ÓBUDA UNIVERSITY

DOCTORAL SCHOOL ON SAFETY AND SECURITY SCIENCES
Bánki Donát Faculty

EUROPEAN (VISEGRÁD COUNTRIES) CYBER-SECURITY IN APPLYING FOR ASIAN COUNTRIES: THE CASE OF VIETNAM

Thesis Statements of Ph.D. dissertation

Author

Nguyen Huu Phuoc Dai

Scientific Supervisors

Prof. Dr. Rajnai Zoltán

DOCTORAL SCHOOL ON SAFETY AND SECURITY SCIENCES
Head of Doctoral School on Safety and Security Sciences: Prof. Dr. Rajnai Zoltán

Budapest, 2019

1. INTRODUCTION

Nowadays, in 2019, according to global risks report, there are five major threats such as "extreme weather events, failure of climate change, mitigation and adaptation, natural disasters, data fraud or theft, and cyber-attacks" [1]. It can be seen that two main global threats related to information loss or damage from computer attacks in the cyberspace are mostly security concerns in many countries. Cyber crimes refer to computer crime, information technology crime or high technology crime based on the computer as a target or a means of attacks [2], [3]. Currently, cyber crimes are more complicated in their attacks due to the development of technology. There are various types of cyber crimes such as malware, spyware, virus, ransomware, and the like. They can cause hazardous impacts not only individuals but also organizations, governments or nations; for instance, loss of sensitive data, financial problems, espionage, terrorism, and so on. At present, cybercrimes can be divided into two main groups: machine-made attack and man-made attack. The machine-made attack is a type of cyber-attacks based on computer network environment as a tool to illegal penetrate system in order to get sensitive data and destroy them with financial damage purposes e.g. hacking; data diddling; web jacking; salami attacks; child pornography; spoofing and phishing. In contrast, man-made attack is another type of attack which is considered as a cyber-terrorist attack from an individual or group of people with finance, politics, and military's purposes like money laundering; fraud and financial crimes; online gambling; data alteration or data theft; email bombing; cyberbullying; steganography; computer vandalism; cyberterrorism; and cyber-extortion. Cyber crimes have no border between one nation and the others because it mainly depends on the Internet environment; as a consequence, the prevention or the fighting against the cyber-attacks are not the responsibility of one country but whole countries in the world. Hence, a legal framework of cybersecurity cooperation, cybersecurity strategy or general model of cybersecurity cooperation is an essential and urgent thing in the modern technology era. This research can bring a general view of the current framework of cybersecurity cooperation among Asia, ASEAN, and EU nations. Moreover, this thesis may clarify the difference of strategies, structures or purposes in cybersecurity cooperation in these areas. Remarkably, the author points out the special case in cybersecurity cooperation of Visegrád countries on the way to protect themselves and their contributions to the other nations in the same region towards global cyber-threats. Furthermore, the author also proves that some cybersecurity strategies may be applied in ASEAN countries, particularly in Vietnam. In addition, the researcher also offers some solutions in cooperation amongst ASEAN countries, especially in Vietnam and its neighbors.

2. PURPOSES OF THE DISSERTATION

In order to investigate whether Viet Nam is ready to face any security problems or find out solutions for them, hence this research aims to figure out the answers for several essential questions; for example, 1) what are the current cyber-threats? 2) What are the influences of global cyber-threats towards Vietnam and its neighbors? 3) How can Vietnam solve these problems through international cooperation? 4) What are the advantages of Visegrád cybersecurity strategies towards cyber-attacks? 5) Which cybersecurity strategy can be suitable for Vietnam? Therefore, there are several hypotheses are suggested as follows:

***Hypothesis 1 (H1)**:* Cybersecurity in Visegrád countries shares similarities in goals, strategies, and strength to align with European Union Member States regarding armed forces, cybersecurity, and national security.

Hypothesis 2 (H2): Cybersecurity in the East Asian and the South East Asian countries aim to create a more secure society and supports economic development.

Hypothesis 2a (H2a): Singapore's cybersecurity strategy may be adapted to Vietnam's legal framework.

***Hypothesis 3 (H3)**:* Cybersecurity, especially in cybersecurity cooperation in Visegrád countries may be adapted and networked with Asian countries, particularly in Vietnam and its neighbors.

3. RESEARCH METHODOLOGY

Data collected in this study were scientific articles, a meta-analysis of literature review of related studies on cybersecurity strategies used by Visegrád countries with those from EU, ENISA, NATO, CCDCOE and the like. Moreover, several interviews were undertaken with cybersecurity experts from cybersecurity service companies to identify cyber threats, dangers of the cybercrimes and cyber-attacks, and methods to control them.

4. RESULTS OF RESEARCH

4.1. Concluding observation

This study gives a general outlook of the cybercrimes and their influences towards the government, citizen's life, and the safety of a country by listing them as two major types of cybercrimes such as machine-made attack and man-made attack. Moreover, a new key factor is that this study also shows the differences in purposes between cybercrime and cyber-warfare; for instance, cybercrimes mainly aims in financial goal meanwhile cyber-warfare targets to politics, critical infrastructure, and national security or citizens. In addition, this research also highlights the bilateral, trilateral, or multilateral cooperation in cybersecurity and public security amongst Asia, ASEAN countries with the USA, China, Russia and EU nations. Currently, Asian countries are facing several security challenges such as nuclear proliferation, terrorism, cross-border crime, pandemics, natural catastrophes, resource conflicts, power rivalries, piracy and so on. However, there are some forums which overlap cooperation each other like Association of Southeast Asian Nations (ASEAN), ASEAN Regional Forum (ARF), Asian-Pacific Economic Cooperation (APEC), East Asia Summit (EAS), ASEAN Defense Ministers Meeting (ADMM), Council for Security Cooperation in the Asia Pacific (CSCAP) and Expanded ASEAN Maritime Forum (EAMF) [Figure 1].

