The State of the Art of Cybersecurity Law in ASEAN

Srirath Gohwong
Faculty of Social Sciences, Kasetsart University, Thailand
E-mail: srirathg3@yahoo.com

Article History
Received: 19 August 2019 **Revised:** 1 September 2019 **Published:** 30 September 2019

Abstract
This paper objective was to investigate the state of the art of Cybersecurity Law in ASEAN by using documentary research for data analysis. The findings found that there were three Laws or Acts for cybersecurity in Thailand, Singapore, and Vietnam. The laws had five outstanding differences in details as follows: policy goals, involved agencies, strata of cybersecurity threats, cybersecurity maintenance, and penalty provision. In addition, there were three issues on the implementation of cybersecurity law-balance between cybersecurity and access; controlling of data, information, and knowledge; and direct effect of a set of classical factors of public policy implementation on the success of cybersecurity policy.
Keywords: State of the Art, Cybersecurity Law, ASEAN

Introduction
The Association of Southeast Asian Nations (ASEAN) is an important regional intergovernmental organization in Asia due to its size of economy as a single market, ranked as the world 5th largest and Asian 3rd largest economy in 2018 (Community Relations Division, ASEAN Secretariat, 2018). ASEAN comprises ten countries in Southeast Asia as follows: Thailand, Malaysia, Myanmar, Laos, Cambodia, Vietnam, Indonesia, Singapore, Philippines, and Brunei (Public Affairs Office, ASEAN Secretariat, 2018). However, growth of openness of this nice community under digital economy has significantly led to significant growth of cyber-attacks in this region according to my studies about cyber-attacks in Thailand, Myanmar, Malaysia, and Vietnam (Gohwong, 2016a, 2016b, 2017a, 2017b). Hence, three countries in ASEAN promulgated Cybersecurity Act in order to manage and control the rise of cyber-attacks in these countries as follows: Thailand's Cybersecurity Act, B.E. 2562 (2019), Vietnam's Law No. 24/2018/QH14 on Cybersecurity, and Republic of Singapore's Cybersecurity Act 2018 (No. 9 of 2018) (Cybersecurity Act, B.E. 2562 (2019), 2019; LAW 24 on Cybersecurity (2018), 2018; Cybersecurity Act 2018 (No. 9 of 2018), 2018). Unfortunately, there is no study about Cybersecurity law in ASEAN. Therefore, this paper objective is to investigate the state of the art of Cybersecurity Law in ASEAN in order to acquire basic data for cybersecurity policy formulation in the rest of ASEAN.

Cybersecurity
Cybersecurity could be defined as the state of being secure from cyber-attacks, such as spam, harassment, malicious code, sniffing, hacking, DoS, DDoS, fraud, in the following areas-tangible assets and physical areas, human resource, operations, infostructure (telecommunication and network), and information security (Whitman and Mattord, 2012; Gohwong, 2016a, Brooks, Grow, Craig, and Short, 2018; Laudon and Laudon, 2019). For national cybersecurity, it is a

form of management by government for protecting her sovereignty in aspects of military, politics, economy, and society.

Methodology

The duration of the study was during 2018-2019 because the first Cybersecurity Law in ASEAN enacted on 2 March 2018 in Singapore. Documentary research was employed for data analysis in this study. Secondary data were from three laws as follows: Thailand's Cybersecurity Act, B.E. 2562 (2019), Vietnam's Law No. 24/2018/QH14 on Cybersecurity, and Republic of Singapore's Cybersecurity Act 2018 (No. 9 of 2018) (Cybersecurity Act, B.E. 2562 (2019), 2019; LAW 24 on Cybersecurity (2018), 2018; Cybersecurity Act 2018 (No. 9 of 2018), 2018).

Findings

The findings in this paper would be separately presented by country as follows: Thailand's Cybersecurity Act, B.E. 2562 (2019), Vietnam's Law No. 24/2018/QH14 on Cybersecurity, and Republic of Singapore's Cybersecurity Act 2018 (No. 9 of 2018).

Thailand's Cybersecurity Act, B.E. 2562 (2019)

First, the cybersecurity law of Thailand was promulgated as an Act on 27 May 2019 in order to protect sovereignty in terms of national security, economic security, martial security, and public order in the country on Critical Information Infrastructure organizations (CII organizations) from both external and internal attacks.

