threats in Indonesia; Second, the analysis of the cyber threat phenomena using the cyber security approach; and the third, the relationship between the transformation of cyber threats with Indonesia's cyber security.[4][5][6]

2. RESEARCH METHOD

This paper uses the descriptive method as approach that focused on deep collecting data from primer and secondary objects. Regarding to the research method, the data collection was

B-SPACE 2019, November 26-28, Malang, Indonesia
Copyright © 2020 EAI
DOI 10.4108/eai.26-11-2019.2295212

conducted on in-depth interview to selected respondents from various government institutions such as Criminal Investigation Division of Indonesia’s National Police, International Police Branch in Jakarta, and State’s Cyber Agency.

3. RESULTS AND DISCUSSION

At the international level, cyber threats have been understood as one of the issues of global security given that many large-scale businesses and administrations are controlled in cyberspace which is very vulnerable to damage caused by viruses created by hackers. To respond to this, several countries in Asia, Europe and North America see some diplomatic opportunities to form elements of cyber policy in international security, which is created by allocating large budgets and resources. For this reason, shared perceptions about cyber security seen as complex realities with various dimensions need to be redefined. According to Joseph Nye, there are four different categories in cyber threat, all of which form the pillars of cyber insecurity. The first is cyber-crime, the second is cyber espionage used for traditional or industrial espionage, the third is cyber terrorism, and the last is cyber warfare.[7][1]

The existence of cyber threats causes an increase in serious risks to the economy as well as national and international security. As explained by Caitríona H. Heinl in Regional Cyber Security: Moving Towards a Resilient ASEAN Cyber Security Regime,[8] a number of regional and international organizations and institutions are currently dealing with cyber security issues, although at different levels, one of which is ASEAN.[8] ASEAN is a strategic region, especially related to international cyber security issues. Why is ASEAN so strategic about cyber security? First, ASEAN's centrality in regional architecture in the wider region of Asia Pacific and its potential as an important neutral party in terms of international cyber security cooperation. Second, although there are gaps in access to information technology in countries in the Southeast Asian region, their development shows an increasing trend. Based on the Impact Assessment report from the European Commission in 2013, it is mentioned that out of 2.1 billion Internet users in the world, the majority were in Asia (922.2 millions). The average population growth in ASEAN countries is higher than the average in Asia for the period of 2010-2015, which increases the possibility of the increasing demand for the use of Information and Communication Technology (ICT).

Geographical proximity that has implications for the close connectivity between ASEAN countries increases the potential for transnational crime and cross-border challenges related to cyber such as cyber threats and cyber incidents. There are various levels of ICT development and adoption throughout the ASEAN region where efforts are being made to "bridge the digital gap" to promote greater ICT adoption.[9] Three ASEAN Community blueprints are aligned with the Initiative for ASEAN Integration (IAI) and the Hanoi Declaration on Efforts to Narrow Development Gaps for Closer ASEAN Integration, which aims to narrow development gaps and provide assistance to Cambodia, Laos, Myanmar and Vietnam (CLMV) to meet targets and commitments throughout ASEAN to realize the ASEAN Community. ASEAN Regional Forum (ARF) must implement capacity building and technical assistance measures by developing assistance programs, trainings and technical assistance, all of which strengthen cyber security capacity and capabilities in crisis management in all countries.

To achieve a more comprehensive order for cyber security throughout ASEAN, member countries must develop and implement cyber security framework with future visions as soon as possible to coordinate cohesive regional cooperation and collectively address global cyber security challenges. Some steps and tools that can be considered to create a comprehensive and multidimensional cyber security framework include: establishing permanent coordination mechanisms, including regional coordination & information sharing; building strong ASEAN-CERT by further enhancing and strengthening operational cooperation & sharing National CERT information; ensuring adequate security from institutions especially ASEAN, creating superior cyber security networks in the regions, including trainings & capacity building; ensuring safe supply chains & regional harmonization to international standards: "cyber-safe zones";[10] raising public awareness & the protection of civil liberties: citizen involvement, increasing defense cooperation & law enforcement coordination for coordination related to cyber threats; approving a joint position on responsible state behavior; and the enactment of international law, strengthening international cooperation.

For Indonesia, the development of the number of Internet users in Indonesia is certainly offset by the development of cyber threats. In 2002 the number of Internet users in Indonesia only reached 4.5 million people, but referring to the fact that this number did not guarantee the number of cyber threats in Indonesia would not be taken into account. Referring to Tata Consultancy Services data, Indonesia is the country, with the second highest credit card fraud in the world in that year with a percentage rate of 18.3% below Ukraine with 19%. The percentage is calculated based on the total amount of loss on a global scale due to credit card fraud estimated at 2.5 billion US Dollars. So, basically the rapid development in the ICT sector in addition to having a positive impact on economic growth, it is also a major threat to Indonesia's cyber security in accordance with the given case.