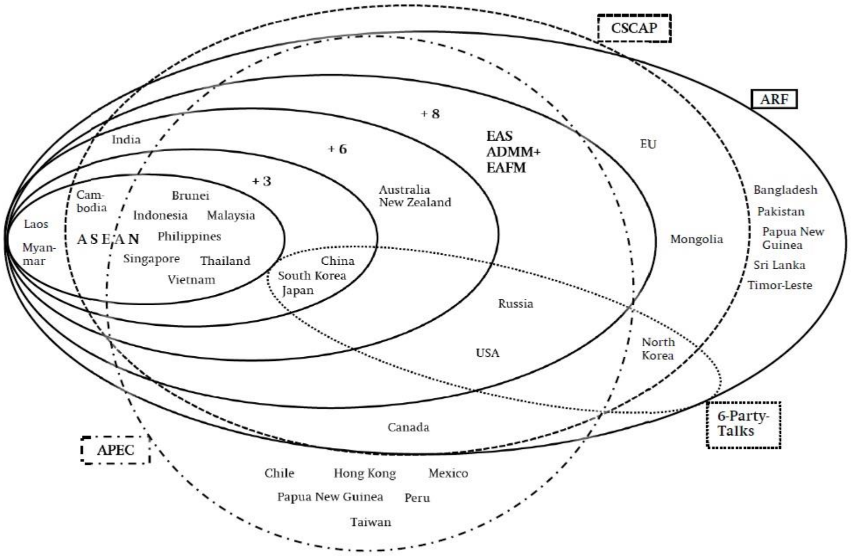


Figure 1: Regional Formats in East Asia and their overlaps [4]

Due to the difference of perception about cybersecurity, lack of cybersecurity capacity building between Asia and Europe, Asia countries' cooperation are mostly in the economy, military, and diplomacy. In fact, it also indicates several Asian organizations cooperation for financial security such as FS-ISAC and HTCIA.

The author helps the viewers have a general overview of Visegrád countries cooperation like the history of them, reasons and purposes for cooperating, its mechanism, their common security threats and its cooperation with other international organizations. Then, the author expresses each cybersecurity strategy of V4 in order to highlight the essential role of V4 cooperation towards EU and NATO in cybersecurity and cyber-defense in front of cyber-threats or cyber-attacks. The main key point is that it proves Visegrád countries' strength and its impact as a big nation's power in the EU.

On the other hand, the author also illustrates the legal framework of Asian countries' cybersecurity. It separates into two groups such as several Asia countries with a strong cybersecurity capacity building (China, Japan, HongKong, South Korea, and North Korea) [Figure 2], ASEAN countries with strong and weak cybersecurity capacity (Singapore, Malaysia, Thailand, the Philippines, Indonesia, Vietnam, Lao PDR, and Cambodia) [Figure 3]. Additionally, it displays several transnational collaboration between Asia, ASEAN nations, and other countries in another region.

Key findings in differences between Asia and EU cybersecurity capacity building

Results of cybersecurity capacity in Asia countries

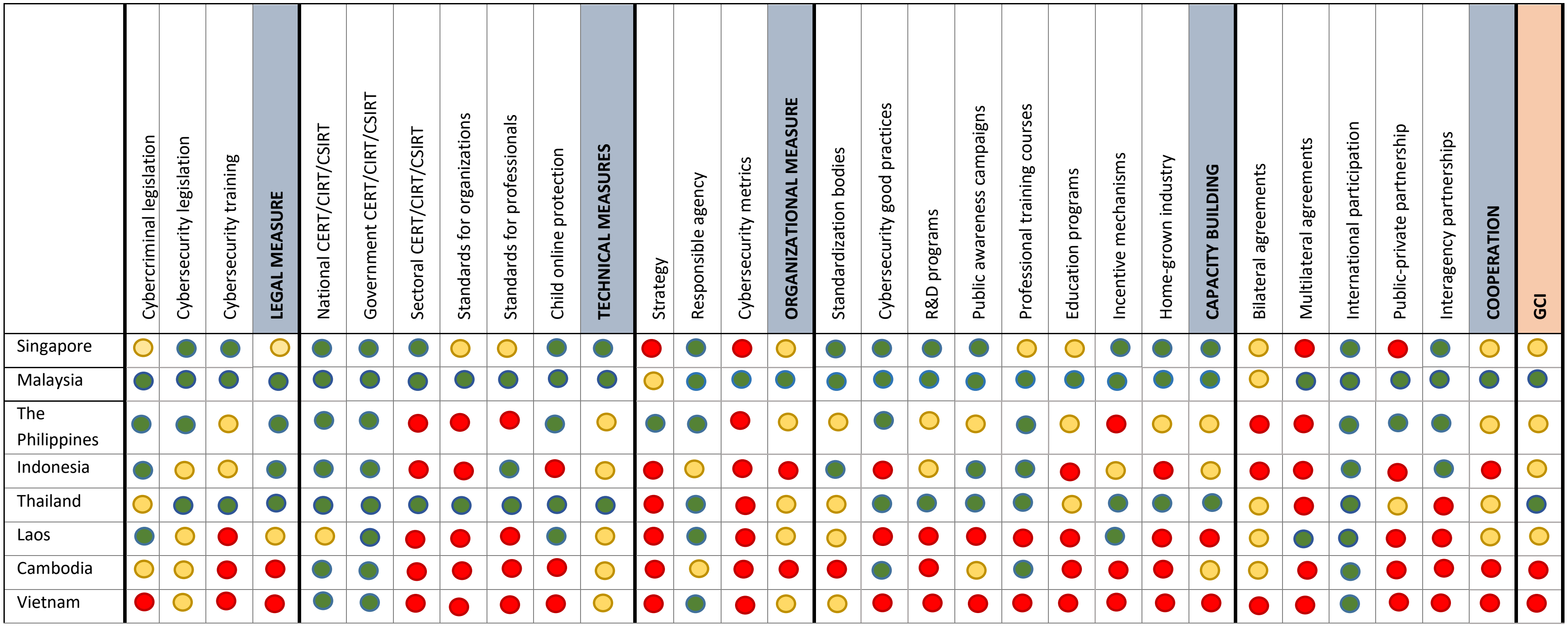
	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	LEGAL MEASURE	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	TECHNICAL MEASURES	Strategy	Responsible agency	Cybersecurity metrics	ORGANIZATIONAL MEASURE	Standardization bodies	Cybersecurity good practices	R&D programs	Public awareness campaigns	Professional training courses	Education programs	Incentive mechanisms	Home-grown industry	CAPACITY BUILDING	Bilateral agreements	Multilateral agreements	International participation	Public-private partnership	Interagency partnerships	COOPERATION	GCI
China	🟡	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🔴	🟢	🔴	🟡	🟢	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🟢	🟡	🔴	🟢	🔴	🟢	🟡	🟡
Hong Kong	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Japan	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🔴	🟢	🟢	🟡	🟢	🟢	🔴	🟢	🟢	🟢
South Korea	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🔴	🔴	🟢	🟢	🟢	🟡	🟢
North Korea	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Figure 2: Global cybersecurity index 2017 of ASIA and PACIFIC region scorecard [5]