Second, there were a set of related agencies, shown in Figure 1, as follows:

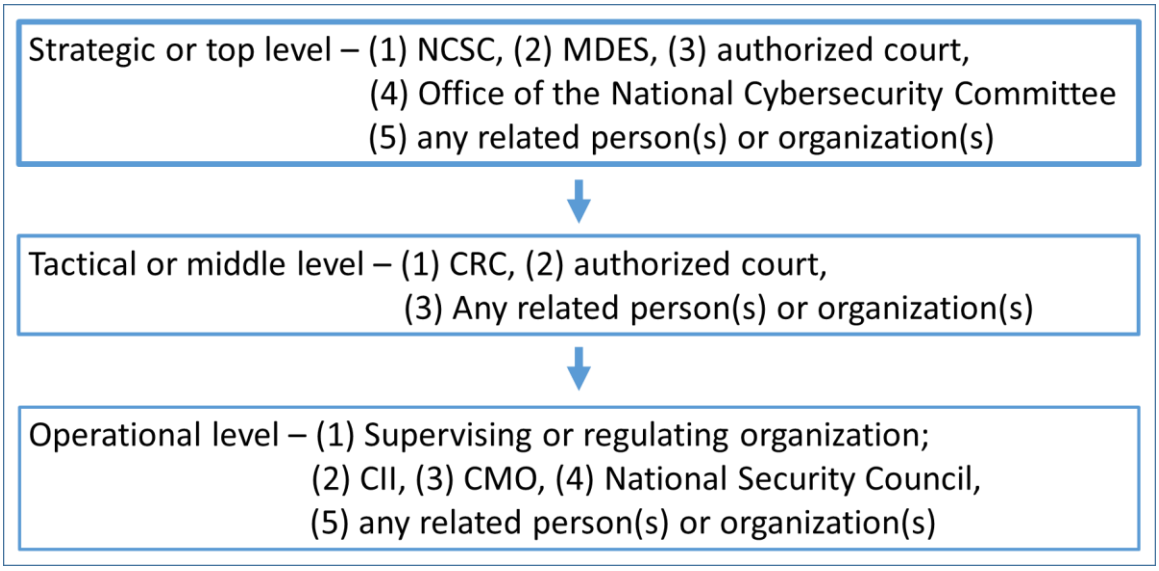

Figure 1. Agency-related Cybersecurity in Thailand

- Government agencies were various agencies such as central government, regional government, local government, state enterprises, the legislative institution, the judicial institution, independent institutions, and public agency.
- National Cyber Security Committee / NCSC was a body at strategic level for mainly setting up any policies and plans on national cybersecurity maintenance for the Cabinet's approval with public hearing or meeting among government agencies, supervising or regulating organization, and CII organizations. NCSC, then, made these policies and plans available to related people and

related agencies in Government Gazette. In addition, NSCS duties were to set up management policy about cybersecurity for government agencies and CII organizations; set up master plan(s) as operational plan(s) for cybersecurity; establish standards and guidelines for developing service systems of cybersecurity; determined standards for cybersecurity; establish minimum standard for computer, computer system, computer program; set up measures and guidelines to enhance knowledge and expertise in cybersecurity of related agencies; prescribe framework(s) for both internal and external coordination for cybersecurity, and made a formal judgment about a problem or dispute on domain or mission of CII organizations or coordinating agency(ies) for cybersecurity.

- Organization of Critical Information Infrastructure (CII) comprised government agencies or firms, determined by NCSC, as providers of Critical Information Infrastructure such as national security, substantive public service, banking and finance, information technology and telecommunications, transportation and logistics, energy and public utilities, public health, and others as NCSC's order(s).
- Supervising or regulating organization comprised government agencies or firms or persons at operational level, appointed by law, for supervising or regulating the operations of government agency(ies) or CII organization(s).
- National coordinating agencies for the security of computer systems and the incident response and computer forensic science
- Coordinating agencies for cybersecurity in the country and foreign countries-For internal cybersecurity, NCSC determined characteristics, duties, and responsibilities of these agencies for CII organizations. In addition, NCSC could assign government agency(ies) or supervising or regulating organization(s) for wholly or partly acting as coordinating agency for CII organization(s).
- Cybersecurity Regulating Committee / CRC was a body at middle level with duties and powers for monitoring the undertaking in accordance with NCSC's policies and plans; monitoring and undertaking in order to cope with cyber-attacks/ cyber threats at critical level; regulating the undertaking of the national coordinating agencies for the security of computer systems and the incident response and computer forensic science; prescribing Code of Practice and standard framework in cybersecurity maintenance as minimum requirement in cybersecurity; prescribing the duties of both CII organizations and supervising or regulating organizations; determining level of cyber threats and submitting measures to prevent, cope with, assess, suppress, and suspend cyber threats to NCSC; and analyzing cyber threats and evaluating their effects for submitting to NCSC.
- Office of the National Cybersecurity Committee was an autonomous public organization for mainly providing academic job and routine jobs (such as general affairs, meeting, and secretarial tasks) of NCSC and the CRC; determining the Code of Practice and standard framework in cybersecurity for CRC's approval, coordinating CII organizations; coordinating and cooperating in the establishment of coordinating agencies for cybersecurity in the country and foreign countries; acting and coordinating with government agencies and firms for coping with cyber threats according to NCSC's order(s); monitoring any occurrence of cyber threats; enhancing knowledge, understanding, and awareness in cybersecurity; acting as center of data collection and analysis for cybersecurity of the country, including dissemination of information of cybersecurity risks and incidents to government agencies and firms; acting as the center of coordination between national and international agencies, both government agencies and firms,

