ВЗГЛЯД ЗАРУБЕЖНОГО ЭКСПЕРТА

DOI: 10.31857/S032150750010451-8

STRUGGLE OF ASEAN IN CYBER SECURITY

© 2020 S.T. MARMITA (Philippines)

MARMITA Sharmaine T. (Philippines), Post-graduate student, School of International Relations, Saint Petersburg State University (stmarmita@yandex.ru)

Abstract. *This article provides an overview of the prevalent struggle in cyber security among ASEAN member states. The author examines the current cyber security problems faced by ASEAN and the factors contributing to their recurrence. ASEAN's potential GDP growth brought by its rising digital economy is at stake. The region is at a risk of losing billions of dollars over the next few years if no improvements shall be made in the current cyber security structure of the region. The major cyber security incidents in the Southeast Asian region are analysed and the struggle of the governing bodies are revealed.*

Comparative case studies of cyber threat incidents in Singapore, Myanmar, and Vietnam are performed, showing attacks ranging from small business to giant establishments such as airport and hospitals. The priority level of cyber security highly vary per member state, ranging from Singapore's top cyber security spending allocation to negligible budgets and awareness in Cambodia and Laos. There is a blatant lack of expertise, community education, and budget allocation for cyber security in the region.

Despite the continual efforts of ASEAN to come up with a solid cyber security strategy, the progress in impeded by the prioritisation of other security threats such as political and economical. The shortage of professionals in the field and the lack of understanding and accurate gauging of the situation are also factors that contribute to the current poor state of cyber security in the Southeast Asian region. With this, the region has become an easy target for attacks, not only domestically but internationally as well. As a result, the author concludes that reforms in ASEAN's cyber security system must be highly prioritised and regional cooperation should be increased.

Keywords: *cyber security, threat, regional cooperation, ASEAN, cyberterrorism, Southeast Asia*

Among the various forms of security risks plaguing societies lies the inevitable circumstance of cyber threats. The Southeast Asian region, an area long afflicted by security risks such as terrorism, is not spared from this phenomenon. Mainly comprised by developing countries, the digital revolution has spread over the Southeast Asian region, bringing enhancements and, at the same time, threats with it. This evident economic growth and prosperity attracts cyber criminals to conduct their malicious deeds in the young and vulnerable region.

As the Southeast Asian region is posed to become one of the world's largest digital economies, its digital grounds have widely opened up to risk of cyber threats. In the most recent years, cyber attacks and cyber terrorism have targeted various operations ranging from private financial departments to government-owned energy sectors.

At present, member states of the Association of Southeast Asian Nations (ASEAN) are lagging behind other states in the battle against cyber terrorism. It is even noted that the Southeast Asian region, despite its growing digital economy, is blatantly underspending for cyber security [1]. Similar to other security threats faced by the collective, the inherent differences between each government type, economic capabilities, and culture all affect the varying response rates, overall taking a toll on the affectivity of the region's preventive measures.

In 2018, a study has been conducted leading to the initial concept proposal of developing a Six-Ware Cyber Security Framework (SWCSF) by researches from Indonesia's Defense University [2]. A deep analysis had been performed to signify the region's need for the development and implementation of such measures, however displaying a juxtaposition of the treatment of cyber threats in other states in the region. The treatment of cyber threats and cyber security among ASEAN member states is, unfortunately, unequal.

HISTORY AND CONCEPT

Cyber security, a fresh term which had gradually emerged after the discovery of the World Wide Web in 1989, could be defined as the "*practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks*" [3]. The dominant cyber threats that the world is facing are mainly classified into three:

(1) Cybercrime, which is characterized by individuals or groups disrupting systems for the sake of financial gain;

(2) Cyber attack, which is identified as a politically-motivated act and usually involves illegal information extraction;

(3) and Cyber terrorism, which sabotages electronic systems with the intent to cause panic or fear.

