4th Asia Pacific Conference on Contemporary Research (APCCR- 2018),
Bali, Indonesia
ISBN :978-0-6481172-9-2
Asia Pacific Institute of Advanced Research (APIAR)
www.apiar.org.au

# BUILDING CYBER SECURITY IN SOUTH EAST ASIA THROUGH MULTILATERAL COOPERATION

Iqbal Ramadhan
Universitas Pertamina, Jakarta, Indonesia.
*Corresponding Email*: iqbal.ramadhan@universitaspertamina.ac.id

**Abstract**

Cyber security is a new form in security studies which emerges with the rapid development of internet communication and technology. Prior to this, security studies in the past was focusing its research on traditional issues such as military and political security. After the end of Cold War, security studies became wider and deeper, especially when contemporary issues such as human, economic and environmental security were playing their role as important as traditional issues. Cyber security, as part of security studies has started to be ASEAN's concern after the implementation of Asian Economic Community. This community was built on top of ASEAN ICT Masterplan which encouraged all ASEAN member to enhance cooperation in cyber security. To secure South East Asia's cyber space, the ASEAN member should implement multinational cooperation to contain any threat that can jeopardize the stability of this region. Cyber security is not a traditional security issue which can be solved by relying on nation-state's self-help system. The threat that come from cyber space has already been institutionalized which means all states are admitting it as their common problem. As in South East Asia, multilateral cooperation can lead to development of norms, ethics, framework and policies on how to address problem in South East Asia's cyber space. Most importantly, this cooperation should unite a wide gap between fast ICT developing countries and those who do not in South East Asia.

***Keywords*:** ASEAN, Cyber Security, Multilateral Cooperation, South East Asia.

## 1. Introduction

It is obvious that the world today has been interconnected. All the cyber world has been an unseparated part from human's life. The cyber world is vast and borderless and sometimes it refers to wild west movie which indicates its untamable world. We all understand that cyber space is an infrastructure backbone in modern world. It gives humanity a benefit and of course cyber world provides a threat. One of biggest consultant firm, Pricewaterhouse Cooper (PwC), had released a research regarding cyber security in 2014 (PwC, 2014). They examined that there were increasing numbers of cyber attacks in 2013. Those numbers rised up to 23 percents in the next year. They also predicted the attack may likely to happen more often in the future. The problem of cyber security is no longer technical, but it involves the role of nation-state.

Nation-states are relying and cannot put aside the effectiveness of cyber space. They mostly used it in their daily life including the defense system. In the military aspect, there is a term called *cyber defense*. North Atlantic Treaty Organization has included cyber defense as part of collective defense policy. As for logical reason, NATO explained that a threat does not come in pyhsical form but also in cyber form. NATO believes a rogue actor such as terrorist groups or "evil state" can use this highly sophisticated technology to cripple critical sector like energy, electricity, water and banking system (NATO, 2014). For the first time in its life, NATO prioritized the cyber security after Estonia suffered from cyber attack in 2008.

In some research, Jonathan D. Aronson described that the development of technology has pushed globalization closer than before. The sign of globalization can be seen from internet utilization massively, dispersion of smartphone, and the absence of state border in cyber space (Aronson in Bayliss, 2005). Nevertheless, this development also has an impact toward national security. There are three consequences which need to be solved by nation-state like security problems, the transformation of government practice into *e-government*, and economic growth who relies heavily on cyber space (Aronson in Bayliss, 2005). From the perspective of security, Aronson explained that nation-states face a serious matter to protect their security. The threat in cyber world could possibly come both from state or transnational actor such terrorist group and even an individual.