Notes: 🟢 : the highest, ○ : no information, 🟡 : low, 🔴 : the lowest

Regarding the [Figure 2], it can be seen that Asian nations like China, Japan, and South Korea have the well-structured organization in cybersecurity. For instance, they established legal frameworks to prevent cybercrime and practice cybersecurity training. The most important thing is that they have stronger data protection regulations than European countries such as China, or Hong Kong. In fact, their data protection regulations restrict the data for the third party outside the border. Furthermore, these countries also had strong capacity building such as best practices, R&D programs, public training courses and the like to enhance the cybersecurity inside. Likewise, they also built several cybersecurity teams like CSIRT, CERT, Gov-CERT, and CIRT to handle the cyber incidents for organizations and individuals. However, their public-private partnership and bilateral agreements in these countries with international cooperation were quite low. The main goal of these countries is that they not only want to protect their national security but also they want to promote their position in cybersecurity aspect with the other countries in the same region; therefore, they focus on building capacity, sharing knowledge, creating cyber-laws, data protection regulations or legal legislation, and so on to mitigate cyber-threats and reduce the damage of cyber-attacks.

Results of cybersecurity capacity in ASEAN countries



	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	**LEGAL MEASURE**	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	**TECHNICAL MEASURES**	Strategy	Responsible agency	Cybersecurity metrics	**ORGANIZATIONAL MEASURE**	Standardization bodies	Cybersecurity good practices	R&D programs	Public awareness campaigns	Professional training courses	Education programs	Incentive mechanisms	Home-grown industry	**CAPACITY BUILDING**	Bilateral agreements	Multilateral agreements	International participation	Public-private partnership	Interagency partnerships	**COOPERATION**	**GCI**
Singapore	🟡	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🔴	🟢	🔴	🟡	🟢	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🟢	🟡	🔴	🟢	🔴	🟢	🟡	🟡
Malaysia	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢
The Philippines	🟢	🟢	🟡	🟢	🟢	🟢	🔴	🔴	🔴	🟢	🟡	🟢	🟢	🔴	🟡	🟡	🟢	🟡	🟡	🟢	🟡	🔴	🟡	🟡	🔴	🔴	🟢	🟢	🟢	🟡	🟡
Indonesia	🟢	🟡	🟡	🟢	🟢	🟢	🔴	🔴	🟢	🔴	🟡	🔴	🟡	🔴	🔴	🟢	🔴	🟡	🟢	🟢	🔴	🟡	🔴	🟡	🔴	🔴	🟢	🔴	🟢	🔴	🟡
Thailand	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🔴	🟡	🟡	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🔴	🟢	🟡	🔴	🟡	🟢
Laos	🟢	🟡	🔴	🟡	🟡	🟢	🔴	🔴	🔴	🟢	🟡	🔴	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟡	🟢	🟢	🔴	🔴	🟡	🟡
Cambodia	🟡	🟡	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🔴	🟢	🔴	🟡	🟢	🔴	🔴	🔴	🟡	🟡	🔴	🟢	🔴	🔴	🔴	🔴
Vietnam	🔴	🟡	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴

Figure 3: Global cybersecurity index 2017 of ASEAN scorecard [5]

Notes:🟢: the highest, 🟡 : low, 🔴 : the lowest

As can be seen in [Figure 3], Singapore and Malaysia are the strongest countries in ASEAN in capacity building, legal measure, technical measure and cooperation in the same region. In addition, their cybersecurity capacity is nearly equivalent to Japan, China, and South Korea. In another hand, Cambodia, Laos, and Vietnam are the weakest nations in every aspect in cybersecurity capacity building. These nations suffered heavy consequences from the war in the past for many years; therefore, it influenced their economic development, social life, especially in technology development. This leads these nations to take a lot of time to reconstruct the infrastructure system, develop the economy, military, capacity building, and technology. As a result, their cybersecurity capacity building is the lowest in the same region. Besides, the lack of expert, technology, and budget are also important problems for the less digitally developed nations to build strong cybersecurity strategy and capacity building in cybersecurity or cyber-defense.