These threats exist in many forms and have been divided into three different stages by Russian cyber security expert, Evgeny Kaspersky, based on its impact to nations [4]. Kaspersky defines the three common stages as: DDos, attacking critical data, damaging infrastructure.

The first stage, Distributed Denial of Service (DDoS), had been commonly observed during the attacks of famous *hacktivists*, people gaining unauthorized to networks access for political or social purposes, such as *Lulzsec* and *Anonymous*. The main concept of this stage is to overload the network with requests until it gives way. The results are expected to set off a network failure, disabling the system. Vulnerable parties are not limited to web servers but include telecommunication systems as well. While DDoS attacks can't be fully prevented at the moment, institutions have the option to strengthen their cyber defenses from attackers and avoid having their systems unresponsive. Recovery plans post-attack are also necessary to help get the system back on its feet.

The 2nd stage, which involves the assault on critical data, is set to compromise critical data which are highly consequential to the operations of organizations, which include firms, governments, and industries. These attacks are mainly aimed at highly-organized infrastructure rather than individuals. The forms of attack could be either be designed to wipe data out of a system or to obscurely modify existing data without being detected by its administrators.

The 3d part is the full corruption of the infrastructure. It entails a full-on attack on critical infrastructure, eventually leading to physical damage on machines, systems, and even whole buildings. This stage is the most difficult to carry out but also the most destructive of all [4].

As the years pass, both cyber threats and cyber security continue to leverage their attacks and defences respectively to maintain their goals. Nations who are highly powered by technology have the ability to defend themselves from attacks but, ironically, are also more vulnerable to it.

Southeast Asia's increasing reliance to the internet has grown in parallel with the technological advances in the region. Due to this, malicious minds have recourse some of their operations online, banking on the region's unstable cyber security and blatant vulnerability.

The progressing digital transformation in ASEAN, where a growing number of people are relying on the Internet for their retail, banking and leisure needs, signifies the increasing importance of data governance and the call for its improvement [5].

According to Naveen Menon, President for Cisco Systems in Southeast Asia, in a CNBC interview, the pivot towards a digital economy, comes digital threats. "As countries get more digitized, you start to see more attacks surface," he stated. "All of a sudden, you're starting to see economies going online and not enough spending being put to protect these services. ASEAN particularly, is underspending relative to other countries worldwide" [1].

Relative to other forms of terrorism and security threats in the region, those of the cyber space appear to be newest and would be demanding more efforts to understand, mitigate, and counter as the years go by.

THREATS AND INCIDENTS

The digital economy in the ASEAN has an estimated value of generating US$ 150 billion annually and is believed to have potential to add up to US$ 1 trillion to the region's GDP by 2025 [1]. Still, the continuous influx of cyber risks are posed to impede credence and resilience in the region's digital economy. This issue holds a high chance of hindering the SEA region from achieving its maximum digital potential [6]. Moreover, the Asia Pacific Risk Centre stated that the global losses due to data breaches was forecasted to reach US$2.1 trillion by 2019 [7].

In 2008, Vietnam, Singapore, Thailand, and the Philippines, four out of ten ASEAN member states, were recorded among the top ten countries for malicious online activity in the whole Asia-Pacific region. Nevertheless, the total accumulated percentile of malicious activities observed in these countries comprised only about 10% of the total criminal cyber activities in the whole Asia-Pacific region [8]. With the rapid growth of internet-dependency in these countries within the last decade, the situation had been bound to change.

From all the ASEAN nations, Singapore ranks first in terms of cyber security spending, cashing in at 0.22% of its total GDP in 2017. This makes it the lone country in the SEA region to allocate more of its budget to cyber security than the global average of 0.13% of GDP [9]. Singapore has also generated a US$10 million ASEAN Cyber Capacity Fund for the purpose of improving the SEA region's cyber security capabilities [7].

