Security:
Cyber Security

How can we enhance cyber security in ASEAN?

Contents

1. Background Information

Under Chapter 1 of the Charter of the Association of Southeast Asian Nations (ASEAN), one of the purposes of ASEAN is to ensure security and stability among nations through mutual cooperation. Cyber security has become one of the major areas of concern for ASEAN.

1.1 Definition

ASEAN has no official definition of the term 'cyber security', hence the definition by the European Union is used.

According to the European Union,
"Cyber security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of information contained therein."

1.2 Cyber Terms

According to McDowell, M. and Householder, A. (2015):

Cyber security
The process of applying security measures to ensure confidentiality, integrity, and availability of data.

Viruses
A malicious code that infects computers only after the victim follows what he/she was being told to do.

Worms
A malware that infects computers through software without intervention and spread to other computers.

Trojan horse
A software that appears harmless when installed on computers but actually does harm.

Hacker

A term to describe people who does harm to other people's software and computer for their own intentions.

2. Genesis

In the past few years, cyber security issues have been plaguing the ASEAN countries. Cyber attacks in the ASEAN region have been prevalent, especially from 2012 to 2013.

Country	Cyber Security Issue
Brunei	November 2012 From 2010 to 2012, IT Protective Security Services of Brunei Computer Emergency Response Team (BruCERT) detected over 2,000 cyber attacks. 62% of the attacks were virus attacks, 26% was spam, 7% was defacement and 4% scams.
Cambodia	September 2012 A hacktivist group, NullCrew, launched attacks on Cambodian government websites after the arrest of Gottfrid Svartholm Warg (co-founder of The Pirate Bay, a popular media sharing platform) in the country itself. The attacks were also a sign of protest against internet censorship. NullCrew successfully hacked into several government websites and even that of the Cambodian army, and leaked highly confidential information. Anonymous, an infamous hacktivist collective, also waged a cyber war against Cambodia in protest of the arrest of Warg. Over 5,000 documents were successfully stolen and leaked from Cambodia's Ministry of Foreign Affairs. January 2013 The website of Cambodia's National Military Police was hacked by an Indonesian hacker called "Hmei7". The website of the Supreme Court was also hacked but no further information could be found from investigations.
Indonesia	January 2013 Indonesia hackers, Anonymous Indonesia launched a cyber attack on the Cambodian government after the arrest of Wildan Yani Ashari who faced charges for hacking the President's website. Several Indonesian government websites were defaced, including the Ministry of Law and Human Rights, the Ministry of Social Affairs and the Ministry of Tourism and Creative Economy.
Laos	August 2013 Government websites in Laos faced 9 cyber attacks from 7 different attackers from January 2013 to August 2013, in the span of just 8 months. The nature of

	these attacks was defacement and some of the websites affected by the attacks were the Department of Cinema and the Ministry of Education and Sports.
Malaysia	<u>February 2013</u> The website of the Department of Information was hacked in an attempt to tarnish the reputation of the department. A false statement about the resignation of Prime Minister Datuk Seri Najib Tun Razak was posted.
Myanmar	<u>May 2013</u> Anonymous launched an Internet campaign as a form of protest against the plight that the Rohingya community faced in Myanmar. The targets of this campaign were the Burmese government websites, the United Nations and Aung San Suu Kyi for their lack of action regarding the violence against Rohingyas. <u>June 2013</u> Another hacker group, the Blink Hacker Group, attacked websites that supported Rohingya. For example, the English-language website of Burmese Media group Eleven Media was defaced.
Philippines	<u>September 2012</u> In protest of the approval of the Cybercrime Prevention Act, Anonymous Philippines attacked government and private websites, effectively crippling them. <u>March 2013</u> The President's website was defaced by Anonymous Philippines and the President was criticised for the way he handled the Sabah conflict. Other government websites were also hacked.
Singapore	<u>November 2013</u> A series of cyber attacks was launched by "The Messiah", a member of hacktivist organisation Anonymous. Web censorship regulations were one of the reason behind these attacks.
Thailand	<u>October 2012</u> The Turkish Agent Hacker group hacked into the database of McDonald's Thailand and released information about 2,000 users. This same group also attacked the website of Red Cross Thailand as a form of protest against the disrespect of the Prophet Mohammad.
Vietnam	<u>July 2012</u> Chinese search engine and web service Baidu infected local computers in

	Vietnam with Trojan software and other viruses. The affected computers are then subject to remote control, information stealing or even used by hackers for cyber attacks.