The South East Asian countries which are joined in Association of South East Asian Nation (ASEAN) cannot put a blind eye on this issue. Based on ASEAN ICT Masterplan 2012, all the members of ASEAN should provide sharing information and implement highly effective cooperation in cyber security. The main purpose of this masterplan was designed to establish mature cyber security systems which were needed to sustain the economics backbone in ASEAN Economic Community (AEC). Another source that can be identified that International Telecommunication Union (ITU) released its research showing the maturity and cyber awareness in Asia-Pacific. The research shows that Australia, New Zealand and Malaysia reached the top three level with an index, 0, 7647. In South East Asia region, the top three level were Malaysia (0,7647), Singapore (0,6765) and Indonesia (0,4706). The fourth and fifth place were obtained by Thailand (0,4118) and Brunei with 0,3824 (ITU, 2015). Meanwhile, the ranks were followed by Myanmar (0,3824), Phillipines (0,3529), Vietnam (0,3235) and Cambodia (0,1176). It is very clear that there is a huge gap between ASEAN members in cyber security.

Discussing the cyber threat, there are several things that needs to be contained by ASEAN countries. The first threat is *cyber espionage*. This activity is not new in security studies. The espionage has been done since the Roman Empire to Cold War. Nation-states can deploy easily both their spy agent and spyware (a modified malware which is designed to steal information through Internet) for gathering the information they needed. Another matter that likely to occur is *hacktivism*. The Anonymous is very notorious for doing this kind of activity. They hack, deface and shut down nation-state's Internet system if the group thinks an official government has conducted a crime against humanity. Meanwhile, the ASEAN countries should prepare for the new form of war, called *cyber war*. Last one, an organizational crime embraces this technology to conduct their operation. They often develop a malware to steal money from bank accounts or hiding their hideous crime such as drug dealing, human trafficking or child pornography (Aronson in Bayliss, 2005).

Looking from the cyber threats above, there are many things that needs to be done. The research questions which is trying to be answered is, would it possible for the ASEAN countries to protect their national cyber security by depending on self-help ability and on the other side they have to close the gap between them?

## 2. Theoritical Approach

To answer the research questions below, theoritical approach is needed as an analytical tool.Security studies in International Relations was born by the intellectual womb of Copenhagen Scholar. Thus, it is no a surprise when most of IR scholars tend to relate the security studies as a part of Copenhagen School. This approach introduces several concepts which mainly are being used to comprehend security issue. Those concepts are *threat, vulnerability, referent object,* and *sector*. Threat defines as an action to degrade the quality of life. Meanwhile, vulnerability is the incapacity to avoid danger, or to be uninformed of impending threat.Referent object is described as a unit who is likely to be threatened. As for sector, it is defined as diversified agenda in security that is ranged from *military, political, economics, societal* and *environmental* (Buzan, Weaver and Wilde, 1998).

The author also uses *Regional Security Complex Theory* (RSCT) from Barry Buzan. Region consists with security issues which are connected within the states inside. This is due to the nature of the security itself where it is often interdependent. One state security issue inside a region are linked and cannot be separated each others (Buzan and Weaver, 2003). The term of RSCT can be defined as '*a set of units whose major processes of securitisation, desecuritisation, or both are so interlinked that their security problems cannot reasonably be analysed or resolved apart from one another'* (Buzan and Weaver, 2003). The problem of cyber security in South East Asia surely is not a matter of one state. Thus, it is a matter of states who are living in it.

Regional Security Complex Theory (RSCT) is useful for main three reasons. First, it tells us something about theappropriate level of analysis in security studies, second it can organiseempirical studies, and, third, theory-based scenarios can be establishedon the basis of the known possible forms of, and alternatives (Buzan and Weaver, 2003). Also, RSCT provides four area of studies linked with security issue. This theory can identify domestic aspects of states within the region and what cause the vulnerability. Second, it also can be harnessed understanding state-to-state relation inside the region. On the other hand, RSCT explains on how region's interaction with neighbouring region. For example, the researcher of security studies may be able to make a comparative study of security issue in South East Asia and its relation toward South Asia. Last one, RSCT emphasizes on the interaction of global power inside world region. The example is shown on the role of USA in Middle East for crippling the terrorist group (Buzan and Weaver, 2003).

