# An Examination of Thai Government Approach in Cybersecurity

*Tawicha Trakulyingyong and Jirapon Sunkpho*
*Thammasat University*
*tawicha.t@gmail.com, jirapon@tu.ac.th*

## Abstract

Implementing cybersecurity policy is challenging task for every country. The Thai government has implemented roadmap to boost country's economy through its so called "Thailand 4.0" campaign. However, during this Thailand 4.0 campaign, ten bills for supporting digital activities were proposed and under reviews. However, public are skeptical and questioning the government's latest measures. This paper seeks to comment on recent legislative developments pertaining to the regulation of cybersecurity in Thailand comparing with international practices in U.S., Europe, two countries in Asia; China and Singapore. While the government already decided to use the legal approach which aim to restrict online activities through legislation, it should also consider the organizational approach which aims to enforce laws, to promote public-private sectors cooperation, and to educate the public through the establishment of dedicated organizations as a sustainable solution.

## Introduction

In recent years, the Thai government has pledged support for the promotion of Thailand's information and communications technology (ICT) sector, with a series of strategies aimed at developing related infrastructure, accelerating innovation, and transforming the country's economy into one that is based on digital technologies.

Various projects are planned under the initiative, including the delivery of affordable broadband internet access to villages nationwide, national e-commerce platform, the deployment of ICT to improve public services offered by state agencies and digital government. In addition, the country's Cabinet officially approved a project titled "Thailand 4.0" which aims to move Thailand's economy out of its middle income status by facilitating the trade in goods and services through e-commerce (MICT, 2016)

As part of the plan, Ministry of Information and Communication Technology (now the Ministry of Digital Economy and Society) proposed the adoption of eight items of legislation, to support development of the digital economy, which are:

1. Electronic Transaction Bill (amendment)
2. Computer-Related Crime Bill (amendment)
3. Cyber security Bill
4. Personal Data Protection Bill
5. Digital Economy Promotion Bill
6. Digital Development for Economy and Society Fund Bill
7. Broadcasting and Telecommunication Regulator Bill (amendment) and
8. Electronic Transaction Development Agency Bill (amendment).

The main intention of the new batch of laws is officially to push for bigger integration of the internet in governance and state business with the ”digital economy” at the very top of the priority list to make the country more competitive. However, this “digital economy” which heavily relies on technology for business transactions opens an avenue for new threats such as online fraud, hacking and distribution of inappropriate materials. Deterring cybercrime is therefore, necessary for boosting public confidence in performing online transaction. It is therefore a priority for legislators to adopt proper legislation to prevent the use of information and communication technologies for criminal activities. As a result, this set of new laws comes with a slew of sections that essentially results in cyber surveillance and monitoring (Tanakasempipat, 2016).

The center of controversy of these set of law are the amendments to the Computer Crime Act and the new Cybersecurity Bill (Jittip, 2016). These new provisions aims to strengthen the country's existing computer crimes act allows the government to shut down websites and penalize internet service providers who fail to remove any content that considered as illegal or sensitive. However, the public appears not to share the government’s thinking behind this rationale, and before the law was passed, more than 340,000 people signed a petition objecting to the amendments as they believe the new CCA gives excessively broad authority to government agencies to act against online content containing information that is deemed inappropriate (Bangkok Post, 2017).

As Thai government tries to strengthen cybersecurity to further drive economy, preserving the openness of the Internet and fundamental values is another key consideration that the government should carefully manage. It may need to revisit its cyber security strategies and the endorsements. This paper seeks to comment on recent legislative developments pertaining to the regulation of cybercrime in Thailand comparing with international practices in U.S., Europe, China and Singapore.

## Thailand’s cybersecurity landscape

According to Thailand’s National Electronics and Computer Technology Center (Nectec, n.d.), there are about 38 million internet users in Thailand in 2015. The country has experienced 100% growth of internet users from 2010 to 2015. As internet penetration is approaching 60% of its population, risk of cybercrime is becoming more relevant. International Insurer Allianz Global Corporate and Specialty SE (AGCS) said that Nearly 20% of Thailand's cybercrime victims reported losses of over US$ 100,000 in 2015, making the country the world's number two target for computer crime (Bangkok Post, 2016). Another report (Oxford Analytica, 2013) states that most cybercrime in Thailand is fraud, but increasing problems are intrusion (14%) and data gathering (11%). The report further stated that the country is modestly defended: the International Security Management System reports 59 public, state and private enterprises in Thailand have certification for readiness against cyber-attacks. In Japan, this figure is 4,152.