3. Sequence of Events

October 2001:

Joint Communique of the Third ASEAN Ministerial Meeting on Transnational Crime

At the Joint Communique of the Third ASEAN Ministerial Meeting on Transnational Crime held in Singapore, the ministers of ASEAN identified cybercrime as a growing problem.

November 2002:

6th ASEAN-China Summit

At the 6th ASEAN-China Summit held in Phnom Penh, ASEAN and China embarked on a cooperation in the field of non-traditional security issues with one of the issues being cybercrime.

March 2005:

ASEAN Regional Forum Seminar on Enhancing Cooperation in the Field of Non-traditional Security Issues

The ASEAN Regional Forum Seminar on Enhancing Cooperation in the Field of Non-traditional Security Issues was hosted by China. Delegates from Australia, Canada, China, Democratic People's Republic of Korea (North Korea), European Union, India, Japan, New Zealand, Pakistan, Papua New Guinea, Republic of Korea (South Korea), Russia, United States of America, the ASEAN member states and the ARF Unit of the ASEAN Secretariat attended the seminar. One of the issues covered during the seminar was Cybercrime - how to enhance cyber security and work with each other to resolve this problem.

July 2006:

ASEAN Regional Forum

The Chairman of the ASEAN Regional Forum issued a statement strongly condemning cyber attacks and terrorist misuse of cyber space.

May 2008:

Joint Communique of the 28th ASEAN Chiefs of Police Conference

The Joint Communique of the 28th ASEAN Chiefs of Police Conference was held in Brunei. One of the issues covered in the conference was cybercrime and the various

representatives agreed on the provision and receiving of support, assistance and expertise as the primary solution.

October 2012:

Third Telecommunications and Information Technology Ministers Meeting

ASEAN Information and Communications Technology (ICT) Ministers attended the Third Telecommunications and Information Technology Ministers Meeting held in Singapore as part of ASEAN's response to widespread cyber threats and viruses. Some of the issues covered discussed the enhancing of cyber security and bridging the digital divide.

September 2013:

ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation

ASEAN embarked on a cybersecurity cooperation with Japan. The Joint Ministerial Statement was adopted and focused on three key areas: (i) Creating a secure business environment; (ii) Building a secure information and communication network; and (iii) Enhancing capacity for cyber security.

May 2014:

Senior Officials Meeting on Transnational Crime (SOMTC)

An ASEAN roadmap on combating cyber crime was finalised in Singapore by the SOMTC Working Group on Cybercrime. The objectives of the roadmap was to enhance regional cooperation on capacity building and training, law enforcement, regulation and legal matters, information exchange and extra-regional cooperation.

ASEAN-Japan Cybercrime Dialogue

Singapore also held the inaugural ASEAN-Japan Cybercrime Dialogue. The main topic of discussion was the enhancement of practical and strategic cooperation in fighting cyber crime.

Present Situation

Up till this date, efforts are still being taken by ASEAN to safeguard cyberspace in Southeast Asia.

All the member states of ASEAN are now equipped with their own Computer Emergency Response Teams. Some of the member states even have national authorities on cyber security. For example, Singapore has the Singapore Infocomm Technology Security Authority (SITSA).

4. Problems

4.1. Political Problems

4.1.1 Policy of Non-Interferences

The policy of non-interferences hinders the enhancement of cyber security. Countries are unable to render immediate help to other countries under cyber attack for fear of violating this policy. Hackers might use this to their advantage and target less digitally developed countries.

