ISSN 2630-0540
Journal of Technology and Innovation in Tertiary Education, Vol.1, No. 2, pp. 37-45, July-December 2018

doi: …../jti…….

The Conception of Cybersecurity in Thailand

Jakkrit Chuamuangphan
Pridi Banomyong International College
Thammasat University, Bangkok, Thailand.
Email: Jakkirt_167@hotmail.com)

Abstract

The National Statistical Office of Thailand (NSO) reported that the Internet penetration in Thailand increased from around twenty-nine percent in 2013 to almost fifty percent in 2016, which means that half of the population in Thailand now have access to the Internet. Following the rapid use of cyberspace, the Internet is now treated as a space for social and economic activities. It now plays a key role in the expansion of digital economy in the digital society. However, it also potentially poses a threat to cyberspace. As a consequence of higher Internet penetration in Thailand, the government regards cyberspace as a territory that needs to be protected due to cyber threats which can cause a cascading effect ranging from individual, society and the government to the international level. In fact, the Thai Government has intensified its efforts in controlling information available on the Internet. This paper presents *the theoretical framework* for *analysis of Securitization* from a *constructivist's point of view* in seeing how *the conception of cybersecurity* itself is constructed or given meaning in Thailand.

Keywords: *Cybersecurity, Securitization Theory, Thailand's Cybersecurit*

1.Introduction

Bitdefender, an Internet security company, reported that Thailand has ranked fifth out of a total of 25 countries in Asia for cyber security risks in 2017 (Leesa-nguansuk, 2016). In the same year, Kaspersky Lab also mentioned that Thailand has become one of the prime targets for cyber-attack in Southeast Asia (Limsamarnphun, 2017). With all the risks from an inevitable growth of the Internet penetration in Thailand, the National Statistical Office of Thailand (NSO) emphasized that the Internet penetration in Thailand increased from around twenty-nine percent in 2013 to almost fifty percent in 2016, which means that half of the population in Thailand now have access to the Internet with more than ninety percent connected to the Internet via smartphone (National Statistical Office of Thailand, 2016). Moreover, Thailand is one of the world leaders in spending time on the Internet and mobile phone per day. It has ranked fourth globally with users' record of 9.38 hours on the Internet per day, after the Philippines, Brazil, Indonesia and South Africa (Leesa-nguansuk, 2018).

A consequence of high Internet penetration in Thailand and a great number of social media users, is seen in popularity of online consumption that spurs the economy to grow digitally, in a new space known as *cyberspace*. However, there are also increasing cyber threats. For example, Thai local authorities caught an Algerian considered to be one of the world's top-20 bank hacking criminal masterminds, responsible for defrauding tens of millions of dollars from computer networks of 217 banks in the world (Yao, 2015). In 2016, the state-owned Thai Government Savings Bank was hacked and 12.29 million baht and 21 ATMs were stolen. More than 3,000 ATMs were temporarily shut down for

inspection. In the same year, six Thai government's websites were hacked by those who have vowed to launch a cyber war against the government due to the endorsement of the new Computer Crime Bill and Single Gateway Policy (Fairfield, 2016). In another case, Burmese hackers said that they attacked the Thai government websites because Thailand sentenced two Burmese to death for the murder of two British backpackers (Holmes, 2016). These are cyber incidents that posed a threat to cyberspace. Cyberspace is now treated as a *country territory* under national protection. Thus, it is the role of the Thai government to safeguard its cyberspace to ensure growth of digital economy of the country.

In so doing, the Thai government has been trying to secure the new domain of cyberspace. The government has launched the Digital Development Plan for Economy and Society initiated by the Committee on Preparations for Digital Economy and Society, chaired by Prime Minister, General Prayuth Chan-ocha. The Digital Economy policy covers 20 years of an administrative reform in order to establish the digital foundation of the country and to introduce digital technology in all sectors of the country with cybersecurity as part of the policy. The Electronic Government Agency (EGA) under the Ministry of Digital Economy and Society of Thailand has defined Digital Economy as an economy/ society which uses communications technology or digital technology to drive into action the reformation of production processes, business operations, services, education, public health, and the government administration. Included are business and social transactions which directly affect the economic development and quality of life of the workforce. Thailand's Digital Economy policy consists of five main strategies: (1) Hard Infrastructure, (2) Soft Infrastructure, (3) Service Infrastructure, (4) Digital Economy Promotion, and (5) Digital Society and Knowledge Resource (Souche et al., 2015).