Defining the pattern of interaction between ASEAN countries, liberal institutionalism is suitable to it. Proponents of neoliberal institutionalism argue that based on increasing interdependence and shared mutual interest. To minimize risking uncertain conditions, states promoteactivities with neighbors most commonly through the creation of stable,formal rules and norms. Based on these norms and rules, institutionsfacilitate the enforcement of agreement, consultation and coordination,the exchange of information, and the pursuit of a common cause (Paul, 2012). This theory will be utilized to address how ASEAN should respond to cyber security issue.

## 3. Analysis

To understand their cyber security problem, ASEAN countries should identify the threats first. The example of threats have been explained in the previous chapter such as cyber espionage, hacktivism, cyber war and organizational crime. Those threats are imminent and can be occured in any states within ASEAN. Many accidents had happened, yet some of them evaporated. In 2013, Malaysia and Singapore suffered from cyber attacks. The Malaysia government had lost $265.7 million caused by online scams. They also indicated that almost 70 percent crimes in that country categorized as cyber crimes. Meanwhile in the same year, Singapore had suffered $1 billion which in 2013 was four times the global average and twice the figure set 12 months earlier (Yao, 2015). The South East Asia is a hotbed for digital growth and innovation. As the experts predict that this region will hit $200 billion internet economy by 2025. Nevertheless, Malaysia, Vietnam, and Indonesia have been monitored due to the recent malicious activity (Choudory, 2018).

It is evidently clear that cyber crime is the biggest problem thatwould disrupt the internet economy in ASEAN. On the other hands, the ASEAN countries not only identify the threats but also their vulnerability. There is a huge gap among ASEAN members in cyber security awareness. Singapore is the most mature country in South East Asia who has already developed their system and is not overtaken by other members of ASEAN. Due to its maturity, many IT companies choose Singapore as their hub not only for expanding their market but also strengthen national capability in cyber security (Yao, 2015). Even an IR scholar like Kenneth Waltz argued that after the downfall of Cold War, state must develop technological advancement in order to survive (Waltz, 1993).Unfortunately, ASEAN members are not only Singapore. They have their own capability which is much lower. This is the vulnerability. The vision of ASEAN in AEC is to integrate the market. It means if there is

an attack to a vulnerable ASEAN member, eventually it can disrupt the whole market. This vulnerability is exist due to the lack of strong data breach notification law in ASEAN countries. As for the result, many of the members tend to invest in cyber security on very small amount of budget. The total investment of ASEAN in cyber security was only $1.9 billion in 2017. The experts argued that ASEAN should invest more (Choudory, 2018).

Based on RSCT, the author uses this theory to analyse level of analysis. The author posits the level of analysis on state-actors (ASEAN members) and the institution of ASEAN itself. Implementing an empirical study is necessary to comprehend the complexity of cyber security in South East Asia. Hence, the author utilizes RSCT's assumption to find a suitable theory for analyzing the issue. As for the area of studies, state to state relations will be used as a part of analysis. From the regional perspective, South East Asia faces an imminent threat from cyber space. They also have a vulnerability where most of its members have a huge gap of cyber security awareness. Not to mention that there is a lack of data breach law notification among its members and the investment to prevent a calamity is under-invest.

Barry Buzan postulated that major proses of securitization and security problem cannot be separated each others. It means that every sector of security are interlinked. An attack from cyber space can disrupt not only the information system, but also othersectors which are dependant on it. Financial and banking systems nowaday are connected to the cyber space. Even government conducts its daily practice using the Internet. One massive cyber attack to the ASEAN countries can jeopardize the entire regional stability.

The impact of this attack is no longer disrupting the economic system, but also political stability. It is very impossible to rely on state's self-help ability. Within the region, there are core and periphery state. The core state such as Singapore or Malaysia have a sophisticated technology and able to help themselves if there is any disruption. On the second hand, periphery state such as Cambodia will be having a difficulty to implement cyber security awareness. Cambodia sometimes has to struggle establishing good governance system in its domestic life. The ability to protect the national cyber security is vary among the ASEAN countries. Old thoughts of realism who were saying nation-state should help themselves is obsolete. Some aspects may require nation's self-help capability. Unfortunately, cyber security is not a matter of one single country. As long as AEC is still integrated with information system, cyber security is a problem of region with the states who live in it.