4.1.2 Low Commitment and Resilience to Counter Cyber Threats or Attacks

As a result of differences in opinions and perceptions, the main focus and attention of the ASEAN community is not on cyber security. The efforts of ASEAN to counter cybercrime had been rather slow and fragmented (Hein, 2013). Some countries have yet to experience serious cyber threats and are not fully aware of the importance of cyber security. This can be reflected in the exclusion of cyber security from the schedule of official ASEAN meetings held in the year 2013.

Countries that are inactive in cyber security efforts often have other compelling matters that need to be taken care of. For example, the later members of ASEAN – Cambodia, Laos, Myanmar and Vietnam (CLMV) are less developed than their fellow ASEAN members and have been putting in efforts to catch up. The ASEAN Heads of States launched the Initiative for ASEAN Integration (IAI) at the Fourth ASEAN Informal Summit 2000 which focus is to narrow the development divide between ASEAN member states (ASEAN Secretariat, 2014). This initiative is being implemented through the IAI Work Plans – IAI Work Plan I (2002-2008) and IAI Work Plan II (2009-2015). Such comprehensive and long-term planning indicates the importance of the issue of development, and CLMV cannot afford to invest time and efforts on cyber security.

4.1.3 Lack of Efficient Strategies to Counter Cyber Threats or Attacks

There is no common stand on cyber security among ASEAN nations. As a result, there is no available organised system to follow in terms of enhancing cyber security. Less digitally developed countries will be the most disadvantaged without any guiding principle or solution. Indecisiveness by countries in making decisions regarding cyber threats or attacks will eventually become an issue. However, in the past few years, ASEAN has recognised the importance of cyber security and detrimental effects of cyber attacks. Efforts have been made on finding measures to counter cyber threats and

enhance cyber security. One good example is the finalising of an ASEAN roadmap on combating cyber crime by the SOMTC Working Group on Cybercrime.

4.2 Economic Problems

4.2.1 Leakage and Loss of Private, Political and Financial information

Most hackers aim to steal or gain access to private, political and financial information of users, government agencies and major economic organisations. Hackers are using advancements in technology to hide their identity. Recovery of the stolen information is also slowed down. In some cases, cyber attacks were identified months after the date of occurrence. This lag in time can lead to adverse effects. By the time of discovery of the cyber attacks, confidential information and bank accounts may already have been misused by the hackers. The economy will also be affected should hackers get their hands on the financial information of the country. The ASEAN Political-Security community has identified cyber security as a crucial issue and that a strong emphasis should be placed on it (ASEAN Secretariat, 2001).

4.2.2 Direction of Focus on Economic Benefits

It is observed that private companies are placing a higher emphasis on economic profits. Companies are coming up with new innovative features with the intention of attracting consumers to buy or use these advancements of technology. There is little focus on protecting the user, due to lack of communication between private companies and government agencies. One such example would be the banking industry. Currently, many banks provide online banking services. In order to entice more users to use online services, banks have come up with features such as convenient online financial transactions. Often, protection of the user's personal information is neglected. Such cyber attacks have been on the rise in the ASEAN region and more are expected to happen (Gemalto, 2009).

4.2.3 Difference in Development of Research and Development Sector and Digital Literacy

In the Joint Media Statement of the Third ASEAN Telecommunications & IT Ministers (TELMIN), the ASEAN community had pointed out the need to bridge the digital divide (ASEAN Secretariat, 2003). The digital development gap among ASEAN countries is still quite significant. A nation's level of digital development is in close relation with its economic status. More economically developed countries can afford to invest more in their research and development sector while less economically developed countries often face difficulties in doing so. Transferring and sharing of technologies among

countries might pose a problem if less digitally developed countries are unable to invest in such technologies. Such technology will only be available to a selected few in less digitally developed countries due to its high cost and unavailability.

This is a prevalent issue, especially in CLMV countries. To alleviate this problem, the master plan for the ASEAN Cyber University was established in the year 2011. This project is an initiative by the Ministry of Education of the Republic of Korea in collaboration with ASEAN. The purposes of this project are: (1) to bridge the development gap among ASEAN Member States and to support ASEAN's efforts for regional integration and (2) to promote education cooperation and people-to-people exchange (AUN Secretariat, 2015).

