Analysis of vulnerability of the ASEAN cyber security cooperation

Aulia Nasyrah1,2
1International Relations Department, Faculty of Social and Political Science, Airlangga University, Indonesia
2email address: Aulia.nasyrah-2016@fisip.unair.ac.id

Abstract. This paper will discuss the issue of cybercrime as international problems and as the new wave of transnational crime nowadays and the impact of cybercrime in Southeast Asia Region. The increasing of technology and information to make an advances of telecommunication and modern technology absolutely will be the goal of every state in the world for their own sustainable development and it also becomes the key of successful government but at the same time the acts of cybercrime have been established as the most rapidly growing and make a negative impact. This article consists of three sections. The first introduces and explain the notion of transnational cybercrime and the discourse of cybercrime impact. The second section to examine the impact of cybercrime itself with a special focus on how it makes a damage to Southeast Asia countries existence. It also discusses the kind of comparison between a few example cases that had a different result on some country in Southeast Asia from the attack of APT 30 hacker that targeting Southeast Asia since more than ten years ago. The final section considers some analysis for the solution of this cybercrime problems with observing several factors to make Southeast Asia solved or at least minimize the cybercrime problems and impact.

1. Introduction
Southeast Asia region is known as a region that has various problems in the field of security. These various security issues arise from within the country, either domestically or abroad. One of the problems encountered and requires special attention from ASEAN is the existence of Transnational Organized Crime (TOC). In identifying the Transnational Crime it is said to be an illegal act in which there are transaction processes that prioritize the profit-making process by using strength and flexibility in it (Thomas and Hans, 2012) and the actions were taken in violation of applicable law (Michael, 2008) Transnational Organized Crime is said to be a dangerous crime because of its contain many group and organized and in determining its target of TOC attacks can pose a threat to anyone including threats to state security.

Because of the negative impact of TOC, Cooperation of the states are required to combat and counter crimes together, TOC is a deadly problem because it borderless and can across the border of the states so easy that makes it more troublesome to solve even with the big regional organization such as ASEAN. Actually as William opinion ASEAN as a regional organization of Southeast Asia whose members of several countries become a sufficient strong factor to make this TOC becoming bigger and bigger by the time, why? The reason is because of differences in capabilities and laws in every country in the face of TOC (William, 2001) This is what makes TOC more worst for the developing or even poorer regions of the country, because of their inability to handle the TOC itself.

Cybercrime is one of the TOC, cybercrime also have a different kind of type, namely hacking, cracking, spamming, phishing, carding, defacing and others (dosenit.com, 2017) but the main focus of the author in this article is about TOC in taking action against the law by utilizing the evolving
of technology and information by retrieving others information without legal permission or known as Hacking. Hacking is an unauthorized intrusion into a computer or a network. The person who engaged in hacking activities is generally referred to as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system. (Technopedia.com) crime activities committed by hackers is disturbing the international party. The power of the hacker capability depends on who behind the hacking system and depending on how widespread network of hackers is in carrying out its mission, the development of technology and information continues to grow making the power of hackers who use it is also increasing. This arrives hot on the heels of an announcement that the Department of Defense is a classification of cyber capabilities as weapons and threats. (Popsci.com 2013).

Increasing of Information Communication and Technologies (ICT) strengthened the interconnectivity between the member states of ASEAN Organization, ICT make a lot of potential and common benefits to make the development in their own state become better, but in the other hand, ICT could also become a threat if it be used by an irresponsible person. With estimated 4 billion population for Asia in 2017 with more than 1.9 billion internet user or 46.7% penetration rate as for June 30, 2017 (internetworldstats, 2017). ASEAN with the growth of Internet Penetration too shows that this community should pay attention to the online threat such as hacking activity. So this article will discuss how to make ASEAN potential not to be threatened by an intelligence hacker by working together on ASEAN cyber security Cooperation.

2. Methods
This study is part of a descriptive study by describing the relationship between Transnationalism and Cybercrime as a Transnational Organized Crime and also how these issues become a threat to Southeast Asia region. Cybercrime called as an international issue because this problem can make a negative effect to every sector in the state development, make an impact for a private and business actors, influence a stabilization of human security, and the worst part is hacker’s activity could steal a private and secret information and state property. And in the end of this study will describe a few factor that becomes the main reason why ASEAN as a regional organization in Southeast Asia struggling and unable to handle cybercrime with a quick response.