In terms of cyber security expenditure in 2017, Thailand and Malaysia followed Singapore, each allocating 0.05% and 0.08% of their GDPs respectively. Collectively, ASEAN member countries utilize 0.06% of their total GDP on cyber security [9].

SINGAPORE

The paradox of cyber security could be applied to the case of Singapore. Among the ten member states of the ASEAN, Singapore is both extremely secure but is also considered to be part of the *Cyber Five* - countries which are disproportionately vulnerable to cyber attacks due to their extreme reliance on technology [10]. In 2013, Singapore had the highest per capita losses due to cybercrime globally amounting to $1,158 [7].

Among the members of the ASEAN, Singapore is the most economically abundant and has a high level of Internet connectivity, making it especially susceptible to cyber terrorism. The prospects of these attacks include individuals, small and medium businesses, and Critical Information Infrastructure (CIIs), which include the government, healthcare, and banking & finance sectors [10].

Cyber security teams in Singapore have faced several challenges and incidents over the last years. Trend Micro detects about 550 threats related to *ransomware*, a type of malware that threatens to publish its victims' data if a certain ransom is not paid, in Singapore each day [10].

In 2016, more than 60 servers capable of launching DDoS were tracked in Singapore's cyberspace. Website defacement is also a rampant case in Singapore. The act of website defacement refers to the case in which hackers or "hacktivists" deliberately alter a single webpage or a entire website to trick its visitors and infect their computers through implanted malicious codes. The motivation of this is mostly ought to be the promotion political or religious agendas through "hacktivism", which is very similar to physical terrorism goals and motives. It could also be a way to distract critical infrastructures and individuals victims from the "real" cyberattack occurring behind it such as a data breach. Around 1,750 website defacements were reported in Singapore last 2016, mainly targeting small and medium enterprise on the fields of construction, manufacturing and logistics. There have also been 2,512 phishing URLs found, tracing back to Singaporean links. Thirty percent of these were identified to be banking and financial services websites. The other high percentages which followed were targeted towards government organizations (such as the Ministry of Manpower and the Immigration & Checkpoints Authority), and the online payment service provider PayPal [10].

In 2017, Singapore experienced three major cyber attacks: the *MINDEF Cyber Breach* in February, *WannaCry Ransomware* in May, and *Petya Ransomware* in June. The WannaCry Ransomware was not limited to Singapore alone but also affected the rest of the SEA region, simultaneously attacking Indonesia, Vietnam, Thailand, Malaysia, and the Philippines as well [11].

In 2018, the worst data breach hit Singapore after hackers stole 1.5 million of patients' data from the National Electronic Health Record project. It was noted that the data of Prime Minister Lee Hsien Loong had been "specifically and repeatedly" targeted during this breach [12]. The data theft also risked exposing the data, names, and addresses of over 5,400 HIV-positive Singaporeans and 8,800 foreigners, instigating fear among those whose names are on the list, worrying that they could be subject to discrimination should their names be made public [5].

At the beginning of 2019, Singapore reported its second health data breach in six months after 2018's worst-ever data breach involving patients' data [13].

MYANMAR

Known for its seclusion, Myanmar has not been included in most of the cyber security surveys in the SEA region. Nonetheless, cyber crimes still occur in Myanmar. Lesser developed compared to some other member states of the ASEAN, Myanmar is highly susceptible to cyber attacks.

In October 2010, the Ministry of Post and Telecommunication, Myanmar's then main internet provider, went under severe DDoS attacks. The attacks occurred from 25 October 2010, just before Myanmar's first national election in the past 20 years. It is believed that the impact of these attacks were recorded to be significantly larger than the Estonia attack back 2007, which crippled the Estonian government's public services for days. Myanmar's military was reportedly rose suspicions of being behind the attacks in order to limit the flow of available information during the election period [8]. Another accused "state-sponsored" cyber attack occurred back in 2013 when Google warned some news correspondents covering Myanmar that their Gmail accounts might be subject to attacks instigated by the military of the state [14].