for cybersecurity; and doing research(s) and providing training(s) and practice(s) in cybersecurity.
- Committee Managing the Office of the National Cybersecurity Committee (CMO) was a body for supervising general administration of NCSC.
- National Security Council was the only legitimate agency under the laws on National Security Council and other relevant laws for coping with the occurrence of crisis-level cyber threats.

Third, cyber-attacks or cyber threats were classified by NCSC in three levels-non-critical level, critical level, and crisis level. For non-critical level, cyber-threat(s) made service unavailability in compromised computer system of CII organization(s). Any person could appeal response order at a non-critical cyber threats only. Next, cyber-threat(s) in the critical level made service unavailability in compromised computer system, computer, or computer data of CII organization(s) public stability, international relations, national defense, economy, public health, public safety, or public order of the people. Last, cyber-threat(s) in the crisis level made severe large-scale service unavailability in computer system, computer, computer data of CII organization(s) and government agency(ies) that caused death to many people or large-scale of sabotage on computer system, computer, and computer data of government agencies and/or CII organizations. In addition, crisis-level cyber threats also caused public disorder or public insecurity in some serious situation such as war, terrorism.

Fourth, cybersecurity maintenance must be done as follows:
- Government agency(ies), supervising or regulating organization(s), and CII organization(s) must maintain cybersecurity in accordance with the Code of Practice and standard framework for cybersecurity of each organization and of CRC.
- Government agency(ies), supervising or regulating organization(s), and CII organization(s) must submit lists or revised list of name of executive officials and operational officials for coordinating cybersecurity to NCSC.
- In the emergency case of crisis-level based cyber threats, NCSC might allow Secretary General of NCSC to do all necessary measures for protection and remedy of cyber-attacks without court's order. However, information about these necessary measures must be submitted to the authorized court after the completeness of the operation(s) as soon as it was possible.
- The NCSC or the CRC might delegate Secretary-General of NCSC to hire fitting expert(s) for some specific tasks and issued identification card for all experts. Every expert must return the card whenever the assigned job was complete.
- CII organization(s) must do risk assessment on cybersecurity by examiner(s) and must investigate readiness of cybersecurity by internal or external information security auditor at least once per year. After that investigation, CII organization(s) must yield a summary report of the evaluation to NCSC within thirty days after the end of investigation. In addition, CII organization(s) must join NCSC's cybersecurity readiness assessment. Last, CII organizations must inform NCSC and supervising or regulating organization(s).
-Supervising or regulating organization(s) must collect information and analyze cyber threats and their effects whenever they found cyber threats by themselves or notification of government agency(ies) or CII organization(s). In addition, they also supported for termination of cyber threats to government agency(ies) or CII organization(s) under their responsibilities. Last, they also informed data about cyber threats to these agencies or organizations under their responsibilities.
- CRC might set Minister of the Digital Economy and Society (MDES), Supreme Commander, and other directors (that assigned by CRC) aside for promptly coping with cyber threats. In

addition, CRC also designated supervising or regulating organization and threatened CII organization(s) to abolish cyber threats.

- CRC was the authorized entity for critical-level based cyber threats by commanding the Office of the National Cybersecurity Committee. In situation analysis and effects evaluation, the Secretary-General of the National Cybersecurity Committee could order the Competent Officials, appointed by Minister of Digital Economy and Society, to issue a letter for requesting cooperation from the relevant persons to get information; bring out a letter requesting for information or documents, or copy of them; asked for information from persons; and enter into a property or place of business with consent from owner of that property or place. In addition, CRC might assign Secretary General of NCSC to issue a formal proposal to competent court. With the authorized court's order, CRC could only access necessary computer data or computer system or other information for cyber threats prevention.
- National Security Council under the laws on National Security Council and other relevant laws was an only authorized agency for mandating all operations against the occurrence of crisis-level cyber threats.
- In order to cope with critical-level or crisis-level cyber threats case, Secretary General of the National Cybersecurity Committee with approval of NCSC or CRC could ask real-time data from a cyber-threat-related person.