3. Discussion
3.1 The impact of cybercrime hacker in Southeast Asia
Transnational crime organized crime has become a difficult problem that is hard to eradicate first. Not only in small or developing countries, developed countries with all the advantage as the United States also have an obstacle in combating this transnational crime. For cybercrime problems globally, the cost of damage by cybercriminals has reached $6 billion by 2017, the cost of ransomware damage exceeds $5 billion globally by 2017 and this figure has risen very drastically from a mere $325 million in 2015 (cybersecurityventures, 2017). Therefore cybercrime in the modern era as it is now said to be the new wave of an online threat to any State in the world as Jeffrey Carr told that cyber war trend will make a negative effect with a global community (Carr, 2010).

Not only troubling the country in America or Europe. Cybercrime also disturbs the countries in Asia and its impact extends to Southeast Asia. Cybercrime as a transnational crime is considered very detrimental to the Southeast Asian region. Things that make cybercrime said to be a serious crime because cybercrime will cause a lot of trouble, one of them is the economic loss for the countries in ASEAN. There have been many cases like in Malaysia from 2007 to 2012 reporting a loss of approximately $900 million to cybercriminal and in the calculation there are at least 30 individuals became a victims of cybercrime every day (Qing 2012) or other cases such as Indonesia, for example, have experienced losses of $ 2.7 billion for similar cases (Norton 2012).
and the country with the biggest losses are Singapore countries that lost approximately $1,158 for 1 year alone (Yao 2015).

Cybercrime not only harmful in the economic field but also in the political sector. For example in April 2015, US online security agency FireEye released data on losses that not only burden the country's economy but are politically based on crimes committed by a group of hackers called Advanced Persistent Threat (APT 30). The operations of their crime to obtain state-confidential information in Southeast Asian countries, and also including India and China. The tactics of this APT 30 crime are different from other cybercrime patrons because the result of their crimes not only make financial losses but also to interest on political issues by creating 200 versions of malware programs designed to steal data related to regional political, economic, and military issues in Southeast Asia. So cybercrime not only leads to economic losses but also threatens the national security of the State.

According to FireEye and other technologists, it difficult to find and examine who the mastermind behind APT cases and especially APT 30 who attacked many of these countries for a long time, until now they have not been found even a small traces of them, FireEye added that with the number of members on APT 30, which is well organized, shows many suspected places such as showing the territory of China, Russia, Iran, North Korea and other regions unexpectedly, for China, APT30 traces point to the place of Chinese Communist Party (CCP) as the center or headquarters of operation of APT 30 hackers (TheDiplomat, 2017). Investigators believe that CCP has searched confidential data and important information belonging to the ASEAN Countries by using the APT 30 hacker group, by looking at information and understanding ASEAN politics and cooperation are said to be used by China to strengthen politics and security in their own country and the information they get they believed to be used to solve the complicated problem of border conflict in The South China Sea. APT 30 is said to receive a sum of money earned from the Chinese government it is known to be disciplined, systematic, and collaborative in carrying out its crimes of long-term espionage operations on the bloc. But this is still under investigation.

The attack methods of the APT 30 is similar to the modern intelligence agency, such as the famous National Security Agency (NSA) that infects its victims with storage devices such as USB or hard drives (TheHackernews, 2015). Not only that, another method that is done by sending an email with a link or malicious program then the program will infiltrate the government computer network or business. From there they will steal important documents relevant to their interests (CNN 2015) for crime operations APT 30 Hacker who in carrying out its operations can use a variety of ways with various names such as Backspace, Shipshape, Spaceship and Flashflood is the name they give to malware or hacking ways since early 2005 and this way is different from hackers who have less ability than hackers APT 30.

The main reason why this advance hacker like APT 30 is targeting Southeast Asia as their primer target because this region has lot of potential in the economic sector, the rapid economic growth makes Southeast Asia has an abundant supply of energy and hydrocarbon area and absolutely a lot of prime fishing area. It contains potential reserves of up to 11 billion barrels of oil, 190 trillion cubic feet of natural gas. So it is not surprising that maritime conflicts are also increasing. And with these factors that make the activity of hackers APT 30 increasing (FireEye). Having some of the world's most active economies without the strict rules of cybercrime, Southeast Asia countries are more likely to be targeted from the rest of the world.