Despite the relatively new emergence of the internet in Myanmar, hacktivism is also a rampant cyber threat in Myanmar. Hackers are believed to make use of social media channels such as Facebook and other private forums to coordinate attacks. In January 2016, internet vigilantes, called *netilantes,* brought down nearly 300 Thai government websites using DDoS attacks. Blink Hacker Group, netilantes from Myanmar, were believed to be responsible for the attacks [8].

VIETNAM

Vietnam itself has also been subject to multiple cases of cyber attacks during the last few years. In the cyber space, the encounter rates of Malaysia and Thailand are estimated to be around 35% in Q4 of 2015, 46.6% for the Philippines and around 50.6% for Vietnam. Indonesia is recorded to have the highest encounter rate, with more than 60%. This means that in Indonesia, computers that run real-time security software have reported detecting malware and other potentially unwanted software simultaneously [8].

For almost one year, spanning from December 2015 to November 2016, Vietnam registered 1.68 million IP blocks, ranking fifth among countries all over the world from which several attacks against Internet of Things (IoT) devices were said to have originated. Repercussions of these attacks threaten to lead Southeast Asian to lose up to $750 billion in market capitalization due to the lurking threats [9].

The Cyber security index of 2016 showed that ASEAN countries are already among the states highly subjected to malware threat in the Asia-Pacific region. Vietnam was then ranked 6th, followed by Thailand, Malaysia and Singapore are ranked 10th, 11th and 12th respectively [8].

In July 2016, Vietnam's cyber space was attacked by the Chinese hacking group '1937CN' which hijacked several flight information screens and sound systems in both the Noi Bai and Tan Son Nhat airports. The attack resulted to loss of local control was used to broadcast anti-Vietnamese and Philippines propaganda on the airport screens [10].

Another aviation-related cyber attack in Vietnam was the hacking of more than 400,000 personal details of Vietnam Airlines frequent flyers and posting them online. Again relating to the territorial waters dispute, the flight information monitor screens at both the Hanoi and Ho Chi Minh City airports were defaced with messages regarding the topic. Not only were the flight information screens the ones affected by these messages but also the rest of the public announcement systems in the airports were subjected to the said broadcasts [8].

Even third party countries have not been spared by these local attacks as Japan's Toyota Motor Corporation divulged a data breach that had been uncovered on their servers from its Thailand and Vietnam Subsidiaries. This led to the unauthorized release of 3.1 million clients' personal information in Japan [13].

CURRENT LAW OR MEASURES

Globally, The Council of Europe Convention on Cybercrime, simply acknowledged as the "Budapest Convention", is the first and the only international convention that deals with cybercrime until the present day. It incorporates both existing and procedural parts of regulation, requesting its signatories to criminalize cyber offences against the confidentiality, integrity and availability of computer data. These also includes offences such as illegal access, interception of non-public transmission, interference with computer data and system, and misuse of computer-related devices. Until the present day, there hasn't still been any ASEAN member state that has signed and/or ratified the "Budapest Convention". Moreover, only eight out of ten ASEAN member states, excluding Laos and Cambodia, have enacted some form of legislation to regulate cybercrimes with laws aligning with the requirements of the "Budapest Convention" [8].

Despite the premise of being a collective entity under the ASEAN, each member states' legislation and counter cyber terrorism measures also vary immensely.

There are currently four ASEAN mechanisms in place to investigate various features of cyber security and cybercrime. The list includes the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), ASEAN Telecommunications and IT Ministers Meeting (TELMIN), the ASEAN Regional Forum (ARF), and the ASEAN Senior Officials Meeting on Transnational Crime (SOMTC).