The threat of cyberspace has the potential to destroy the economy and disrupt the stability of the country's security. In order to anticipate threats that come from cyberspace or cyber threats, the government needs to develop defense and security systems and strategies in the form of the adoption of the Telecommunications Law adopted in 1999 (Telecommunications Law No. 36/1999). However, this still cannot optimally resolve the development of cyber threats in Indonesia. The development trend of cyber threats in Indonesia initially dominates the banking sector as in the previous example, but in a broad scope, these actions could be categorized into hacking categories. Hacking itself according to the United Nations Office on Drugs and Crime (UNODC) is a category of cyber crime in the form of illegal access to computer systems remotely.[11] The access aims to obtain data or information in order to obtain benefits.[11] The trend periodically, according to a report from McAfee (2010), at least continued until 2005 which integrated with the spread of adware, spyware, rootkits, and botnets.

The spread of these forms of malware is intended to generate profits by stealing important data about financial information and damaging the computer system that has been built.[12] That period is also identified with the development of Distributed Denial of Service (DDoS), macro viruses, identity theft via Wi-Fi networks, and dangerous MP3 files.

The continuing trend of cyber threats in Indonesia entered a new period from 2006 to 2008 when cyber criminals began to form groups and act in a more organized manner. During this period, the trans-nationalization of cyber crime in Indonesia became increasingly apparent. This was proven from 55 reports from 17 countries that entered the Cyber Crime of the Indonesian National Police Headquarters (Mabes Polri) in the period 2006 to 2008.[13] The complexity of the types of cyber crime after the 2010 period made it more difficult to categorize cyber crime. In relation to the cyber crime itself, especially in finance and trading, the number of losses that have emerged in the last few years shows quite numerous figures. The losses incurred due to cybercrime in the Indonesian banking sector reached Rp 33.29

billion until 2014. According to the Criminal Investigation Police (Bareskrim Polri) the amount was far greater than conventional bank customer robberies.

To overcome problems related to cyber crime, several efforts need to be made including the making of policies, strategies, systems and all matters related to cyber security. According to ITU (International Telecommunication Unit), cyber security is a collection of tools, policies, security concepts, security protections, guidelines, risk management approaches, actions, training, practices, guarantees and technology, which can be used to protect the environment of cyber institutions and user assets. There are five dimensions of cyber security in Indonesia based on the cyber security agenda for developing countries by ITU, namely: legal steps, technical and procedural steps, organizational structure, capacity building, and international cooperation.

First, legal steps. The Indonesian government has made a series of efforts to protect cyberspace from the threat of cyber crime. One of the efforts is by making the Telecommunications Law (Telecommunications Law No. 36/1999) and ITE Law No 11/2008.[14] Both of these regulations form the basis of policy making and regulations related to information security. However, ICT policies and security regulation that are owned are still very limited in protecting the growth of the ICT sector in Indonesia. Due to the limitations of legislation regarding cyber, cyber crime in Indonesia can be adjudicated using procedural law of other criminal acts. Second, Technical and Procedural Steps. Indonesia has adopted international standards related to security management namely ISO 27001. Meanwhile, national standards in security management are called SNI ISO / IEC 27001: 2009[15], which covers all types of organizations including commercial companies, governments and non-profit organizations. Third, related to the organizational structure in which there are several organizations, institutions, agencies or teams involved in information security in Indonesia, namely the Security Coordination Team, the Directorate of Information Security, and the Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). ID-SIRTII is the first institution established by the government to overcome the security of internet infrastructure. Fourth, capacity building. Capacity building contributes to the creation of an information security component that can be obtained through human resource development, organizational development, and institutional and legal framework development. Several actions that have been done by the Indonesian government are the formation of the SKKNI and the KAMI Index.[15] Fifth, international cooperation; in the international cooperation related to cyber security, Indonesia has become a permanent member of Asia Pacific and APCERT FIRST.

To deeper the discussion in this paper the authors include the results of interviews from several institutions that have a concern on cyber issues. The first is INTERPOL Indonesia which has the authority only as a liaison between INTERPOL of other countries with the Indonesian police, not as an actor who has direct authority in the action or the handling of cyber crime problems. At present Indonesian INTERPOL focuses on cases of human trafficking, specifically for the purpose of prostitution. The cyber threat that is currently being worked on is about the use of cyberspace in the case of human trafficking. In this case, Indonesia is one of the hub countries in the human trafficking network; that is why the use of the Internet through computers, especially through gadgets is a new modus operandi in the issue of human trafficking in Indonesia, the same as the case of online prostitution in the early 2019 even though the case has a domestic coverage with local users. But in fact the case being investigated is the existence of networking with foreign countries as in the case of Serbs mentioned earlier.