It has been mentioned before that APT 30 not only causes a harm to economic but also political losses, for Southeast Asia APT 30 itself attacks various sectors such as Telecommunication where APT 30 attacks Regional Telecommunication Providers, Asia-Based Employees of Global
Telecommunications and Tech Firms and Military Application Technology too (Kaspersky, 2015). APT 30 also attacking Transportation sector, a threat APT 30 group that has historically focused its operations on targets in the Philippines and Malaysia spoofed the domain names of two well-known international shipping companies. And the most severe is the banking sector where banks in Southeast Asia appear to face a double threat. The first is the pernicious cybercrime activity we observe around the world, such as credit card fraud and the theft of banking credentials. The second threat is focused specifically on the banks of a development mission in the region (FireEye, 2015). With disadvantages to various major sectors supporting the development of a State, Southeast Asian countries agreed to cooperate to overcome the problem of cybercrime especially hacking.

3.2 Analysis of vulnerability of the ASEAN cyber security cooperation

With the enormous power of APT 30 hackers managed to make Southeast Asian countries cooperation look very weak in the face of cybercrime cases. Though hacker attacks targeting Southeast Asia is quite heavy. The most notorious attack by APT 30 hackers that strongly demonstrates the weakness of ASEAN in tackling the cybercrime case is APT 30 in its crime operations that use the same tools, tactics and procedures within 10 years of the creation of a large hacking organization suspected of external parties Southeast Asia (FireEye.com, 2015), whereas with the same patron, ASEAN should be able to take precautionary action against a predictable attack because of the same patron but APT 30 can perform its consistent long-term mission and make big losses on ASEAN side for more than 10 years has proven that the cooperation undertaken by ASEAN countries is not very effective and efficient in combating cybercrime crime.

Though characteristic inherent in APT 30 organization that is doing crime operation by way of same tactics, tools and procedure and act differently from other hacker group, and sure they will keep trying to do something new of unpredictable action and also make a sudden movement order so the state technology agency can’t do much because not predict it first. But this APT 30 group can be free to commit crimes in the ASEAN region without changing their habits proves that ASEAN cyber security has not stabilized yet. And pretty sure is not responsive to face cybercrime crime and take a long time to take an action and do not want to acknowledge their weakness by asking for help to the other state.

The weakness of ASEAN cooperation in cyber security initiatives to combat cybercrime is also seen from its own organizational body, for example from the lack of legal authority and coordination procedures in ASEAN regional organizations as well as coordination of ASEAN organizations to each of the countries which still difficult to cooperate in counteracting the increasing of cybercrime days by days and still keep coming in the future (Mofa, 2006). The lack of coordination procedures of ASEAN legal authorities is also due to differences from ASEAN countries which differ in many respects such as different governmental capacities, differing levels of development in every countries or difference in providing personnel who are tasked to handle everything about cybercrime threat in ASEAN countries.

The number of differences among each ASEAN member will undoubtedly the decision-making process and the difficulty of making effective responses when they needed (Jakarta Post 2007). Countries with high incomes and are said to be the upper echelons in ASEAN development such as Singapore, Brunei, and Malaysia certainly have differences in capacity and governance compared to countries still struggling to develop their economies such as Cambodia, Laos and Myanmar meanwhile APT 30 has a structured and organized workflow, illustrative of a collaborative team environment, and its malware reflects a coherent development approach.

In 2003 ASEAN held a meeting of Telecommunications and IT Ministers Meeting (TELMIN) which discussed the importance of each Southeast Asian Country forming their own Computer
Emergency Response Team (CERT) (CERT.org, 2017), this policy took years to follow by ASEAN countries, the ability of each country, of course, their CERT ability is also different. Each Country will perform the duties of their own CERT State in the face of the cybercriminal. Team CERT since 2015 then began to look at new cybercrime attack models such as Ransomware and cyber forensics. The difficulties faced by Southeast Asian countries in the CERT issue is certainly the awareness of the countries in Southeast Asia to run CERT properly.

The differences are also seen with the variety of perspective to see the cybercrime and cybercriminal itself. For developed countries such as Singapore as a global financial center, Singapore, of course see the threat of cybercrime as a major threat to big business in their country so Singapore will strengthen the country's security system especially with a technology and information sector or an expert agency that can handle this problem issue and multiply the policy to respond to cybercrime more quickly and effectively. Unlike Myanmar, they will face differently of cybercrime threats than Singapore depending on the ability of its government, Myanmar is a country that still facing difficulties in facing basic electrification and insufficient information and technology improvements now on they sure will restrict its country's actions in this sector and prefer to prioritize other sectors that they thinks more important to improve. Therefore, differences of interest also become an important factor.