Fifth, Penalty provisions were based on violation of confidentiality, integrity, and availability (CIA triangle) of data under this Act, except for the benefit of legal proceedings under this Act or other laws. The related persons were officers under this act and unauthorized persons whereas CII organizations or any legal entities (such as firms) were related agencies. Maximum fine and/or imprisonment were two key penalties under this Act.

Republic of Singapore's Cybersecurity Act 2018 (No. 9 of 2018)

First, the cybersecurity law of Singapore was published as an Act in Government Gazette on 16 March 2018 in order to prevent, manage and respond to cybersecurity threats and incidents, to control owners of critical information infrastructure (CII) and cybersecurity service providers by rules, and to make an official change of other written laws.

Second, there were a set of related authorities and agencies, shown in Figure 2, as follows:

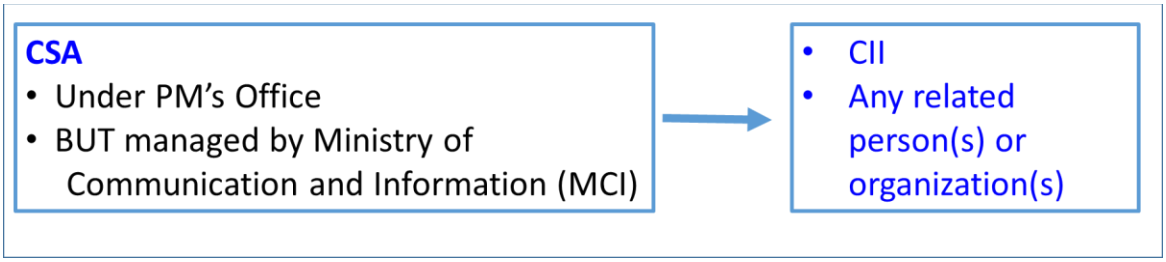

Figure 2. Agency-related Cybersecurity in Singapore

- Cyber Security Agency (CSA) was one and only one government agencies under the Prime Minister's Office but directly managed by the Ministry of Communications and Information (MCI) for maintaining cybersecurity in Republic of Singapore (Cyber Security Agency of Singapore, 2019). It comprised Commissioner (head of CSA), Deputy Commissioner, and one or more Assistant Commissioners of Cybersecurity, and cybersecurity officers. The Commissioner had important duties as follows: (1)to supervise and increase cybersecurity in Singapore; (2) to monitor both internal and external cyber threats; (3) to cope with both internal and external cyber threats on national security, defense, economy, foreign relations, public health, public order or

public safety, or any essential services, of Singapore; (4) to determine CII, and to supervise owners of CII; (5) to set up cybersecurity on codes of practice and standards of performance for owners of CII; (6) to cooperate with foreign computer emergency response teams (CERTs); (7) to strengthen the cybersecurity services industry in Singapore; (8) to grant licenses to cybersecurity service providers (9)to set up standards of cybersecurity products or services in Singapore; (10) to enhance research and development in cybersecurity; and (11) to encourage awareness on cybersecurity in Singapore. In addition, the Deputy Commissioner could do the same duties as Commissioner, except designation and withdrawal of CII.

- Critical Information Infrastructure (CII) Organization were government agencies or firms, determined by Commissioner, as providers of Critical Information Infrastructure, whether the computer or computer system was wholly or partly in Singapore. There were 11 categories of CII agencies as follows: Services relating to energy (1. Electricity generation, electricity transmission or electricity distribution services; 2. Services for the supply or transmission of natural gas for electricity generation); Services relating to info-communications (3. Fixed telephony services; 4. Mobile telephony services; 5. Broadband internet access services; 6.National domain name registry services); Services relating to water (7. Water supply services, 8.Services relating to collection and treatment of used water, 9. Services relating to management of storm water); Services relating to healthcare (10. Acute hospital care services, 11. Services relating to disease surveillance and response); Services relating to banking and finance (12. Banking services, including cash withdrawal and deposits, corporate lending, treasury management, and payment services, 13. Payments clearing and settlement services, 14. Securities trading, clearing, settlement and depository services, 15. Derivatives trading, clearing and settlement services; 16.Services relating to maintenance of monetary and financial stability; 17. Currency issuance, 18. Services relating to cash management and payments for the Government); Services relating to security and emergency services (19. Civil defense services, 20. Police and security services, 21. Immigration services, 22. Registration services under the National Registration Act (Cap. 201), 23. Prison security and rehabilitation services); Services relating to aviation (24. Air navigation services, 25. Airport passenger control and operations, 26. Airport baggage and cargo handling operations, 27. Aerodrome operations, 28. Flight operations of aircraft); Services relating to land transport (29. Rapid transit systems operated under a license granted under the Rapid Transit Systems Act (Cap. 263A), 30.Bus services operated under a bus service license granted under the Bus Services Industry Act 2015 (Act 30 of 2015), 31. Monitoring and management of rapid transit systems operated under a license granted under the Rapid Transit Systems Act, 32. Monitoring and management of bus services operated under a bus service license granted under the Bus Services Industry Act 2015, 33. Monitoring and management of road traffic); Services relating to maritime (34. Monitoring and management of shipping traffic, 35. Container terminal operations, 36. General and bulk cargo terminal operations, 37. Cruise and ferry passenger terminal operations, 38. Pilotage, towage and water supply, 39. Bunker supply, 40. Salvage operations, 41. Passenger ferry operations); Services relating to functioning of Government (42. Services relating to the electronic delivery of Government services to the public, 43. Services relating to the electronic processing of internal Government functions); and Services relating to media (44. Services relating to broadcasting of free-to-air television and radio, 45. Services relating to publication of newspapers, 46. Security printing services). For government agencies, CII organizations belonged to Ministries, led by Permanent Secretary of each Ministry. For owners of private CII organizations, the Commissioner send a notice of information to the owners such as identification of computer and