Second, the Criminal Investigation Police (Bareskrim Polri) which specifically has a special directorate to deal with cyber crime, namely the Directorate of Cyber Crime (Direktorat Tindak Pidana Siber) which was previously known only a Cyber Crime Sub Directorate (Subdit Cyber Crime). The Directorate, which has been established since 2017, is responsible for dealing with ITE (Information and Electronic Transaction) crimes, which include the crime of using a computer either as a primary tool or as an assisting tool. In many cases today, electronic crimes are not only computer-based but also include the use of Internet-connected gadgets. According to the Head of the Collaboration Unit of Directorate of Cyber Crime of the Criminal Investigation Police, the directorate is only a law enforcement unit for the problem of cyber crime in Indonesia if the cyber case has entered the stage of a criminal act, while the institution that has great authority in cyber issues is the BSSN.

Third, BSSN is an institution that has full authority on the issue of the cyber world in Indonesia. This institution is still relatively new in Indonesia because it was established in 2017 through Presidential Regulation (Perpres) No. 133 Year 2017.[16] This institution has a relatively complete function compared to the two previous institutions, namely the function of detecting, preventing and maintaining cyber security in Indonesia. In dealing with cyber threats that occur in Indonesia, BSSN itself has a platform called the Cyber Threat Intelligence Platform (CTI) which is used to detect cyber threats that occur in various parts of the world. CTI can detect the actors or the perpetrators of the threat, either the government of a country, hackers created by the government of a country, and hacker activists. In addition to detecting actors from the aforementioned threats, CTI can also detect the intended motives of the perpetrators who spread the cyber threat itself. However, not only CTI, Indonesia through BSSN also has an Instruction Detection System (IDS) which serves to prevent cyber threats that attack Indonesia.

4. CONCLUSIONS

The preventive approach on how to tackle cyber threats can be developed in two different aspects namely : Suprastructure and Infrastructure. Suprastructure is related to the holistic approach of cyber security for example cyber literacy, cyber science, and cyber access, while infrastructure is more related to the hardware and software preparedness of Indonesia's cyber security agenda. This also markes Indonesia's dependence to othercountries' cyber infrastructure like satellite access that leads to Indonesia's will to become an independent cyber security state.

Meanwhile, Indonesia is also challenged by the rise of the cyber era where almost all of the Indonesian people's activities now rely more on cyber world. Even tough the government has already formed a state's cyber agency but the duty to tackle the cyber threats is not solely the government's responsibility. It is also noted the urgency of the integrated cyber security bodies that involve both government and non-government actors to solve this issue

REFERENCES

[1] L. Hansen and H. Nissenbaum, "Digital disaster, cyber security, and the copenhagen school," *Int. Stud. Q.*, 2009.

[2] J. Arquilla and D. Ronfeldt, "The Advent of Netwar (Revisited)," *Networks netwars Futur. Terror. crime, militancy*, 2001.

[3] A. Karatzogianni and A. Robinson, *Power, resistance and conflict in the contemporary world: Social movements, networks and hierarchies*. 2009.

[4] H. Yeli, “Institute for National Strategic Security , National Defense University A Three-Perspective Theory of Cyber Sovereignty Author (s): Hao Yeli Source : PRISM , Vol . 7 , No . 2 , THE FIFTH DOMAIN (2017), pp . 108-115 Published by : Institute for Nationa,” vol. 7, no. 2, pp. 108–115, 2017.

[5] A. Karatzogianni, *The politics of cyberconflict*. 2006.

[6] A. Karatzogianni, *Cyber conflict and global politics*. 2008.

[7] F. G. Cempaka Timur, “The Rise of Cyber Diplomacy ASEAN’s Perspective in Cyber Security,” *KnE Soc. Sci.*, 2017.

[8] C. H. Heinl, “Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime,” *Asia Policy*, 2014.

[9] J. Eriksson and G. Giacomello, “The information revolution, security, and international relations: (IR)relevant theory?,” *Int. Polit. Sci. Rev.*, 2006.

[10] K. Krause, M. Williams, K. Krause, and M. Williams, “Security and ‘Security Studies,’” in *The Oxford Handbook of International Security*, 2018.

[11] UNODC, “The Globalization of Crime: A Transnational Organized Crime Threat Assessment,” *Secretary*. 2010.

[12] K. Krisman, “A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation,” *JAS (Journal ASEAN Stud.*, 2013.

[13] D. G. D. R. M. Ilham Panunggal Jati Darwin, “PERAN KEPOLISIAN DALAM PENYIDIKAN TINDAK PIDANA PENYEBARAN BERITA BOHONG (HOAX),” *J. POENALE*, 2018.

[14] A. E. Atmaja, “Kedaulatan Negara Di Ruang Maya: Kritik UU ITE Dalam Pemikiran Satipto Raharjo (State Sovereignty In The Mayan Room: Criticizing UU ITE In Satipto Raharjo Thought),” *J. Opinio Juris*, 2014.

[15] I. Afrianto, T. Suryana, and S. Sufa’atin, “Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI - SNI ISO/IEC 27001:2009,” *J. Ultim. InfoSys*, 2015.

[16] CNNIndonesia/Christie Stefanie, “Mengenal Badan Siber dan Sandi Negara Bentukan Jokowi,” *Nasinal*, 2018. .