The state to state relations in South East Asia is non-intervention. The code of conduct is written in the mission of ASEAN itself. Though it will be so hard to solve the humanity case such as Rohingya using non-intervention policy, the enigmatic case of cyber security will be different. From the author's point of view, cyber security is related with the stability of economics growth where most ASEAN countries heavily depend on it. Economics growth correlates with national capability to build their nation and give welfare for their subject. Surely, the members will act so fast because they do not want anything disturb the economic stability.

Nonetheless, ASEAN as an embodiment of hope of its members has to play a pivotal role. ASEAN is perfect hub in South East Asia to conduct multilateral cooperation. The proponents of liberal institutionalism argue that institution is needed to pursuit a common interest and establish legal formal among them. Cyber threat has to be treated equally like other discourses in ASEAN. When threat has become an urgent matter, it should be institutionalized. ASEAN has a responsibility to make a guideline that can be adapted and implemented by its members. Non-intervention should come first when ASEAN make a guideline. Rather than make a strict regulation like in EU, ASEAN can create a guideline which accomodate the diversity of the countries. Every nation have a unique cyber security problem and cannot be handled similarly. Hence, this guideline can be adjusted with their necessity.

Another task that should require attention from ASEAN is bridging the gap between the members. To avoid intervention, ASEAN can create a forum to share information regarding

cyber security issues. When they find a difficult task to solve, ASEAN is able to conduct a cooperation among the members and play its role as an important hub of region. The cooperation framework should contain technical cooperation, training mechanism, exchange of expert, consultation and sharing knowledge. On the other side, ASEAN should put cyber security as an important issue to be discussed at high offical meeting. ASEAN has already had annualy important meetings which is attended by head of governments or top ministers. Adding the cyber security issue into high official meeting, slowly but sure can build an awareness between ASEAN top leaders.

## Conclusion

The conclusion that can be drawn from this article is ASEAN countries cannot depend on self-help ability to prevent cyber attack. Cyber space is borderless, hence it is impossible to define state border. Eventhough it seems uncertain to prevent cyber attack, multilateral cooperation through ASEAN is suitable in South East Asia. ASEAN has had the members and body of organization. It will be no obstacle for the members of ASEAN addressing the cyber security problem. This organization can create framework and guidelines to protect the cyber security region from catastrophe. As long as ASEAN prioritizes cyber security as a main issue and develop cyber security cooperation framework, it can close the gap between them.

## References


i. Aronso, D. Jonathan., 2005. *Causes and consequences of the communication and Internet Revolution dalam John Baylis dan Steve Simth (ed). The Globalization of World Politics: An Introduction to International Relations*. London: Oxford University Press.

ii. Buzan, Barry, Weaver, and Wilde ., 1998. *Security: A Framework of Analysis*. USA: Lynne Rienner Publisher.

iii. Buzan, Barry and Weaver, Ole., 2003. *Regions and Power: The Structure of International Security*. England: Cambridge.

iv. Choudory, Saheli Roy.,2018. *Southeast Asia is Hugely at Risk of Cyberattacks*. [Online] Available at: http://cnbc.com/2018/01/23/asean-need-to-increase-cybersecurity-spending-says-new-report.html, [Aaccesed 29th of July 2018].

v. International Telecommunication Union, 2015. *Global Security Index 2014*. S.l.: ABI Research.

vi. NATO. nd. [Online] Available at: http://www.nato.int/cps/en/natohq/topics _78170.htm [Accesed 29th of July 2018].

vii. Paul, T.V., 2012. *International Relations Theory and Regional Transformation*. England: Cambridge.

viii. PwC Global, 2014.*Managing Risk Cyber With Insurance*.S.l.: s.n

ix. Waltz, Kenneth, 1993. The Emerging Structure of International Politics. *International Security*vol. 18, no.2.

x. Yiao, Sophia.,2015. *ASEAN Organizations Braced for Cyber Attack*. [Online] Available at:https://computerweekly.com/features/ASEAN-organizationms-braced-for-cyber-attack [Accesed on 29th of July 2018].