computer system as CII, identification and duties of owner(s) of CII, name and contact of officers, appointed by the Commissioner, who observe and direct CII, give the owners of CII essential information about deviation from the Commissioner's designation and appeal to Minister of MCI. In addition, validity of designation of CII was 5 years, if not withdrawn by the Commissioner.

- Cybersecurity service providers were licensable provider for managed security operations centre (SOC) monitoring service (for observing and checking the quality of cybersecurity via flow and usage of data in a computer or computer system in a specific entity) and/or penetration testing service (for observing and checking the quality of cybersecurity by seeking vulnerabilities of a computer or computer system in a specific entity).

Third, cybersecurity threat or cybersecurity incident or cyber threat was defined as an unlawful act or activity on or through a computer or computer system that attacked another computer or computer system. There was two strata of cybersecurity threats-normal and serious level.

Fourth, cybersecurity maintenance must be done in two areas-CII and cybersecurity service providers. Due to the scope of the study, only a set of measures for CII was shown as follows:

- The Commissioner had to get information from any person by notice with a reasonable period, given in the prescribed form and manner, which confirmed computer or computer system in a ready to use condition according to the criteria of CII.
- The Commissioner might withdraw the designation of any unqualified CII by written notice.
- The Commissioner might ask owner(s) of CII for necessary information by notice with a reasonable period, given in the prescribed form and manner. In addition, owner(s) of CII must submit any change of necessary information, such as change of ownership in any CII organization, to the Commissioner within a prescribed time, 7 days for change of ownership.
- The Commissioner might issue or approve one or more codes of practice or standards of performance for owners of CII. Any different provision from this Act under any code of practice or standard of performance did not have effect.
- The Commissioner might issue a general or specific written direction to the owner of a CII or a class of owners.
- The owner of any CII must report cybersecurity incident in the prescribed form and manner within the prescribed period.
- The owner of any CII must do, in the prescribed form and manner, cybersecurity audits of CII at least once every 2 years (or higher frequency according to the specific order of the Commissioner) and risk assessments of CII at least once a year. The owner of CII must send a copy of the report of the audit or assessment to the Commissioner within 30 days. If necessary, the Commissioner might order the owner of CII to do the audit or assessment again. In addition, in a serious case, the Commissioner would appoint an audit or a cybersecurity service provider to conduct another audit or cybersecurity risk assessment of CII. The owner must be responsible for any cost of audit or assessment.
- Every owner of CII must join in a cybersecurity exercise, conducted and directed by written notice by the Commissioner in order to testing the readiness of owners of CII for cyber threats.
- The owner could appeal to Minister of MCI. If necessary, an Appeals Advisory Panel, a group of experts, would be set up by the Minister for giving policy advice.
- The Commissioner might investigate and prevent cybersecurity threats in normal and serious level. If necessary, the Commissioner might delegate the Deputy Commissioner, an Assistant Commissioner, a cybersecurity officer or an authorized officer to do this affair. All mentioned above officers acted this affair as incident response officer. In any case of serious level of cyber

threats, the incident response officer must return the computer or other devices to the owner immediately after the completion of any examination or analysis on these devices, possessed by the officer with the consent of owner.
- Declaration of identification card when exercising power under this Act must be done to any affected person by every incident response officer.
- The Commissioner might appoint any cybersecurity technical expert in writing for a specified period to support any incident response officer for coping with cyber threats. The Commissioner must give every cybersecurity technical expert an identification card, which must be carried at all times when doing this job. Every expert must return this ID card to the Commissioner after work.
- For emergency cybersecurity measures and requirements, the Minister might issue a certificate for directing any person or organization specified in the certificate in special affairs such as entered into a property or place of business with competent court's order, concealed name of informer by competent court's order, and access necessary information for identifying, detecting and preventing cyber threats.