ASEAN's cyber security regulatory framework is still lagging behind compared to those of other neighboring countries and regional bodies such as the European Union's. The lack of public awareness about cyber risks and cyber security incidents are problematic and is observed to be lower in the SEA region compared to other countries where data breach laws are in force. This issue on the lack of awareness has influenced the pace and perspective as to how lawmakers in the SEA region to perceive and carry out cyber security measures in their directives. Among the ASEAN states, only Singapore and Malaysia are equipped with a number of advanced cyber security regulatory tools. On the other hand, the Philippines and Thailand have already began establishing a number of regulatory frameworks required to address cyber security. Despite this, the majority of ASEAN member states are yet to develop a sturdier rules on cyber security [15].

The ASEAN Political-Security Community Blueprint 2025 emphasises the need to combat cyber crimes by means of regional collaboration. It upholds the strengthening of cooperation between all ten ASEAN member states in battling cyber terrorism, calling to develop and improve appropriate laws to address cyber crimes as well as strengthening private to public partnerships in order to enhance secure information sharing within the region [11].

CONTINUING STRUGGLE

Despite these efforts to build a better cyber security strategy and response system in the ASEAN, firms and governments in the region are still not up to par. It is reported that firms and organisations in the region take 1.7 times longer compared to the global median when it comes to discovering a breach in the system. Furthermore, 78% of internet users in Asia are reported to have not received any form of education about cyber security [9]. Linking to the number of published research works among ASEAN member states, there are also relatively few being conducted on the theme of cyber security. From 2014-2019, a recent study showed that there have been no published research about cyber security found in Laos and Cambodia, both at 0%. The tops percentage belonged to Malaysia (9.33%), Myanmar (5.19%), and Singapore (5.18%) [16]. This reflects the lack of understanding and sufficient interest in the existing cyber threats in many Southeast Asian countries and shortage of effort for cyber space protection.

It should also be noted that cyber security awareness is an initiative that had been brought up in ASEAN's Master Plan 2015 and 2020 [17]. To date, there has not been much progress and the turn of events in 2020, for example the emergence of COIVD-19, is slowly forcing the ASEAN to adapt a more electronic and cyber-dependent such as increased reliance on online transactions and even the shift to online work, creating more data for possible exposure. It is time to expedite the efforts on understanding and combating cyber threats in the region, now more than ever.

CONCLUSION

At the moment, the regional policies of the ASEAN member states are still limited due to the consideration of non-interference on a nation's right to self-determination. The ASEAN states are highly encouraged to develop a deeper understanding of the security threats in the cyber space and act upon the matter, enforcing a swift and higher level of cooperation.

Similar to the ASEAN's issue with combating physical and regional terrorist threats, posing peril to the region's security, the expansion of malicious motives on a whole new different medium is not a matter to ignore. The region ought to learn from various developed frameworks of its neighboring countries in order to flourish economically and securely in this growing digital era.

To sum up, the following conclusions and recommendations could be made.

First, ASEAN is not spending enough for the region's cyber security. It is necessary to increase the region's cyber security budget given what is at stake. The cost of investment for data protection may be high but if ignored may lead to greater losses in the economy and decreased societal trust.

Second, there is a lack of cyber security education among the masses. This circumstance is substantial especially among children who are prospectively the most vulnerable targets. From a young age, it is advisable that children be taught the significance of keeping their personal information private. Such actions will ripple throughout the society and will be valuable in the future. Prevention is the best practice rather than trying to salvage data which have already been compromised. Therefore, basic cyber norms are necessary in the region.

Third, the Southeast Asian region's lag behind cyber security is also attributed to the shortage of professionals in this field. With the ASEAN states' varying qualities and accessibility of education, particularly in the field of cyber security, the small pre-existing pool of professionals handling the situation is another alarming predicament in the region which must be given attention to.

Fourth, regional cooperation should constantly be updated and monitored, taking into consideration international help for the strengthening of ASEAN's cyber security practices. The world of cyber crime and security is picking up a pace faster than before and it is deemed crucial for the latter to always be two steps ahead.