The most successful thing of this thesis dissertation is that it reaches the aims of the research when it offers clear answers for four important hypotheses, as follows: 1) ***Hypothesis 1 (H1)**:* Cybersecurity in Visegrád countries shares similarities in goals, strategies, and strength to align with European Union Member States regarding armed forces, cybersecurity, and national security. 2) ***Hypothesis 2 (H2)***: Cybersecurity in the East Asian and the South East Asian countries aim to create a more secure society and supports economic development. 3) ***Hypothesis 2a (H2a):*** Singapore's cybersecurity strategy may be adapted to Vietnam's legal framework. 4) ***Hypothesis 3 (H3)**:* Cybersecurity, especially in cybersecurity cooperation in Visegrád countries may be adapted and networked with Asian countries, particularly in Vietnam and its neighbors.

New results findings

1) For **H1:** I analyzed and compared the cybersecurity strategies of Visegrád countries through their documents, cyber-laws and so on. I clarified the differences amongst V4 countries in protecting national security strategies, institutional backgrounds, and political plans. I figured out the major difficulty of these countries is the lack of experts in the public and private sector. In another hand, I recognized that they have the same main aims to ensure national security level and contribute to cybersecurity agendas of EU and NATO. In addition, I found out the common security threats of Visegrád countries towards their national security level such as terrorism, cyber-attacks, international immigration, regional conflicts, and transnational crimes, interruption of supplies of raw materials or energy, and natural disasters. As a result, I determined the V4 cooperation not only help themselves but also promote EU and NATO in security structure in cybersecurity, cyber-defense more effectively. Moreover, this cooperation enriches the power of V4 nations in supporting military capabilities, armed forces, cyber-defense, energy supplement, cybersecurity as a nation in the EU.

2) For **H2 and H2a**: I introduced several particular East Asia and the South East Asian countries' cybersecurity situation. Based on the main challenges, aims and cybersecurity capacity in protecting cyberspace, I defined two main groups like several strong nations in cybersecurity's capacity building and the weak ones. I considered that the strong cybersecurity

capacity nations including China, South Korea, North Korea, Japan, Hong Kong, Singapore, and Malaysia have an early cybersecurity strategy, strong cybersecurity policy as well as cyber-laws, legal framework to handle the cyber-threats. In contrast, I pointed out the important problems of the weak cybersecurity capacity building countries (the Philippines, Thailand, Cambodia, Indonesia, Cambodia, and Vietnam) are the inadequacy of technology, experts, and budgets to build strong cybersecurity strategy and capacity building in cybersecurity and cyber-defense. Otherwise, the author distinguished that Singapore cybersecurity strategy can be used for Vietnam's legal framework.

3) For **H3**: I analyzed the common history, geography, and culture of Vietnam and its neighbors (Lao PDR, Cambodia, and Thailand). Then, I found that they are not only similar to culture, suffering heavy damage from the war, history but also they are lack of technology and experts in cybersecurity aspect. Moreover, they are less digitally developed countries, low cybersecurity awareness, capacity building, and high challenges in global cyber-threats. Consequence, I highly believe that the cooperation of A4 nations can enhance their cybersecurity capabilities, mitigate the damage from cyber-attacks. Additionally, I analyzed the cooperation of Visegrád countries and I figured out these countries were also the same in some aspects like A4 group such as small countries, close geography, history, culture, security problems, and so on. This cooperation supported each nation in V4 group in many aspects; therefore, I highly believe that the cooperation amongst Vietnam and its neighbors not only supports for each nation but also contributes to ASEAN members' development in many areas. Fortunately, Vietnam is one country which has cooperation with the Czech Republic in cybersecurity. As a result, when Vietnam and its neighbors cooperate together, they can share technology, best practices in cybersecurity or cyber-defense more conveniently and effectively. After all, I strongly agree that the cybersecurity cooperation of V4 can be applied and networked with Asian countries, especially Vietnam and its neighbors.

Furthermore, main problems in cybersecurity of Vietnam and its neighbors are reported. Due to lack of technology, experts and legal national cybersecurity strategy; Vietnam and its neighbors are the targets of a lot of cyber-attacks every year. In addition, sharing cyber incidents or best practices is also major difficulty amongst the ASEAN members because they are non-state or federal cooperation, different perceptions about cybersecurity and lack of trust; therefore, it is highly hard to give the decision in time towards the cyber-attacks. Besides, ASEAN nations almost are developing countries; consequently, their infrastructure is quite low to approach the new technology in order to prevent, protect or mitigate the cyber-attacks. On the other hand, the main key point is that the author proposes two options for enhancing cybersecurity strategy for Vietnam; for instance, Singapore cybersecurity strategy may be adapted for Vietnam's legal framework and Visegrád countries' cybersecurity strategies also can be used for Vietnam and its neighbors in cybersecurity cooperation.

4.2. Scientific contributions of the thesis

The thesis has reached its purposes: it generally overviewed the types of cybercrime (man-made attacks and machine-made attacks) and cyberwarfare towards the national security, the negative and different impacts of them to the security at the government level and citizens’ life; especially in economy, finance and information infrastructure system of a nation. Moreover, this thesis particularly showed the bilateral and multilateral cooperation among Asian countries in security and economy, as well as in trade, economy, military, energy, peace, friendship and diplomacy for ASEAN nations.

The most important ***professional contribution*** of the thesis is that it gives significant differences in cybersecurity cooperation between Asia and the EU. For example, in Asia countries, cybersecurity cooperation mainly focused on sharing the information and knowledge to prevent the cyber-attacks towards economy via several private sectors in finance and intelligence because of non-state political connection. In contrast, in EU nations, they have the same legal framework, standards, strategies, and regulations; therefore, their cybersecurity cooperation not only concentrates on the safety of politics but also on the security of the cyberspace to reduce the damage and protect their national sovereignty or national security. In addition, data protection regulations or data policy in several ASIA countries are more secure than GDPR in EU because they restrict the third party outside the host country access the data.