Cybercrime has been raised as an issue the Thai government wants to tackle in order to ensure public confidence in performing online activities. As a result, it considered the current laws to be outdated and cannot keep up with cyber criminals' evolving methods. One of the Government's responses to the perceived risk of criminal activity which either uses the Internet to facilitate or directly commit crime has been to promote interception and surveillance of communications over the Internet. On December 16, 2016, Thailand’s Parliament approved an amendment to the country’s Computer Crime Act of 2007 by a unanimous vote. This Act was amended with the purpose of clarifying its provisions. However, the revised version is even more vaguely-worded than its predecessor, broadening the scope of the government's surveillance and censorship powers (Kanin, 2016). The new CCA is also likely to increase censorship due to its ambiguity because of the broad grounds for offenses “likely to cause damage to the public” under article 14, including “false or partially false” data, “distorted or partially distorted” data, or data likely to “cause public panic” or harm “maintenance of national security, public safety, national economic security, public infrastructure serving the public interest.” Service providers such as social media platforms and Internet Service Providers (ISP) will also be required to delete or otherwise prevent the availability of such content following government notification, or they will also be subject to punishment for that content. Furthermore, new provisions state that the court can order information that is found to be false and having caused damage to other persons or the public to be removed from the Internet and deleted from computer systems. If these articles are enforced arbitrarily, such actions will have dire consequences on research and reporting on contentious topics of public concern, including incidents related to serious state-sponsored rights violations (Kanin, 2016).

Hence, the CCA has faced criticism that it has been exploited as a tool of legal intimidation by the state and others in tandem with defamation suits. It can arguably be used as a tool to suppress political freedom and control the voice of dissents. It has caused alarm among human rights activists as it becomes possible for government agencies to peak into individuals' electronic lives and profiles. According to the Asian Human Rights Commission, the vague wordings in the Act raise questions over the notion of law. The adoption of the Computer Crime Act drastically tightens the chokehold on online expression in Thailand – though the intention is to prevent mishandling the information that could damage others (The Human Right Watch, 2016).

Another measure being proposed is Cybersecurity Bill. It is intentionally designed to protect the Internet system, which is different from the Computer Crime Bill's protection of victims. The Cybersecurity Bill does not emphasize "content" but instead focuses on "computer systems. However, many critics say it would allow authorities to wiretap phones and computers without a court warrant (Channel NewsAsia, 2016). The Bill also features a reporting mechanism for state agencies and/or designated persons in each agency to provide information to the secretary of the committee so it could determine what further actions to take in response to particular cyber threats. Further, where maintaining cybersecurity is necessary—for example, in a case where there may be an effect on financial and commercial stability or national security—the committee may even order a state agency to take particular actions and report as the committee may instruct. The most controversial provision of the Bill relates to accessing personal communications content (Tanakasempipat, 2016). The Bill also would empower officials to access communications information, be it in the form of posts, telegrams, telephones, faxes, computers, or any mechanism or device for electronic communication or telecommunications, for the purpose of cybersecurity. Indeed, commentators around the world have expressed concerns about access to personal communications by state agencies of various countries. These concerns are understandable and legitimate. Nevertheless, current public discourse seems to reflect that policymakers' concerns about terrorism and national security are outweighing traditional concerns about personal privacy.

Besides new and amended legislations being proposed, the National Cybersecurity Committee, a five-person committee will be established. The committee would have the responsibility to determine how to respond to serious cyber threats, effectively serve as the center of operations in the event of an IT calamity and cooperate with other state bodies and private entities for this purpose, among related responsibilities. The Office of the National Cybersecurity Committee would be responsible for implementing the committee's policies, as well as related responsibilities specified in law.

In the next section, the practice of cybersecurity in other countries, especially for the US, European Union, China, and Singapore, will be examined.

## Cybersecurity Practices in Other Countries

### *USA*

In the US, There are few federal cybersecurity regulations and be more industry specific. The three main cybersecurity regulations are the 1996 Health Insurance Portability and Accountability Act (HIPAA), the 1999 Gramm-Leach-Bliley Act, and the 2002 Homeland Security Act, which included the Federal Information Security Management Act (FISMA). These three regulations mandate that healthcare organizations, financial institutions and federal agencies should protect their systems and information.

The latest attempt to govern cyberspace is the Cybersecurity Information Sharing Act (CISA). It is a United States federal law designed to "improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes". The law allows the sharing of Internet traffic information between the U.S. government and technology and manufacturing companies. The bill was introduced in the U.S. Senate on July 10, 2014, and passed in the Senate October 27, 2015. Opponents question CISA's value, believing it will move responsibility from private business to the government, thereby increasing vulnerability of personal private information, as well as dispersing personal private information across seven government agencies, including the NSA and local police.