References

1. Gnanasagaran A. The flip side of a digital ASEAN. *The ASEAN Post*, 10.02.2018. https://theaseanpost.com/article/flip-side-digital-asean (accessed 11.27.2019)

2. Supriyadi A.A., Gultom R.A., Kustanta T., 2018. A Strengthening Asean Cyber Cooperation in Countering Cyber Terrorist Groups Activities on the Internet by Implementing the Six-Ware Cyber Security Framework. *International Journal of Management and Information Technology*. Vol. 13, Issue 1.

3. Kaspersky. What is Cyber Security? https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (accessed 11.04.2019)

4. Gibbs S. Eugene Kaspersky: major cyber terrorist attack is only matter of time. *The Guardian*, 01.05.2014. https://www.theguardian.com/technology/2014/may/01/eugene-kaspersky-major-cyberterrorist-attack-uk (accessed 10.18.2019)

5. Thomas J. ASEAN's data governance challenge. *The ASEAN Post*, 20.06.2019. https://theaseanpost.com/article/aseans-data-governance-challenge (accessed 01.26.2020)

6. Dobberstein N. et. al. Cyber security in ASEAN: An Urgent Call to Action. *AT Kearney*. https://www.southeast-asia.kearney.com/article/?/a/cybersecurity-in-asean-an-urgent-call-to-action (accessed 02.22.2020)

7. Subhan A. Cyberattacks on Southeast Asia: Who's Next? *The ASEAN Post*, 01.06.2018. https://theaseanpost.com/article/cyberattacks-southeast-asia-whos-next-0 (accessed 10.14.2019)

8. Chang L. Cybercrime and cyber security in ASEAN. Monash University, 2017. https://www.academia.edu/32258162/Cybercrime_and_Cyber_security_in_ASEAN (accessed 03.28.2020)

9. Subhan A. Southeast Asia's cybersecurity an emerging concern. *The ASEAN Post*, 20.05.2018. https://theaseanpost.com/article/southeast-asias-cybersecurity-emerging-concern (accessed 10.19.2019)

10. Raska M., Ang B. Cyber security in Southeast Asia. Asia Centre, 2018. https://centreasia.eu/wp-content/uploads/2018/12/NotePre%CC%81sentation-AngRaska-Cybersecurity_180518.pdf (accessed 02.15.2020)

11. Victor P. ASEAN in dire need of sturdier cybersecurity. *The ASEAN Post*, 02.02.2018. https://theaseanpost.com/article/asean-dire-need-sturdier-cybersecurity (accessed 11.29.2019)

12. The ASEAN Post, 2018. Singapore data breach could affect banks. https://theaseanpost.com/article/singapore-data-breach-could-affect-banks (accessed 10.20.2019)

13. Thomas J. Intensifying ASEAN's cybersecurity efforts. *The ASEAN Post*, 10.11.2019. https://theaseanpost.com/article/intensifying-aseans-cybersecurity-efforts (accessed 11.27.2019)

14. O'Toole B. Hacking Exposes Cybercrime in Myanmar. *Myanmar Times*, 03.06.2013. https://www.mmtimes.com/national-news/4168-email-hacking-exposes-cybercrime-in-myanmar.html (accessed 01.17.2020)

15. Sociedade Portuguesa de Inovação. Overview of Cybersecurity Status in ASEAN and the EU. 2018. https://project-yaksha.eu/wp-content/uploads/2019/05/D1.1_Overview-of-Cybersecurity-Status-in-ASEAN-EU_vf.pdf (accessed 11.19.2019)

16. Shahar S.M., Ma'arif M.Y., Mizan N.S., Zatar N.S. 2019. CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries. *International Journal of Advanced Trends in Computer Science and Engineering*. Vol. 8. No. 1.4.

17. Strengthening ASEAN's cybersecurity. 2018. https://theaseanpost.com/article/strengthening-aseans-cybersecurity (accessed 12.04.2019)