Furthermore, the doctoral thesis'***scientific contribution*** is that it made clear the cybersecurity cooperation amongst V4 countries considered as one nation's power in the center of EU in order to strengthen national stability, decrease the cyber-threats, enhance the relationship and improve the cybersecurity, cyber defense or other future challenges between EU, NATO and other organizations. Likewise, there are several organizations like ENISA, NATO, the Three Seas Initiative, and E3PR which offer general legal frameworks (GDPR, NIST 800-53, NIS directive, Digital Single Market Initiative, and CPPP) in cybersecurity cooperation strategies for EU countries.

In this thesis, it also has ***an additional contribution*** which is the general overview of ASEAN nation's cybersecurity strategy and its current cyber issues or challenges. Simultaneously, it expressed that the weakness in responding towards cyber incidents and low awareness about the importance of national information cybersecurity of some countries because of the inadequacy of cybersecurity cooperation with the others in the same region.

5. DISCUSSION AND SUGGESTIONS

❖ *Option 1: Singapore cybersecurity strategy can be adapted in Vietnam*

Firstly, Singapore is one of ASEAN countries and a small country with its population approximately 5.792 million people in 2018; nonetheless, the technology development's speed is extremely high and it quickly becomes not only a massive technology hub but also finance center in the world. In fact, its global cybersecurity index (GCI) in 2017 was the first rank in the world with a score of 0.925 [5]. Due to the aim of building the Smart Nation infrastructure, Singapore spent a lot of budgets 1% of GDP on R&D for scientific and technology research [6]. Meanwhile, Vietnam is a developing country with crowded population and high speed approaching in technology; as a result, Vietnam government needs to build the concrete and resilient infrastructure systems for government and officials similar to Singapore [7]. For instance, they may create the government networks for e-government and e-business to keep important services and let the participation of all stakeholders – government, private sectors, security community in order to ensure the safety of sharing information among them. Besides, the government desires to implement several programs or projects to protect critical infrastructure information from cyber threats. Additionally, enhancing cyber capability and improving the legal framework to address cyber threats are also urgent requirements. For instance, Vietnam government may establish more cyber laws, Acts or Decrees, especially national cybersecurity strategy which declare responsibilities and function of agencies, operators, private sectors and public sectors to safeguard their system, networks and protect government system and citizens as well. Secondly, Vietnamese requires to encourage the cooperation of private sectors like VNISA, VSISA, VIA, VEA, VAIP, BKAV, white hacker teams and the like with public sectors (VNCERT) to share cybersecurity bills, exercises or experiences in order to increase cybersecurity awareness for citizens, officials, and organizations towards cyber-threats; and know- how to protect sensitive data or information. Indeed, in 2017, according to Vietnamese Ministry of Information and Communication (MIC), Vietnam ranked 16th out of 20 countries in using Internet in ASIA with approximately 53% Internet users over the population; however, based on the International Telecommunication Union (ITU) and Global cybersecurity index (GCI) in the same year, Vietnam ranked 101th of 193 countries in network security [8]. For this reason, the role of education in cybersecurity is an essential and urgent requirement to raise the safety and security information's awareness for every individual or organization through training, contests, or educational programs in school or universities. Thirdly, Vietnam needs to build more institutions, training centers or universities to train or educate the experts in cybersecurity aspect. In 2017, according to the Vietnamese Department of Information Security and Communication, there was 8 institutions or universities which recruited the students in information security and 953 IT security engineers in the whole nation [9]. Finally, the Vietnamese government requires to expand the international cooperation in cybersecurity with several developed countries in the same region like Singapore, Malaysia, Japan or other regions like EU and USA.

❖ ***Option 2: Visegrád countries cybersecurity strategies can be adapted towards Vietnam and other neighboring countries.***

In ASEAN nations, Vietnam, Thailand, Lao PDR and Cambodia (**A4**) are the small and developing countries which have quite weak cybersecurity in the same region. However, they have several similar aspects such as social, geography position, agriculture and rice cultivation, and historical development.

Cybersecurity states in A4 (Thailand, Lao PDR, Cambodia and Vietnam)

According to GCI 2017 [5], Thailand and Lao PDR were on the same "Maturing" stage with Visegrád countries (Czech Republic, Poland, Hungary, and Slovakia) in cybersecurity, meanwhile, Cambodia, and Vietnam were still in the "Initiating" stage countries. In fact, Thailand was the highest nation in comparison with V4 and its neighbors in GCI 2017- ranked the 20th, Czech Republic 35th, Poland 33rd, Hungary 51st Slovakia 82nd, Lao PDR 77th, Cambodia 92nd, and Vietnam 101st, respectively. Thus, Thailand can be the leader of the **A4** group in cybersecurity cooperation like Poland's role in V4 cooperation. Currently, Thailand, Lao PDR, and Vietnam already have standalone cybersecurity laws but Cambodia has a draft in cybercrime law and it has not affected yet [10]. Nevertheless, these countries signed MOU among CERTs to enhance the cybersecurity against cyber – attacks. Hence, when the cooperation amongst these countries is established, this may support cyber policy development, enhance capacity building and facilitate operational issues in preventing cyber-attacks and promoting cybersecurity for these nations and ASEAN in general.