Cybersecurity policy and law were initiated in support of the Soft Infrastructure Strategy of Digital Economy by the purview of EGA. In so doing, ETA as a primary organization has developed a series of legislations related to the Digital Economy Policy. There are eight drafted laws proposed by ETA and approved by the Cabinet on 16 December 2014. Currently, there are three bills already enacted and published in the Gazette: (1) Reorganization of Ministry, Sub-Ministry, and Department Act for Ministry of Digital Economy and Society, (2) Digital Development for Economic and Social Development Act, and (3) Computer Crime Act (amendment). The other five drafted versions include: (1) Personal Data Protection Act, (2) Electronic Transactions Act (amendment), (3) Digital Development for Economy and Social Development Act, (4) Broadcasting and Telecommunication Regulator Act (amendment), and (5) Electronic Transaction Development Agency Act (amendment).

As Thailand is now forming the cybersecurity law and policy with its foremost eagerness. Thus arises *the question on how we can understand the emerging conception of Thai cybersecurity*. In this regard, the theoretical framework is required for an analysis of Securitization theory from a constructivist's point of view in examining the question.

2. The Definition of *Security* and *Cybersecurity*

The conception of security is so diverse. The traditional notion of security is mainly about the well-being of the nation. Walter Lippmann (1943) asserted that the nation has *security* when it does not have to sacrifice its legitimate interests to avoid war, and is able, if challenged, to maintain them by war. Thus, the traditional meaning of *security* refers to the nation's well-being in political and military affairs. Later on, especially after cold war era, the world has changed, and so has the notion of security. To Hotoshi (2011), security has become much more complex and has broadened its owns field beyond the traditional political and military sector. It is interesting that

constructivists like McDonald (2008) suggested that the world is constituted socially through *intersubjective interaction*, which means that agents and structure in society are mutually constituted with norms of identity and ideas or even a speech acts; such norms designate the particular issues or actions as existing threats. This notion can affect *security* as a social construction. To understand the emergence of an idea considered *security*, one has to perceive a particular issue being constructed by an act to make it secured. Constructivists studied approaches to study security in the Securitization theory of the Copenhagen School. This school has developed the Securitization theory to approach the construction of *security* based on *speech acts* that designate particular issues or actions as existing threats (McDonald, 2008). The Securitization theory provided *a constructivist operational method* for understanding and analyzing how and when issues become *security issues* (Nyman, 2013).

When the Securitization theory is applied to the study of *cybersecurity*, there are two distinctive ways to look at it as *the security of cyberspace* and *the security of the nation*. According to the dualistic model of "*Technical Computer Security*" and *"Cyber Security*" developed by Helen Nissenbaum (2005), the two models have drawn constructivists' viewpoint influenced by the Securitization concept of the Copenhagen School of International Relations.

The concept of *Securitization* claims that any specific issues can be processed into the security issues when they require emergency actions. This kind of action is called *an act of securitization* or *securitizing moves*. The act or move of securitization is naturally connected with a 'speech act' which is the main mechanism through how security is constructed. The speech act is the product of the 'securitizing actor' who uses the language to express a problem into a security term and tries to persuade an 'audience' to perceive it in the same way. Moreover, the securitizing actor has to possess a 'referent object' that it is a legitimate claim to justify a threat (Buzan et al., 1998). In short, Securitization refers to the process in which an issue is labeled as a "security issue" by the securitizing actor using a speech act to move this issue out of the political sphere.

As mentioned, Nissenbaum (2005) has developed and applied the concept of Securitization to Cybersecurity and out it in the so-called dualistic model of "Technical Computer Security" and "Cyber Security." As shown in Table 1, each model has its own implications and values while, the two conceptions share similar elements in contemporary concerns on the vulnerability of computers and networks to holistic attack. "Technical computer security" is defined by its goals of ensuring information availability, integrity, and confidentiality through the protection of computer systems and users by making the protection of information as the referent of securitization; included are many securitizing actors such as individuals, private institutions, such as private internet security companies, the media, and non-government organizations (NGOs).