Fifth, Penalty provisions were based on violation of confidentiality, integrity, and availability (CIA triangle) of data under this Act, except any information enforced by or under any law, contract or rules of professional conduct. However, disclosure of any information enforced by or under any law, contract or rules of professional conduct could be done in some cases, such as by owner(s) of CII with reasonable care and good faith according to the Commissioner's request. The related persons were officers under this Act and unauthorized persons whereas CII organizations or any legal entities (such as firms) were related agencies. Fine, maximum fine or day fine or part-of-a-day fine, and/or imprisonment were two key penalties under this Act.

Vietnam's Law No. 24/2018/QH14 on Cybersecurity

First, the cybersecurity law of Vietnam was published as a Law in Government Gazette on 26 September 2018 in order to protect national security, public order and safety in cyberspace; and regulate responsibility of related organizations and individuals.

Second, there were a set of related agencies, shown in Figure 3, as follows:

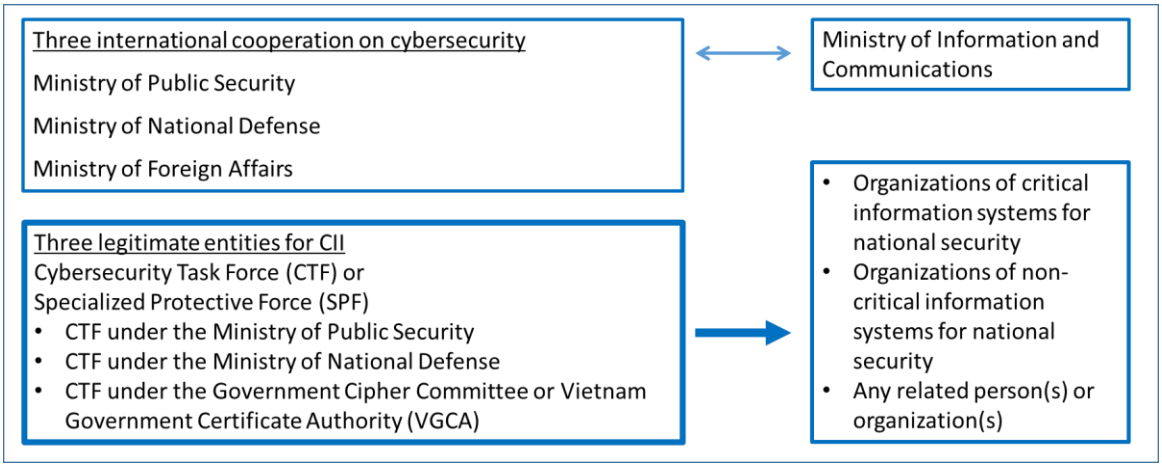

Figure 3. Agency-related Cybersecurity in Singapore

- Three international cooperation on cybersecurity were the Ministry of Public Security or the Ministry of Interior (for every activities, except for any international collaboration of the Ministry of National Defense), the Ministry of National Defense (for any international collaboration of Armed Forces), the Ministry of Foreign Affairs (for any collaboration with the

Ministry of Public Security and the Ministry of National Defense in international cooperation on cybersecurity). The Vietnam government was the entity who determined the international cooperation on cybersecurity's responsibility of line ministries (a number of ministries and branches). However, any other Ministry, line ministry or locality might handle international cooperation on cybersecurity after written allowance from the Ministry of Public Security, except any case of the Ministry of National Defense.

- Three legitimate entities for presiding over coordination for supervision and remedy; evaluating critical information systems in order to produce basic data for upgrading the systems for national security; and assessing critical information systems in order to ensure qualified cybersecurity conditions for national security were the Cybersecurity Task Force (CTF) or Specialized Protective Force (SPF) under the Ministry of Public Security (except cases of the Ministry of National Defense and the Government Cipher Committee), the CTF under the Ministry of National Defense (for evaluating cybersecurity of military information systems), the Government Cipher Committee or Vietnam Government Certificate Authority (VGCA) (for evaluating cybersecurity of cipher information systems under the Government Cipher Committee).
- Organizations of critical information systems for national security were government organizations and political organizations at the central and local levels in the list of Critical Information Infrastructures-based information systems, which was issued, added and amended by the Prime Minister of Vietnam, as follows: information systems for Military, security, diplomatic and cipher (or cryptography); Information systems for classified State secret; Information systems for important items and documents; Information systems for maintaining dangerous materials and substances to humans and environment; Information systems for storage, manufacture and management of critical material/physical facilities related to national security; critical information systems for any operation of central agencies; National information systems for critical sectors such as energy, finance, banking, telecommunications, transport, natural resources and environment, chemicals, medical health, culture and press authorities; and automatic surveillance and control systems for critical works related to national security or national security targets.
- Organizations of non-critical information systems for national security were organizations besides the list of Critical Information Infrastructures-based information systems for cybersecurity of Vietnam that must conduct the audit of cybersecurity of their information systems due to an infringement of the Law violating national security or disrupting public order; and a request of information system administrator from each agency and organization.
- The Ministry of Information and Communications must cooperate with the Ministry of Public Security and the Ministry of National Defense in cybersecurity protection, cooperate with related agencies against spreading propaganda information about Vietnam government, and submit any necessary notice to transmission systems of telecommunications service providers (TSP), Internet service providers (ISP), providers of value-added services in cyberspace (VAS), and information system administrators to remove unlawful data and information on their systems or services.