4.3 Social Problems

4.3.1 Breach in National Security

Cyber threats or attacks can lead to devastating impacts such as the destruction of the social and moral fabric of a country (ASEAN Secretariat, 2001). Hackers are sought after by terrorist organisations due to their capabilities and resourcefulness. Hackers may be used to recruit manpower and cripple the cyber defence of a nation. Terrorists can also work together with hackers to spread threats and this lethal combination will result in devastating effects on countries. There is also the risk that citizens may be influenced negatively by these hackers and even become hackers themselves due to lack of education.

Hackers can use their technical abilities to hack government databases to spread their own propaganda. Unnecessary fear and social tension will arise from all these attacks. Citizens will lose trust in their government and this can lead to severe consequences such as the destruction of the social and moral fabric of a country. One significant example is the series of attacks by 'Anonymous' that happened in Singapore in 2013. Various government agencies were successfully hacked into and a video threatening war against the Singapore government was posted online (Lee, 2013). The video caused heated discussions among Singaporeans – some condemned the actions of Anonymous while some gave the hackers their full support. Doubts about Singapore's cyber security also arose and made many Singaporeans worried. This example highlights the high possibility of cyber attacks affecting the stability of a country negatively.

4.4 Miscellaneous Problems

4.4.1 Increase in Sophistication of Cyber Attacks

Cyber hackers have been increasing the sophistication of their attacks. It is increasingly more difficult to track down hackers and restore any information stolen. This issue was first raised at the 6th ASEAN-China Summit held in Phnom Penh on 4 November 2002. Technology has improved by leaps and bounds, and the consequences of cyber attacks now will be more detrimental. This will also become a bigger problem should hackers target less digitally developed countries, as there is a lack of expertise and technology to tackle this issue.

References

1. ASEAN-Japan, 2013. *Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation* [online]. Tokyo: ASEAN. Available at: http://www.asean.org/images/Statement/final_joint_statement%20asean-japan%20ministerial%20policy%20meeting.pdf [Accessed 1 July 2015].
2. ASEAN Regional Forum, 2005. *Chair's Summary Report: Seminar on Enhancing Cooperation in the Field of Non-traditional Security Issues* [online]. Available at: http://www.asean.org/archive/arf/12ARF/Chairs-Sanya-7-8March05.pdf [Accessed 3 July 2015].
3. ASEAN Regional Forum, 2006. *Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space*. Kuala Lumpur: ASEAN.
4. ASEAN Secretariat, 2001. *Joint Communique of the Third ASEAN Ministerial Meeting on Transnational Crime (AMMTC) Singapore, 11 October 2001* [online]. Available at: http://www.asean.org/communities/asean-political-security-community/item/joint-communique-of-the-third-asean-ministerial-meeting-on-transnational-crime-ammtc-singapore-11-october-2001 [Accessed 3 July 2015].
5. ASEAN Secretariat, 2002. *Joint Declaration of ASEAN and China on Cooperation in the Field of Non-Traditional Security Issues 6th ASEAN-China Summit Phnom Penh, 4 November 2002* [online]. Available at: http://www.asean.org/news/item/joint-declaration-of-asean-and-china-on-cooperation-in-the-field-of-non-traditional-security-issues-6th-asean-china-summit-phnom-penh-4-november-2002-2 [Accessed 3 July 2015].
6. ASEAN Secretariat, 2008. *Joint Communique of the 28th ASEAN Chiefs of Police Conference Brunei Darussalam, 25-29 May 2008* [online]. Available at: http://www.asean.org/communities/asean-political-security-community/item/joint-

communique-of-the-28th-asean-chiefs-of-police-conference-brunei-darussalam-25-29-may-2008 [Accessed 5 July 2015].