On the other hand, "Cyber Security" is defined by its goals of protecting *the state* from the use of networked computers for subversive purposes, actual attacks on critical societal infrastructure dependent on computers, and from the threat of network disablement. As this model focuses on protection of the state, securitizing actors in this model are state or government bodies, and sovereignty of the state. These actors focus on objects that should be protected for national interest. This model therefore allows the state to justify specific measures to curtail freedom of other actors for national security. Their protective actions include centralization of control over networks, mass surveillance, technical barricades to restrict access to online information, and mechanisms to monitor and filter information flows from users.

Table 1: Nissenbaum's Conceptions of Security (Putra & Punzalan, 2013)

	"Technical Computer Security"	"Cyber Security"
Securitizing Actors	Individuals, media, NGOs, business, private internet security companies	State, government organs
Referent objects	Protection of information availability, integrity, and confidentiality	Protection of national interest, classified information infrastructure from subversion, disruptive attacks and network disablement
Measures to attain security	Reduction of security vulnerabilities, strengthening of individual security capacity	Centralization of network control, technical barricades, monitoring and filtering information from users, surveillance and repression of user.

3. The conception of cybersecurity in Thailand

Since the military took over the government in 2014, the bid by the military government to pass *the cybersecurity bill* showed securitizing moves, bringing the cybersecurity into an arena of national security. It is interesting to examine the way the military government linked *cybersecurity* to *national security*.

There are three main elements to be analyzed in the framework of Nissenbaum's Conceptions of Security shown in Table 1:

First, *the securitizing actors* are clearly the heads of the state and the government of Thailand alongside with their defense ministers and ministers of digital economy and society. The senior officials of the Ministry involved in cybersecurity are also considered securitizing actors. These actors are mainly involved in formulating the policy and drafting the cybersecurity bill. We can see these actors in their securitizing moves in the later part of this paper.

Second, the referent object is defined as what the securitizing actors are trying to protect due to its existing threat. In this case *the referent object* of Thailand is *national security*, sovereignty and territorial integrity of Thailand, as stated in the meaning of cybersecurity in the Cybersecurity Bill (draft version 2018). The Cybersecurity Bill states that "Cybersecurity" means measures and operations that are conceived in order to maintain national Cybersecurity, enabling it to protect, prevent and promote in order to tackle circumstances of cyber threats which may affect or pose risks to the service or application of computer network, the Internet, telecommunications network, satellite services, utility network, critical public affairs service—which are the networks at the national level—in ways that affect national security, military security, domestic peace and order, and economic stability (Ministry of Digital Economy and Society of Thailand, 2018). The definition of cybersecurity is related to the meaning of national security, as stated in the National security Act B.E. 2559 (2016). Thailand has defined *National Security* as the state in which the nation is without threat to Sovereignty, Territorial Integrity, Religious Institution, the Monarchy, Public Safety, Safety of the citizens in

daily life, National interest, the democratic regime with the King as the head of the state, including the readiness of the nation in facing any kind of threat (the National security Act B.E. 2559, 2016). According to the statements above, *the securitizing actors* associate the security of the computer system to the national security.

Third, the securitizing moves cybersecurity in Thailand are identified by securitizing actors as referent objects they needed to protect. Those securitizing actors hold the idea that cybersecurity is in fact the safety of the whole nation. Such a view point has stemmed from two elements of the securitizing moves in Thailand as follows:

(1) *External conditions*: it is the context in which the securitizing actors are performing their moves. Thailand had a coup d'etat in 2014 and since then, the political system has been controlled by the military government. The securitizing actors are authorities from the Cabinet, who have created the cybersecurity policy in association with political security and stability. Up to 2018, the parliament consists of 250 members appointed by the National Council for Peace and Order. In 250 members, 145 members are from the Military sector which counts more than fifty percent of the National Legislative Assembly. Thus, it means that new policies or laws focus on security of the military Cabinet rather than national concerns from the actual legislative body (Prachathai, 2017). In particular, the Head of National Council for Peace and Order has also served as the Prime Minister with absolute political power authorized by Article 44 in the temporary Constitution of the Kingdom of Thailand (interim) B.E. 2557 (2014). The Head of the National Council for Peace and Order is authorized to order reforms in any social/ political sectors to strengthen public unity, security and harmony, or prevent/ suppress any acts claimed as undermining public peace, order or national stability. The Head of the National Council for Peace and Order has power to maintain the pillars of the society, ranging from the monarchy, the country's economy and social development, educational systems, cultural preservation and promotion, foreign diplomacy and all matters related to the country's peace and stability. Under such *external conditions*, any orders, acts or any desirable behaviors of citizens are justified as constitutional and conclusive. (Constitution of the Kingdom of Thailand (Interim), 2014).