Third, cybersecurity threat or cybersecurity incident or cyber threat was defined as an unlawful attack on or through national cyberspace infrastructure in Vietnam. There was two strata of cybersecurity threats-normal and dangerous level.

Fourth, cybersecurity maintenance must be done in critical information systems for national security as follows:

- Information system administrator(s) of organization(s) of critical information systems for national security, CTF(s), and competent related agencies (such as any agency that collected and stored any classified data and information as State secret, any agency that detected any act or indication of cyberterrorism) must undertake any necessary measures for preventing and coping with any infringement as follows: any violation of law on national security, social order and safety by using cyberspace, information technology and electronic media, espionage, propaganda against Vietnam, cyber-attacks, cyberterrorism, cybersecurity, dangerous cybersecurity situations. In addition, system administrator(s) and cyberspace service providers (TSPs, ISPs, and VAS providers) under this Law must coordinate with CTF(s) and competent related agencies.
- Ministry of Public Security (except cases of the Ministry of National Defense and the Government Cipher Committee), the Ministry of National Defense, and the Government Cipher Committee were also responsible for cybersecurity in espionage of State secret, cyber-attacks, and cyberterrorism.
- In case of cyberterrorism, individuals might be requested for cooperation from any CTF(s).
- In case of block and deletion of any propaganda-related information within 24 hours, and cessation of any propaganda-related information providers, both organizations and individuals, under this Law, CTF of the Ministry of Public Security or a competent authority of the Ministry of Information and Communications sent a request to any related providers such as TSP, ISP and VAS providers.
- Audit of cybersecurity of critical information systems for national security must be conducted when started employing e-facilities and network information security services; changed in the critical information system; conducted an annual audit; and a one-off audit due to damage from a cybersecurity incident, government agency's request, and CTF's recommendation of an expiry of the deadline for fixing vulnerabilities after a fixed length of time. For the first three audits, the information system administrator(s) must submit written results of audit to the CTF(s) under the Ministry of Public Security or the Ministry of National Defense before October in each year. For one-off audit, the CTF(s) must send written notice in case of damage from a cybersecurity incident for doing audit at least 12 hours in advance or at least 72 hours in advance for government agency's request, and CTF's recommendation of an expiry of the deadline for fixing vulnerabilities after a fixed length of time. The CTF(s) must send written results of audit to the administrator(s) of inspected organization(s) within 30 days.
- Organizations and individual users were responsible for protection of cybersecurity of national cyberspace infrastructure and international internet gateways according to Vietnam's socio-economic development. In addition, international internet gateways were encouraged to locate in Vietnam.
- The controlling of information flow in cyberspace were in two ways. First, Websites, portals, and social media pages of any organization or individual must not disseminate unlawful information against cybersecurity of Vietnam. Latter, any domestic or foreign cyberspace service providers under this Law, such as TSP, ISP, and VAS, must be responsible for user authentication, preservation of confidentiality, provision of user information to the CTF under the Ministry of Public Security if necessary in case of law violation; block and deletion of every unlawful information; obstruction of all cyberspace services providers (TSP, ISP, and VAS providers) under this Law to illegal information dissemination of unauthorized organizations and individual users.

- Related organizations and individual users under the Law could legitimately do research and development of cybersecurity; and continuously improve their skills in cybersecurity and productivity, audit, and testing of digital devices, network services and network applications.
- Information system administrator(s) and cyberspace service providers under this Law, such as TSP, ISP, and VAS, were responsible for controlling child's data protection, data access, and cyberspace participation according to the CTF(s) and related organizations' measures.

Fifth, Penalty provisions were not identified in the Law.