CISA requires businesses to determine whether any personal information is included in any cyber threat indicators they share with the federal government, and to remove such personal information if it is not "directly related to a cybersecurity threat." However, this removal requirement applies only to

information that is known, at the time of sharing, to be personal or personally identifiable to a specific individual. Businesses are required to develop "technical capability" to assist in the identification and removal of personal information.

The law requires the US Attorney General and Secretary of Homeland Security to publish guidelines to assist businesses in identifying information that would qualify as a cyber threat indicator and eliminating personal information from shared cyber threat information. These guidelines will seek to (1) identify cyber threat indicators that contain personal information and are unlikely to directly relate to a cybersecurity threat, and (2) identify types of information that is protected under privacy laws and are unlikely to directly relate to a cybersecurity threat (Boris et al., 2016).

### *European Union*

The EU takes a more government-centric approach to cyber security. The 2012 revisions to the EU Data Directive seek to create a national data protection authority in each EU nation. The 2012 revisions want to strengthen the power of the national data protection authority to better enforce the EU data rules. The 2012 revisions propose penalties for breaches of up to 1 million Euros or up to two-percent of the global annual turnover of the offending company (Barnard, 2013).

One of the interesting approach of EU's approach to cyber security is its position on the conflict between privacy and security. While many countries use the 'balance' metaphor to explain the inter-relationship between privacy and security, EU policy documents frequently construct privacy and security as complementary rights that must be 'respected'. Security and fundamental rights (including privacy) are complementary, not in contradiction. Fundamental rights and freedoms are to be 'respected' more than 'balanced'. Many scholars have taken issue with the notion of balancing privacy and security, as in a zero-sum game, where the reduction in one is at the expense of the other. Data protection, privacy and security are all represented as fundamental rights, and the European Parliament asserts that citizens should not have to choose between being free and being safe (Franziska B., 2015).

### *China*

China's state strategies with regard to cybersecurity have been to balance economic modernization and political control. Stated simply, this strategy broadly corresponds to China's unique approach and perspective to cyber-security is reflected in the various cyber-control measures (Kshetri, 2013). The Chinese government has emphasized on healthy and harmonious Internet environment. A healthy cyberspace is "porn-free" and "crime-free" and "harmonious" means that it does not threaten to destabilize the state's social and political order.

China's cybercrime and cyber security laws expands from controlling the Internet, requiring all existing computer networks to liquidate and re-register, and banning pornography and political content. All computer networks must use channels provided by the ministry of posts and telecommunications to link up with networks abroad, and new networks must get approval from the State Council.

China took the first major step toward criminalizing cybercrimes in February 2009 by including computer crimes in its Criminal Law (Kshetri, 2013). The punishment for hacking includes up to seven-year prison sentence. Since 2009 the Chinese government also tightened the registration requirements and processes for getting .cn domain names. The new rules do not allow individuals to register .cn domains. To register for businesses, it is required to submit a copy of the business license. The government has gone so far by launching a program called Green Dam Youth Escort Firewall which is a plan to make it mandatory to have the government's "internet protection" software installed in all new PCs in the country but subsequently terminating the project after raising strong public resistance (Owen, 2010).

The most notable standard for censorship is the Chinese government's digital barrier. 'The Great Firewall of China' that affects China's 600 million users reputedly employs some 50,000 workers to enforce internet censorship. It is the main instrument to achieve Internet censorship in China including criminalizing certain online speech and activities, blocking from view selected websites, and filtering key words out of searches initiated from computers located in Mainland China (Great Firewall, n.d.)

### *Singapore*

The Singapore Broadcasting Authority (SBA) is responsible for the regulation of the Internet in Singapore. The Internet is subject to Singapore's traditionally strict laws that apply to all other media, including the Defamation Act, Sedition Act, and Maintenance of Religious Harmony Acts. However, Singapore has gone a step further in its regulation of the Internet, encompassing a wide variety of subjects in its definition of "undesirable content." (Ang et al., 1996).