❖ *Child online protection*

Nowadays, there are many types of crimes related to children such as child pornography, sexual exploitation, child trafficking, child labor, forced marriage, prostitution, and so on [11]. Particularly, these crimes usually occur in the developing countries in ASEAN such as Lao PDR, Vietnam, Cambodia, Thailand, and Myanmar. In fact, in Thailand, children are traded from Cambodia, Lao PDR and Myanmar with the aims for labor trafficking, sexual exploitation and forced begging [11] because it is quite easy to enter Thailand via the border by various means of transportation from these countries. In addition, according to the United Nations Office on Drugs and Crime (UNODC) reported that Vietnamese children trafficking victims were found in neighbor countries. According to the International Telecommunication Union (ITU), Child online protection is a global issue which needs the cooperation of all nations at the international level. It also clarifies five major keys to protect and develop child online protection such as "legal measures, technical and procedural measures, organizational structures, capacity building, and international cooperation" [12]. ITU started the Child Online Protection (COP) Initiative in 2008 within the Global cybersecurity agenda framework [13]. It supports the Member States, especially in developing countries to promote and deploy guidelines for COP initiative. At present, Thailand, Cambodia, and Vietnam are the members of ITU except for Lao PDR; as a consequence, with the cooperation of A4, this cooperation helps not only Lao PDR but also four nations in improving public awareness; sharing best practices, tools, and resources to adapt in each countries; clarifying policies, risks and vulnerabilities; and enhancing the capacity building in protecting child online [14].

❖ *Human trafficking*

Human trafficking refers to three main types such as sexual exploitation, labor exploitation and organ trafficking [15], [16]. According to UNODC, the human trafficking victims found in East Asia and the Pacific more than 85 percent, 6 percent from South Asia. Besides, trafficked victims from Indonesia, the Philippines, and Vietnam were mostly found in Malaysia while the human trafficking people from Cambodia, Lao PDR and Myanmar were recognized in Thailand [17]. However, in 2015, on the 27th ASEAN SUMMIT, it established the ASEAN Convention Against Trafficking in Persons, Especially Women and Children to combat against trafficking in person, especially women and children (ACTIP) [18]. This convention requires at least six members of ASEAN countries to ratify it in order to go in to effect. Until now, Thailand, Lao PDR, Singapore, Cambodia, Vietnam, and Myanmar have ratified on the convention against human trafficking. It is visible that four countries of A4 have ratified the convention to fight against human trafficking, as a sequence, this can increase public awareness of trafficking in persons, people smuggling and transnational crime for each other and other ASEAN countries in the same region.

In another hand, A4 countries are also members of the International Criminal Police Organization (INTERPOL) – an inter-governmental organization with 194 members located in Singapore [19]. This organization gives technical and operational support to help police amongst members in sharing and accessing data on crimes and criminals. In addition, this organization mainly focuses on three crime's programs such as counter-terrorism, cybercrime, and organized and emerging crime. Human trafficking is one kind of international organized crimes which Interpol helps its members to counter against. Hence, with the cooperation of A4, it can help these countries prevent human trafficking themselves and it can contribute to Interpol operations and the other members in the same region.

❖ ***Economics***

As the author mentioned above, Thailand, Laos, Cambodia, and Vietnam are Indochina countries and they have the same water rice cultivation culture. Moreover, their large contribution to the economy based on the export of agricultural products. For example, in 2017, the Gross Domestic Products (GDP) per capita of these countries was Thailand 6,125$ USD, Lao PDR 1730.40$ USD, Cambodia 1,379.34$ USD, and Vietnam 1834.65$ USD, respectively [20], [21], [22], [23]. Remarkably, Thailand ranked the 2nd after Indonesia, while Vietnam ranked the 6th, Lao PDR ranked 9th, and Cambodia ranked the 8th about GDP in 2018 [Figure 4]. At present, ASEAN nations have the free trade area (FTA) with some countries such as China, Japan, Republic of Korea, Australia, New Zealand, and India [24]; as a consequence, A4 group may take the advantages of this agreement to boost their competitiveness, trade development, expand cross-border cooperation with the other nations. Besides, Vietnam began a new step in dealing with a free trade agreement between Vietnam and EU (EVFTA) which is on the process for final ratification from European Council before it comes into force [25]. With this agreement, it may bring a lot of benefits for both Vietnam and EU members. In fact, Vietnam is a potential trade partner of EU after Singapore based on heavily exporting products and lower wages labor's price in some aspects such as mobile and electronic products, footwear, textiles and clothing, coffee, rice, seafood, and furniture. In another hand, if this agreement is established, it can open up big opportunities not only for Vietnam but also for A4 group in reducing tariffs on goods, increasing trade competitiveness in the same region, developing economy growth, expanding the market to a new area, and promoting their position in the global.

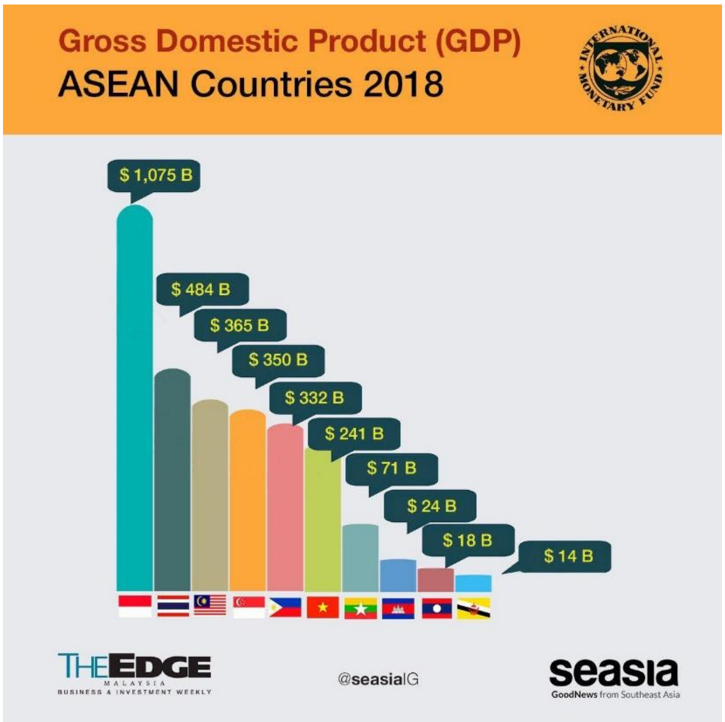


Figure 4: Ranking of GDP Per Capita of Southeast Asian Countries [26]