Discussion

According to the above findings, there is three issues in this part as follows:

First, the balance between cybersecurity and access is not an easy affair to do. Due to Laws in Thailand, Singapore, and Vietnam, the relationship between cybersecurity for national security and privacy rights and data access of people is strongly negative. The more cybersecurity stands for the less privacy rights and data access (Whitman and Mattord, 2012). Therefore, high concern of people and firms is a direct consequence of the conflict of needs between two sides. According to Van Meter and Van Horn (1975) and Mazmanian and Sabatier (1983), the effect of economic condition is directly on the success of public policy implementation. For people and firms under condition of liberal digital economy, they need more privacy and confidentiality than any cybersecurity acts or laws could offer to them.

Next, though Thailand (2019), Singapore (2018), and Vietnam (2018) had different regime when they promulgated Cybersecurity Laws or Acts, they all had the same goal that is to absolutely control data, information, and knowledge in terms of lawful acquisition, storage, dissemination, and application (Gohwong, 2017c).

Last, according to the public policy implementation literature of Pressman and Wildavsky (1973), Van Meter and Van Horn (1975), Bardach (1977), Mazmanian and Sabatier (1983), a large amount of involved agencies, diversity of targeted groups' behavior (such as people, firms, government agencies, political organizations), the fruitfulness of valid technical theories and technologies in cybersecurity, and the complexity of communications networks, coordination, cooperation, compliance mechanisms, and appeal procedure under these Laws or Acts in Thailand, Singapore, and Vietnam make much difficulty in cybersecurity policy implementation.

Conclusion

This paper objective was to investigate the state of the art of Cybersecurity Law in ASEAN in order to obtain basic data for cybersecurity policy formulation in the rest of ASEAN. Documentary research was employed in this research. The findings found that there were Cybersecurity law only in Thailand (as an Act), Singapore (as an Act), and Vietnam (as a Law, equivalent to an Act). The findings of Cybersecurity Laws were presented by country in five issues-policy goals, involved agencies, strata of cybersecurity threats, cybersecurity maintenance, and penalty provision. In addition, three concerns about implementing cybersecurity policy in ASEAN were balance between cybersecurity and access; controlling of data, information, and knowledge; and direct effect of a set of classical factors of public policy implementation on the success of cybersecurity.

References

Bardach, E. 1977. **The Implementation Game: What Happen After a Bill Becomes a Law**. Cambridge: MIT Press.

Brooks, C., Grow, C., Craig, P., & Short, D. 2018. **Cybersecurity Essentials**. Indiana: SYBEX.

Community Relations Division, ASEAN Secretariat. 2018. **ASEAN Key Figures 2018**. Jakarta: ASEAN.

Cyber Security Agency of Singapore. 2019. **Our Organisation**. Retrieved from www.csa.gov.sg/who-we-are/our-organisation.

Gohwong, S. 2016a. **The Cyber-attacks and digital economy in Thailand during 2012-2016**. (A paper presented in the 1st International Conference, Hong Kong, 25-27 August 2016).

Gohwong, S. 2016b. **The Cyber-attacks and digital economy in Malaysia during 1997-2016**. (A paper presented in the 2nd International Research Conference, Kuala Lumpur, Malaysia, 27-29 October 2016).

Gohwong, S. 2017a. **The Cyber-threats and digital economy in Myanmar during 2014-2017**. (A paper presented in the 8th ASEAN Conference on Humanities and Social Sciences, Siem Reap, Cambodia, 24 February 2017).

Gohwong, S. 2017b. "The Cyber-attacks in Vietnam during 2010-2016." **Asian Political Science Review** 1 (1): 51-55.

Gohwong, S. 2017c. **IT as the modern invisible jail**. (A paper presented in the 3rd International Conference on Government and Politics, Pathum Thani, Thailand, 24 March 2017).

Laudon, K. and Laudon, J. 2019. **Essentials of MIS**. Harlow: Pearson Education.

Mazmanian, D. and Sabatier, P. 1983. **Implementation and Public Policy**. Illinois: Scott Foresman.

Pressman, J. and Wildavsky, A. 1973. **How Great Expectations in Washington Are Dashed in Oakland; Or, Why It's Amazing that Federal Programs Work at All, This Being a Saga of the Economic Development Administration as Told By Two Sympathetic Observers Who Seek to Build Morals on a Foundation of Ruined Hopes**. California: University of California Press.

Public Affairs Office, ASEAN Secretariat. 2018. **ASEAN Economic Community Blueprint**. Jakarta: ASEAN.

Republic of Singapore Cybersecurity Act 2018 (No. 9 of 2018).

Thailand Cybersecurity Act, B.E. 2562 (2019).

Van Meter, D. and Van Horn, C. 1975. "The Policy Implementation Process: A Conceptual Framework." **Administrative and Society** 6 (4): 445-488.

Vietnam LAW 24 on Cybersecurity (2018).

Whitman, M. and Mattord, H. 2012. **Principles of Information Security**. China: Course Technology.