(2) *Internal conditions:* there have been moves performed with a specific meaning of *securitization* via the rhetoric of the securitizing actors to emphasize national security. Cybersecurity is related to threats to national security.

The rhetoric asserts that *cybercrime* is harmful to the country's national security from both inside and outside the territory. The government has urgently launched a suppressive measure known as as *the Single Gateway Policy* to handle with the current and foreseen problems in cybersecurity. The Single Gateway Policy was secretly included by a committee appointed by the Cabinet by having an amendment in the Computer Crime Act.

Section 1.2 of the Cabinet Resolution on 30 June 2015 reads:

> *"The Ministry of Information and Communication Technology must proceed with the implementation of a single gateway to be used as a device to control inappropriate websites and flow of news and information from overseas through the Internet system."* (KhaosodEnglish, 2015)

General Prawit Wongsuwon, Deputy Prime Minister and Defense Minister, said on 14 December 2016:

> *"The country needs a single internet gateway to cope with "information attacks" launched from other countries ... for the sake of our defense a single*

> *gateway was necessary, because ill-intentioned people with just a mobile phone could send audio to another country, from where they could be transmitted back to the country over the Internet."* (Nanuam, 2016)

The Prime Minister, General Prayut Chan-o-cha asserted on 15 December 2016:

> *"The computer crime act is aimed to delete the flow of illegal information from outside the country especially lèse majesté contents that we cannot delete … so, this computer crime bill is the tool for minimizing the terrorist, threat to security, illegal website and also cyberattack…."* (Khaosod, 2016)

The securitizing actors believe that cybercrime is an existing threat to the nation and freedom of speech in cyberspace is harmful to national security. As cyberspace is the only space of communication left for Thai people to express their opinions to friends and fellowmen. As seen, the aftermath of the 2014 coup has led Thai people inside the country and particularly dissidents to act like online activists in fiercely criticizing the military government. As a result, the Thai government has considered social media as a threat to their security and thus used rhetoric as a tool to retaliate.

A report titled *Social Media and the Threat to National Security* released by the Committee on Armed Forces Group, which is part of the Secretariat of the Senate (2012) reads:

> *"… Social media has tendency to be used as serious threat to the national security in the future."* (Committee on Armed Forces Group, 2012)

The Announcement of the National Council for Peace and Order No. 18/2557 (A.D.2014) states:

> *"All kinds of communication including the online social media is forbidden to share the news that could be a threat to national security"* (National Council for Peace and Order, 2014)

A report of the international media Reuters cites Surachai Srisaracam, Permanent Secretary of the MICT in an interview:

> *"We have blocked Facebook temporarily and tomorrow we will call a meeting with other social media, like Twitter and Instagram, to ask for cooperation from them …. Right now, there's a campaign to ask for people to stage protests against the army so we need to ask for cooperation from social media to help us stop the spread of critical messages about the coup."* (Reuters, 2014)

Another securitizing move of the Thai government is the rapid creation of policies, laws and government agencies. The move has stemmed from the need of the government to take a full control over cyberspace. A good example of such creation is a set of digital economy legislations that surprisingly and quickly secured the Cabinet's approval on 16 December 2014. One of these legislations was the Cybersecurity Bill for the government to limit and to monitor any kind of communications including the Internet (Laungaramsri, 2016). Here are some examples of the government's rhetoric.