According to Hogan, 1999, Administration of censorship in Singapore has been performed in a typically methodical manner. First, materials going into the home are more heavily censored than those going into the corporate world. The Singapore authorities have drawn a distinction between information for business uses, which should be as free-flowing as possible, and information for non-business uses. Information for the home is seen to be of a less critical nature, so censorship of such information is regarded to have not as deleterious an effect. Second, materials for the youth are more heavily censored than those for adults. This is an admittedly paternalistic principle of protecting the weaker members of society from the possible harm of the materials in question. Third, materials for public consumption are more heavily censored than those for private consumption. This is a corollary of the second principle as it is assumed that the public includes those who are "weaker." Also, regardless of the level of censorship, those who are determined can always get their hands on censored materials. Hence, private consumption can only be policed to a limited extent. Further, it is more efficient to police public instead of private consumption. It should be noted that private consumption of censorable materials is still policed in that those found in private possession of such materials can be convicted in court

## Analysis

In general, two different approaches of cyberspace governance can be categorized. First, the self-regulation approach. This approach maintains that too much regulation may harm free flow of the information and emphasize the private sector's engagement. They employ and give right to civilian but able to monitor and capture who's outlaws. Data protection especially in an e- commerce context is left mostly to the evolution of industry norms and voluntary compliance. The United States has been employing this approach and is a prime example of this self-regulation approach. Recently, it begins to alter its course with the introduction of CISA bill which exerts more governmental mandates. Another approach is government regulation approach. The governments develop and enact clear legislation how cyberspace should be governed, roles of government vs public and private sectors and how information should be treated. The Organization for Economic Co-operation and Development (OECD)'s privacy principle is a prime example which EU decided to adopt the form of the data protection act (Barnard, 2013).

Analysis from international cyber security and data privacy laws point out two key strategies that governments should consider in developing their regulatory framework and executions of measures. First, public-private co-operation should be reinforced. All regulatory frameworks recognize that cyberspace is largely owned and operated by the private sector and that users also play a key role. They acknowledge that policies must be based on inclusive public-private partnerships, which may include business, civil society, the Internet technical community, and academia. Secondly, fundamental values must be respected. All strategies place a strong emphasis on the need for cybersecurity policy to respect fundamental values, which generally include privacy, freedom of speech, and the free flow of information. The government must take steps to ensure that provisions of the cyber security acts are not used to violate the right to freedom of expression. It needs to maintain the openness of the Internet and no strategy suggests modifying it in favor of strengthened cybersecurity. On the contrary, the openness of the Internet is generally described as a requirement for the further development of the Internet economy.

Cultural values and privacy perceptions also exert a significant influence over how privacy is respected and treated in a given country. Cultural values and privacy perceptions differ from country to country (Sarathy & Robertson, 2003). This, in turn, determines which cyber governance approaches a country adopts or if a country has an effective one. Thai government wants to assume parental roles to direct and protect their citizen. Western concepts of law, due process of law, democracy, human rights and so on, have not been deeply rooted in the "duty-based", patronage-based and authoritarian Thai society. Cybersecurity laws in Thailand, therefore, tend to focus more on surveillance, rather than putting the

foundation framework that can prevent or lower the risk of cyber attack, and thus, provide more stability and control to the government.

Thailand is not unusual in its desire to control Internet access to undesirable content as one of the instruments to prevent cybercrime activities. These new laws could bring military-run Thailand much closer to the kind of scrutiny that more authoritarian nations such as China and Vietnam apply to the web, and poses a risk to fundamental civil liberties (Tanakasempipat, 2016). However, censorship does not sit well with computer culture, where freedom is celebrated. Cyberspace culture regards free speech and the free flow of ideas as a route to social and intellectual progress. As a result, several offline and online protests have been organized. An example is a Facebook group, with the name Citizens Against Single Gateway, on Dec. 19, 2016, claimed responsibility for temporarily bringing down the Thai defense ministry's website (Associate Press, 2017).

The authors believe that attempting to prevent the cybercrime by compromising on public privacy simply cannot coexist with a desire to harness the technology for its economic potential. Many nations worldwide are trying to protect their citizens from pornography, deviant materials, and, in some cases, conflicting cultural values. The methods of censorship used vary, but in most cases, the lesson is the same.

## Summary and Conclusion

Recently, the Thai government has introduced a new set of laws that aim to boost public confidence in performing online activities in order to promote its so-called "Thailand 4.0" agenda. However, public are skeptical about the government's effort as they feel that these laws, in fact, aiming at suppressing online activities of its citizen rather than trying to boost public confidence. Several online and offline demonstration and debates have still been going on. However, under a military-led government, the law will soon be enforced and thus provide more stability and control for the government.

While the government already decide to use the legal approach which aim to restrict cybercrime activities through legislation, the authors argue that it should also consider the organizational approach which aims to enforce laws, to promote public-private sectors cooperation, and to educate the public through the establishment of dedicated organizations. The government should implement measures that aim to improve the coordination between states and reduce the possibilities of conflict rather than creating more. In addition, self-regulation may be the more sustainable and effective way to regulating the online space as compared to legislative measures. National cybersecurity programs need to address numerous issues, including organizational structures, government oversight, public–private partnerships, awareness-raising and international cooperation (OECD, 2012). To maintain effectiveness of the laws and gain wide public acceptance, it will would require that the laws, (1) are consistent with international law and standards on any contemplated restrictions on freedom of opinion and expression; (2) clearly define the prohibited expressions; (3) ensures that any restriction to freedom of expression and information, including any sanction provided for is necessary to a legitimate objective and proportionate to the harm caused by the expression.