7. ASEAN Secretariat, 2012. *Joint Media Statement of the Third ASEAN Telecommunications & IT Ministers (TELMIN)* [online]. Available at: http://www.asean.org/news/item/joint-media-statement-of-the-third-asean-telecommunications-it-ministers-telmin [Accessed 5 July 2015].
8. ASEAN Secretariat, 2013. *ASEAN's Cooperation on Cybersecurity and against Cybercrime* [PowerPoint presentation]. Available at: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/Presentations/Workshop1/ASEAN%27s_Cooperation_on_Cybercrime_and_Cybersecurity.pdf [Accessed 30 June 2015].
9. ASEAN Secretariat, 2014. *ASEAN Steps Up Fight against Cybercrime and Terrorism* [online]. Available at: http://www.asean.org/news/asean-secretariat-news/item/asean-steps-up-fight-against-cybercrime-and-terrorism [Accessed 7 July 2015].
10. ASEAN Secretariat, 2014. *Declarations and Work Plans* [online]. Available at: http://www.asean.org/communities/asean-economic-community/category/declarations-and-work-plans [Accessed 11 July 2015].
11. ASEAN Secretariat, 2014. *Initiative for ASEAN Integration (IAI) and Narrowing the Development Gap (NDG)* [online]. Available at: http://www.asean.org/communities/asean-economic-community/category/initiative-for-asean-integration-and-narrowing-the-development-gap [Accessed 11 July 2015].
12. ASEAN Secretariat, 2015. *ASEAN-JAPAN DIALOGUE RELATIONS* [online]. Available at: http://www.asean.org/news/item/asean-japan-dialogue-relations [Accessed 7 July 2015].
13. ASEAN Secretariat, 2015. *ASEAN, United States to Bring Partnership to New Height* [online]. Available at: http://www.asean.org/news/asean-secretariat-news/item/asean-united-states-to-bring-partnership-to-new-height [Accessed 7 July 2015].
14. ASEAN Secretariat, 2015. *ASEAN SecGen Attends Inauguration of New INTERPOL Centre in Singapore* [online]. Available at: http://www.asean.org/news/asean-secretariat-news/item/asean-secgen-attends-inauguration-of-new-interpol-centre-in-singapore [Accessed 7 July 2015].
15. AUN Secretariat, 2015. *ASEAN Cyber University* [online]. Available at: http://www.aunsec.org/aseankoreaacademic.php [Accessed 9 July 2015].
16. Heinl, C., 2013. *Regional Cyber Security: Moving Towards a Resilient ASEAN Cyber Security Regime* [online]. Singapore: S. Rajaratnam School of International Studies. Available at: http://www3.ntu.edu.sg/rsis/publications/WorkingPapers/WP263.pdf [Accessed 28 June 2015].
17. Khamla Sounnalat, 2013. *ITU Cyber Security Forum and Cyber Drill: Country updates on Cyber Security (Lao PDR)* [PowerPoint presentation]. Available at:

http://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2013/ITU%20Cybersecurity%20Workshop%20and%20Cyberdrill_Vientiane_Lao_PDR/Presentation/Cyber%20drill%20(LaoCERT%20).pdf [Accessed 6 July 2015].

18. McDowell, M. and Householder, A., 2015. *Why is cyber security a problem?* [online]. United States of America: Clemson University. Available at: https://www.clemson.edu/ccit/help_support/safe_computing/tips/why_cyber_security.html [Accessed 28 June 2015].
19. Mogherini, F., High Representative of the European Union for Foreign Affairs and Security Policy, 2013. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* [online]. Brussels: European Commision. Available at: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf [Accessed 30 June 2015].
20. Noor, E., 2014. *Securing ASEAN's Cyber Domain: Need for Partnership in Strategic Cybersecurity* [online]. Singapore: S. Rajaratnam School of International Studies. Available at: https://www.rsis.edu.sg/wp-content/uploads/2014/11/CO14236.pdf [Accessed 30 June 2015].
21. Storey, R., 2009. *Gemalto warns against dangerous IT security complacency* [online]. Available at: http://www.networkworld.com/article/2273097/lan-wan/gemalto-warns-against-dangerous-it-security-complacency.html [Accessed 8 July 2015].
22. Terence Lee, 2013. *'Anonymous' hackers threaten war with Singapore government* [online]. Available at: https://www.techinasia.com/youtube-anonymous-hacker-group-threatens-war-singapore-govt-video-removed-viral/ [Accessed 8 July 2015].