In responding to a question from one news reporter on 28 January 2015 about the necessity of the National Cybersecurity Bill, the Prime Minister, General Prayut Chan-o-cha asserted that:

> *"If there is a threat to national security—a violation, or someone committing a crime—we need to empower state officials to investigate."* (The Bangkok Post, 2015)

> *"… the new cyber laws in Thailand are necessary to help protect the nation and will only be used on occasions when the authorities suspect Thailand's national security is at risk."* (Fairfield, 2018)

Moreover, Thailand's Digital Economy and Society (DE) Minister Pichet Durongkaveroj has planned to set up a cybersecurity agency and a hacker training center to serve Thailand's digital economy in justifying its mandate in the Cybersecurity Bill. He asserted:

> *"The government is focusing on digital and IT security because it is very important for the country's protection."* (Apisitniran, 2018)

Another move related to the Cybersecurity Bill is the project called 'cyber warriors' proudly presented by the government as part of making cyberspace safe by militarization as a new domain of warfare. Air Chief Marshal Prajin Juntong, Deputy Prime Minister cum Minister of Justice said on 10 May 2018:

> *"we will install 5,000 cyber warriors within five years…as now we have the Internet, which allows us to communicate in every aspect…both positively and negatively…. We need laws and a department to monitor issues of violations ...including in matters of security, and someone must act on it when there is an infringement."*
>
> *"Digital Economy and Society Ministry will set up a special course, in partnership with the police force, security departments and the National Broadcasting and Telecommunications Commission, and start building the first batch of 200 cyber warriors next month with the budget of 350 million baht."* (Saksornchai, 2018)

These are examples of the securitizing moves in explicit rhetoric--treating *cybersecurity* in aligned with *national security* of Thailand. According to the three elements analyzed in this paper, it can be concluded that Thailand is constructing the *conception of the cybersecurity*, apparently in the model of "Cybersecurity" by Nissenbaum (2015).

4. Conclusion

As shown in this paper, Thailand is constructing the conception of cybersecurity apparently in the model of "Cybersecurity" with three elements of Nissenbaum (2005). The analysis of the three elements explains the way that the Thai government has taken extreme measures on cyberspace, such as censorship, repression, surveillance, and militarization. The government has considered *cybersecurity* as a matter of *national security*. Moreover, the government has treated *cybersecurity* as a threat from Thai dissidents and the opposition groups. The government's severe measures taken against these critics prove its intention as such.

Whether the government's securitization move--for all its intents and purposes--would be successful or not, requires further examination. The analysis of the cybersecurity elements in this study would serve as a springboard for further research into Thai people's perception of the effects of the constructed cybersecurity unique to Thailand.

5. The Author

Jakkrit Chuamuangphan is a Master's degree graduate in the ASEAN Studies Program at Pridi Banomyong International College, Thammasat University, Bangkok,

Thailand. His research interest lies in ASEAN developments as well as issues in cybersecurity and state intervention in security control.

6. References:

Apisitniran, L. (2018). Digital Ministry plans cybersecurity agency Retrieved May 14, 2018 from https://www.bangkokpost.com/business/news/1393674/de-ministry-plans-cybersecurity-agency.

The Bangkok Post. (2015). Prayut defends cyber-security law. Retrieved July 14, 2017 from https://www.bangkokpost.com/news/general/460856/prayut-defends-cyber-security-law (2015)

Buzan, B., Waever, O. and Wilde.J. D. (1998). *Security: A New Framework for Analysis*. Colorado: Lynne Rienner.

Committee on Armed Forces Group. (2012). Social media and the threat to National Security. Retrieved July 14, 2017 from http://www.senate.go.th/w3c/senate/pictures/comm/66/file_135329 8809.pdf.

Constitution of the Kingdom of Thailand (Interim) B.E. 2557. (2014). Retrieved July 14, 2017 from https://www.isranews.org/isranews-article/31533-translation.html.

Fairfirld, J. (2018). Gen Prayut Defends Controversial New Cyber Laws Thailand. Retrieved May 14, 2018 from https://tech. thaivisa.com/gen-prayut-defends-controversial-new-cyber-laws-thailand/3438.

Fairfield, J. (2016). Hackers launch cyber-attack on Thai government websites. Retrieved December 10, 2018 from https://tech.thaivisa.com/hackers-launch-cyber-attack-on-thai-government-websites/19055/.

Hitoshi, N. (2011). The expanded conception of security and International Law: Challenges to the UN Collective Security system. *The Amsterdam Law Forum*, *3*(2).