6. LIMITATIONS

Two limitations of this research include the small amount of data and time. Firstly, the research data were limited because this topic to date was quite new. Moreover, security information is sensitive information; therefore, it has some security restriction issues and it is not public information on public media communication or international publications. In addition, the formulation of every nation's new security strategy is related to national security; as a result, it cannot completely reveal for every individual even the citizen of that nation. Furthermore, there is the only available dataset and the official legal data document source which is Global Cybersecurity Index including statistical data; as a consequence, it is also a limitation of collecting and making statistics for data. Because of these reasons, the author could not obtain adequate data as much as the desired one. Secondly, due to time limitation, only a limited number of interviews was conducted with cybersecurity experts in order to obtain more valuable guidance and information. Hence, if given more time, data, and interviews, this research may provide a broad picture of the findings of the study.

7. LIST OF PUBLICATIONS

International journal

[1]. Nguyen Huu Phuoc Dai, Kerti Andras and Rajnai Zoltán**.** *E-learning security risks and its countermeasures*. Emerging Research and Solutions in ICT 1 (1):17-25, Doi: 10.20544/ERSICT.01.16.P02, Macedonia, April, 2016.

[2]. Nguyen Huu Phuoc Dai. *Fingerprint device (Suprema), Is safe or not*? HADMÉRNÖK XI: (4): 10-18. (ISSN: 1788-1919), Hungary, November, 2016.

[3]. Nguyen Huu Phuoc Dai, Phan van Thanh. *The Role of E-Learning in Sustainable Business: A Case Study in Vietnamese SMEs,* Doi: https://doi.org/10.19275/RSEP020 (pp 99-105), (ISSN:2149-9276), Barcelonia, Spain, November, 2017

[4]. Nguyen Huu Phuoc Dai, Rajnai Zoltán. *The current state of information communication technology in critical infrastructure: the case of Vietnam*. HADMÉRNÖK XII: (4): 173-179. (ISSN: 1788-1919), Hungary, December, 2017.

[5]. Nguyen Huu Phuoc Dai, Lourdes Ruiz, Arnold Őszi. *Biometrics acquisition in a Hungarian university. The Óbuda University case - Bánki Donát Faculty*. BÁNKI KÖZLEMÉNYEK: (1): 30-34. Hungary, 05th, March, 2018

[6]. Nguyen Huu Phuoc Dai, Dang Thai Binh. *The impact of ecommerce in Vietnamese SMEs*. European Journal of Business Science and Technology (2): 90-95, ISSN 2336-6494, Doi: https://doi.org/10.11118/ejobsat.v3i2.106, December, 2017

International conferences

[7]. Nguyen Huu Phuoc Dai and Rajnai Zoltán**.** *General audit of the infrastructure, improvements in network security features, fixing potential security holes in small company*. Proceedings of International conference on applied internet and information technologies, ICAIIT October, 2015, Zrenjanin, Serbia, and ISBN: 978-86-7672-260-0.

[8]. Nguyen Huu Phuoc Dai, Duong Van Thinh and Rajnai Zoltán. *Learning attitude in XXI century*. SAMI 2016, IEEE 14th International Symposium on Applied Machine Intelligence and Informatics, Herl'any, Slovakia 21st - 23rd January, ISBN: 978-1-4673-8739-2.

[9]. Nguyen Huu Phuoc Dai and Duong Van Thinh. *E-Learning methods in XXI century*. Proceedings of the XXI- The international scientific conference of young engineers, March, 2016, ISSN: 2393-1280.

[10]. Nguyen Huu Phuoc Dai, Rajnai Zoltán and Dang Thai Binh**.** *The impact of e-learning towards small and medium sized enterprise in Vietnam.* 3rd International Conference on Finance and Economics, ICFE 2016, 15th-17th June, Viet Nam, ISBN: 978-80-7454-598-6

[11]. Fehér Dávid János, **Nguyen Huu Phuoc Dai.** *Security concerns towards Security Operations centers.* IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI 2018), Romania, 2018.05.17-2018.05.19, IEEE Hungary Section; IEEE Romania Section, 2018. pp. 273-278. (ISBN: 978-1-5386-4639-7). Doi: 10.1109/SACI.2018.8440963.

Project

[1]. Nguyen Huu Phuoc Dai, Rajnai Zoltán. *The Current Security Challenges of Vehicle Communication In The Future Transportation system.* SISY 2018 - IEEE 16th International Symposium on Intelligent Systems and Informatics, September 13-15, 2018, Subotica, Serbia, ISBN: 978-1-5386-6841-2 (EFOP-3.6.2-16-2017-00016 project in the framework of the New Széchenyi Plan 2020 - funded by the European Union and co-financed by the European Social Fund).

Publications related to the dissertation

1. Nguyen Huu Phuoc Dai and Rajnai Zoltán. *General audit of the infrastructure, improvements in network security features, fixing potential security holes in small company*. Proceedings of International conference on applied internet and information technologies, ICAIIT October, 2015, Zrenjanin, Serbia, and ISBN: 978-86-7672-260-0.

2. Fehér Dávid János, **Nguyen Huu Phuoc Dai**. *Security concerns towards Security Operations centers.* IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI 2018), Romania, 2018.05.17-2018.05.19, IEEE Hungary Section; IEEE Romania Section, 2018. pp. 273-278. (ISBN: 978-1-5386-4639-7). Doi: 10.1109/SACI.2018.8440963.