Not only in perspective of the view but in terms of handling cybercrime also different. Handling cybercrime in unequal Southeast Asia region. Whereas the crime of cybercrime can target a large region or a particular region than just one nation-state. As an example of the APT 30 cybercrime crime case that attacked a large region of ASEAN consisting of many countries due to its bloc-wide program (Gady 2016). Additionally, APT 30 appears to have registered domain names close to asean.org (such as asean.com), hoping to steal data from Internet users seeking ASEAN information. Cybercrime handlers submitted to each country will certainly make a big gap on one state and another state. For example, Singapore, which costs not less than US $ 10 million with ASEAN Cyber Capacity Program (ACCP) with funding resources, expertise and training to strengthen the ability of ASEAN countries in the field of cyber. The amount of budget spent by Singapore is certainly bigger than other Southeast Asian countries because it sees the number of cybercrime that ravages the country. Singapore also has a national plan for cyber security for the next five years by regularly executing the annual agenda of the Senior Officials Meeting on Transnational Crime with ASEAN organizations and in routine consultation with the Japanese state in the Cybercrime Dialogue as an effort by Singapore to continuously learn to prevent and overcome cybercrime threats that lead to country and also lead the Interpol Global Complex for Innovation (IGCI). (Tao 2015)

Other reasons that make ASEAN cooperation weaker to cybercrime attacks are some ASEAN countries are very careful in incorporating elements of sovereignty to ASEAN regional body even though they are somewhat worried about the supranational organization, it’s not a secret that sometimes not every state will share information of their own problem because of the bureaucracy or a competition but the hacker also make a competitive advantage with their increasing capability, it is certainly necessary for a State to survive in playing its role globally but unknowingly. With the closing habit of countries under the auspices of the ASEAN organizations, a mechanism to force Southeast Asian countries to update the national law on these transnational issues will be more difficult as in the ASEAN Ministerial Meeting on Transnational Crime (AMMTC) in which ASEAN has difficulty in awakening Southeast Asian countries against transnational dangers that threaten their State (OECD 2005). Speaking of the AMMTC also shows the weakness of ASEAN cooperation with outside parties such as ASEANPOL or ASEAN drug officers who should cooperate well so that transnational crime problems are not protracted. Looking at the data that APT 30 is likely to be based outside of the Southeast Asian region but targeting its operations for
Southeast Asia that cybercrime is a difficult crime to be wiped out due to the fact that this crime can be done remotely overseas and allows for cybercriminals to commit this crime on site which can’t be found. With the increase of internet users who can access anything and anywhere without checking personal data of the host will also make it hard to find these cybercriminals.

4. Conclusion
After seeing the case of APT 30 that successfully running its crime for 10 years the author analyzes that ASEAN is still fragile in combating transnational organized crime especially cybercrime problems. The impact of cybercrime that clearly looks very serious and makes a lot of losses and damage in every sector from the ASEAN side so these cybercrime problems by increasing the cyber security and completely improve the cooperation of every member of ASEAN in order to preserve economic power and political stability going forward without any threat from a hacker. The vulnerability of the ASEAN economy to cybercriminals that causes loss of financial loss will certainly make investors to think twice to provide any investment in ASEAN countries and of course it will bring new problems in the field of ASEAN economy. And in terms of political threats, cyber espionage is a threat to the national security on every state especially ASEAN countries are vulnerable to cybercrime attacks.

In the future ASEAN should seek for some ways to strengthen cooperation not only to mobilize the strengths of the integration of ASEAN countries but also to cooperate outside the ASEAN region so that the ASEAN region has stronger power not only to take preventive action but also to solve the problem of cybercrime in the next few year in order to protect the economic, political and national security for their own development. The cooperation between stakeholder is needed too because the hacker not only targeting the government but also the company. The need for convention not only as a convention against the transnational crime as ASEAN did in 2007 until 2016 but the need for a special convention with the theme of convention against cybercrime so that ASEAN can make quickly respond to cybercrime threat that will endanger ASEAN as the main regional organization so ASEAN can make a counter action for combat the cybercrime from cybercriminal.

References
[9] Gady and Stefan F 2016 Revealed: China Spies on India and ASEAN Member States
[10] Internetworldstats news 2017 Asia Marketing research, internet usage, population statistic and facebook subscribers.
[14] Popsce 2013 Five ways hacker could kill you right now
[16] Technopedia news 2017 The definition of hacking and what does hacking mean?
[17] The diplomat news 2017 Five Things you should to watch out for at the Chinese Communist Party Congress 2017
[20] Liau Yun Q 2012 Malaysia loses $897.6M to cybercrime ZDNet
[22] Sophia Y 2015 ASEAN Organization Braced for Cyber Attack