Holmes, O. (2016). Anonymous hacks Thai police sites over Burmese jailings for British backpacker murders. Retrieved December 10, 2017 from https://www.theguardian.com/world/2016/ jan/06/ anonymous-hacks-thai-police-sites-over-burmese-jailings-for-british-backpacker-murders.

Khaosod. (2016). Gen Prayut ordered the National Legislative Assembly to launch computer crime bill. Retrieved July 14, 2017 from https://www.khaosod.co.th/politics/news_145380. (In Thai).

Khaosod English. (2015). Govt 'Gateway' denials contradict cabinet resolutions. Retrieved July 14, 2017 from http://www.khaosodenglish.com/politics/2015/10/02/1443777645/.

Laungaramsri, P. (2016). Mass surveillance and the Militarization of Cyberspace in Post-Cope, Thailand. *Austrian Journal of South-East Asia Studies*, *9*(2) 195-214.

Leesa-nguansuk, S. (2016). Thailand ranked 5th for threats. *The Nation*. Retrieved July 14, 2017 from https://www.bangkokpost.com/news/security/880236/thailand-ranked-5th-for-threats.

Leesa-nguansuk, S. (2018). Thailand tops internet usage charts. in The Nation. Retrieved May 14, 2018 from https://www.bangkokpost.com/tech/local-news/1408158/thailand-tops-internet-usage-charts.

Limsamarnphun, N. (2017). Thailand prime target for computer attacks cyber-security forum told. in The Nation. Retrieved July 14, 2017 from http://www.nationmultimedia.com/detail/ Economy/30322117 (2017)

Lippmann, W. (1943). *United States Foreign Policy: Shield of the Republic*. Little Brown and Co, University of Michigan .

McDonald, M. (2008). Constructivism, in 'Security Studies: An Introduction' (ed).: Williams, P. D. Routledge, Oxon, 59-72.

Ministry of Digital Economy and Society of Thailand. (2018). Cybersecurity Bill drafted version. Retrieved May 14, 2018 from http://www.lawamendment.go.th/index.php/component/k2/item/1211-2018-03-08-01-17-38 (In Thai).

Nanuam, W. (2016). Prawit Single gateway is a must. in Bangkok Post. Retrieved July 14, 2017 from https://www.bangkokpost.com/tech/local-news/1159396/prawit-single-gateway-is-a-must.

National Council for Peace and Order. (2014). The Announcement of the National Council for Peace and Order No. 18/2557. (In Thai).

National Statistical Office of Thailand. (2016). The Information and Communication Technology Survey in Establishment. Retrieved July 14, 2017 http://web.nso.go.th/en/stat_theme_ict.htm.

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology*, *7*, 61-73.

Nyman, J. (2013). Securitization Theory. In Shepherd, L. J. (ed.). (2013). *Critical Approaches to Security An introduction to Tories and Methods*. Routledge, Oxon, 51-62.

Prachathai. (2017). Junta's reform policies literally copy and pasted Retrieved May 13, 2018, 2018 from https://prachatai.com/english/node/7309.

Putra, N. A. & Punzalan, K. (2013). Cyber Security. In Caballero-Anthony & Cook, A.D.B. (eds). (2013). *Non-Traditional Security in Asia: Issues, Challenges and Framework for Action.* Singapore: ISEAS, 267-289.

Reuters. (2014). Thai ministry sparks alarm with brief block of Facebook. Retrieved July 14, 2017 from https://in.reuters.com/article/thailand-politics-facebook-idINKBN0E80U520140528.

Saksornchai, J. (2018). Govt to buit cyber warriors Army to monitor Netizens Retrieved May 14, 2018 from http://www.khaosodenglish.com/politics/2018/05/11/govt-to-build-cyber-warrior-army-to-monitor-netizens/.

Souche, A., Rueangkul, K., Sachdev, K. & Moore, K. (2015). Thailand's Implementation of a Digital Economy. Retrieved July 14, 2017 from https://www.dfdl.com/wp-content/uploads/2015/09/TAB_Magazine_Issue_4_2015__DFDL__Article_Thailands_Implementation_of_a_Digital_Economy.pdf.

Yao, S. (2015). Asean organizations braced for cyberattack. Retrieved December 10, 2017 from http://www.computerweekly.com/feature/Asean-organizationms-braced-for-cyber-attack.