3. Nguyen Huu Phuoc Dai, Rajnai Zoltán. *The current state of information communication technology in critical infrastructure: the case of Vietnam*. HADMÉRNÖK XII: (4): 173-179. (ISSN: 1788-1919), Hungary, December, 2017.

4. Nguyen Huu Phuoc Dai, Dang Thai Binh. *The impact of ecommerce in Vietnamese SMEs.* European Journal of Business Science and Technology (2): 90-95, ISSN 2336-6494, Doi: https://doi.org/10.11118/ejobsat.v3i2.106, December, 2017

5. Nguyen Huu Phuoc Dai, Rajnai Zoltán and Dang Thai Binh**.** *The impact of e-learning towards small and medium sized enterprise in Vietnam.* 3rd International Conference on Finance and Economics, ICFE 2016, 15th-17th June, Viet Nam, ISBN: 978-80-7454-598-6

8. REFERENCES

[1] W. E. Forum, *The Global Risks Report 2019 13th Edition*, vol. 14, no. 1. 2018.

[2] P. Kleve, R. De Mulder, and K. Van Noortwijk, “The definition of ICT Crime,” *Comput. Law Secur. Rev.*, vol. 27, no. 2, pp. 162–167, 2011.

[3] M. D. G. and S. W. Brenner, “The emerging consensus on criminal conduct in cyberspace,” *World*.

[4] G. Wacker, “Security Cooperation in East Asia. Structures, Trends and Limitations,” no. May, 2015.

[5] ITU, *Global Cybersecurity Index & Cyberwellness Profiles 2017*. 2017.

[6] T. Macaulay, “How the Singapore government supports the country’s tech scene,” 2018. [Online]. Available: https://www.cio.com/article/3299480/how-the-singapore-government-supports-the-country-s-tech-scene.html.

[7] Cyber Security Agency of Singapore, “Simgapore’s Cyber Security Strategy,” no. 12, p. 2015, 2011.

[8] ICTNews, “Việt Nam xếp thứ 101 trên 193 nước về khả năng đảm bảo an ninh mạng,” 2017. [Online]. Available: https://ictnews.vn/cntt/bao-mat/viet-nam-xep-thu-101-tren-193-nuoc-ve-kha-nang-dam-bao-an-ninh-mang-160652.ict.

[9] Bnews, “Nhân lực ngành an toàn thông tin mạng cần cả ‘lượng’ và ‘chất,’” 2018. [Online]. Available: https://bnews.vn/nhan-luc-nganh-an-toan-thong-tin-mang-can-ca-luong-va-chat-/77086.html.

[10] Z. Reed Smith LLP - Charmian , Aw ; Xiaoyan, “Southeast Asian nations to form regional framework for cybersecurity cooperation,” 2018. [Online]. Available: https://www.lexology.com/library/detail.aspx?g=844560db-ad55-48e9-aafb-ad5328c192a9.

[11] UNDOC Regional Office for Southeast Asia and the Pacific, Thailand Institute of Justice, and United Nations Office on Drugs and Crime, “Trafficking in Persons from Cambodia, Lao PDR and Myanmar to Thailand,” *United Nations Off. Drugs Crime*, no. August, 2017.

[12] ITU, “About the Child Online Protection Initiative,” 2019. [Online]. Available: https://www.itu.int/en/cop/Pages/about_cop.aspx.

[13] T. Carla, Licciardello; Amanda, “Celebrating 10 years of Child Online Protection,” 2018. [Online]. Available: https://news.itu.int/celebrating-10-years-child-online-protection/.

[14] S. Framework, “Statistical Framework and Indicators 2010 ITU-D,” 2010.

[15] ASEAN, “ASEAN Plan of Action against Human trafficking,” p. 302.

[16] ASEAN, “Asean trafficking Law 1.PDF.” .

[17] M. Ismail, “ASEAN: Epicentre of human trafficking,” 2018. [Online]. Available: https://theaseanpost.com/article/asean-epicentre-human-trafficking.

[18] T. globla initative A. transnational O. Crime, “ASEAN & ACTIP: Using a Regional Legal Framework to Fight a Global Crime,” 2017.

[19] INTERPOL, “What is INTERPOL?,” 2019. [Online]. Available: https://www.interpol.int/en/Who-we-are/What-is-INTERPOL.

[20] T. Economics, “Thailand GDP per capita 2017,” 2019. [Online]. Available: https://tradingeconomics.com/thailand/gdp-per-capita.

[21] T. Economics, “Lao PDR GDP per capita 2017,” 2019. [Online]. Available: https://tradingeconomics.com/laos/gdp-per-capita.

[22] T. Economics, “Cambodia GDP per capita 2017,” 2019. [Online]. Available: https://tradingeconomics.com/cambodia/gdp-per-capita.

[23] T. Economics, “Vietnam GDP per capita 2017,” 2019. [Online]. Available: https://tradingeconomics.com/vietnam/gdp-per-capita.

[24] ASEAN Secretariat, “Free Trade Agreements with Dialogue Partners in ASEAN,” 2018. [Online]. Available: https://asean.org/asean-economic-community/free-trade-agreements-with-dialogue-partners/.

[25] V. News, “Vietnam Free Trade Agreement (EVFTA) heralds new chapter for Vietnam -EU relations,” 2019. [Online]. Available:

https://vietnamnews.vn/media-outreach/484633/vietnam-free-trade-agreement-evfta-heralds-new-chapter-for-vietnam-eu-relations.html#z1041pQF3K2kLivY.97.

[26] A. Salikha, “LATEST: 2018 Economies & Ranking of GDP Per Capita of Southeast Asian Countries,” *2018*. [Online]. Available: https://seasia.co/2018/08/10/latest-2018-economies-ranking-of-gdp-per-capita-of-southeast-asian-countries.