## References

Ang, P.H. & Nadarajan, B. (1996), "Censorship and the Internet: A Singapore perspective", *Association for Computing Machinery. Communications of the ACM, vol. 39, no. 6, pp. 72.*

Associate Press (2017), Thai police charge man in hacking attacks on gov't sites, http://bigstory.ap.org/article/117f4af6867d4103882c851b4a48b573/thai-police-charge-man-hacking-attacks-govt-sites

Bangkok Post (2016), AGCS: Thailand second worst for cybercrime, http://www.bangkokpost.com/tech/local-news/1004649/agcs-thailand-second-worst-for-cybercrime

Bangkok Post (2017), The new Computer Crimes Act and concerns over online freedom , http://www.bangkokpost.com/business/news/1183561/the-new-computer-crimes-act-and-concerns-over-online-freedom

Barnard-Wills, D. (2013), "Security, privacy and surveillance in European policy documents", *International Data Privacy Law, vol. 3, no. 3, pp. 170-180.*

Boris S., Andrew H. and Kathryn L. (2016), "Federal Cybersecurity Information Sharing Act signed into law", *Data Protection Report*, Norton Rose Fubright, http://www.dataprotectionreport.com/2016/01/federal-cybersecurity-information-sharing-act-signed-into-law/

Channel NewsAsia (2016), Critics concerned over privacy as Thailand pushes to tighten cybersecurity, http://www.channelnewsasia.com/news/asiapacific/critics-concerned-over-privacy-as-thailand-pushes-to-tighten/3317136.html

Cybersecurity Information Sharing Act of 2015. https://www.congress.gov/bill/114th-congress/senate-bill/754/text

Franziska B. (2015), "A comparison between US and EU data protection legislation for law enforcement purposes", *Directorate-General For Internal Policies*, Policy Department : Citizens' Rights and Constitutional Affairs.

Great Firewall, (n.d.), In Wikipedia, Retrieved Febuary 11, 2017, from https://en.wikipedia.org/wiki/Great_Firewall

Hogan, S.B. (1999), "To Net or not to Net: Singapore's regulation of the Internet", *Federal Communications Law Journal, vol. 51, no. 2, pp. 429-447.*

Jittip Mongkolnchaiarunya. (2016), "The Trouble with Thailand's New Cyber Approach." *The Diplomat*. http://thediplomat.com/2016/08/the-trouble-with-thailands-new-cyber-approach/

Kanin Srimaneekulroj. (2016), "Cybersecurity laws in flux but set to flex". *Bangkok Post*, http://www.bangkokpost.com/tech/local-news/1057753/cyber-security-laws-in-flux-but-set-to-flex.

Kshetri, N. (2013), "Cybercrime and cyber-security issues associated with China: some economic and institutional considerations", *Electronic Commerce Research, vol. 13, no. 1, pp. 41-69.*

MICT Ministry of Information and Communication Technology. (2016), Thailand digital transformation roadmap. http://www.mict.go.th/assets/portals/1/files/590613_4Digital_Economy_Plan-Book.pdf

Nectec (n.d.), Internet Information Research Network Technology Lab, http://internet.nectec.or.th/webstats/home.iir

OECD. (2012), Cybersecurity policy making at a turning point: Analysing new generation of national cybersecurity strategies for the internet economy. *OECD digital economy papers 21. OECD Publishing. http://dx.doi.org/10.1787/5k8zq92vdgtl-en.*

Owen F. (2010), "Green Dam Comes Back to Haunt Beijing", The Wall Street Journal, *http://blogs.wsj.com/chinarealtime/2010/12/02/green-dam-comes-back-to-haunt-beijing/*

Oxford Analytica (2013), SOUTH-EAST ASIA: Cyber crime inspires new responses, https://dailybrief.oxan.com/Analysis/DB188025/Cyber-crime-inspires-new-responses-in-South-east-Asia

Sarathy R. and Robertson C. (2003), "Strategic and Ethical Considerations in Managing Digital Privacy," *Journal of Business Ethics, no. 46, p. 111–126*

Tanakasempipat, Patpicha. (2016), "Thailand Seeks to Tighten Cyber Security, Raising Questions about Privacy Protection." *Reuters*. Thomson Reuters, http://www.reuters.com/article/us-thailand-cyber-idUSKBN13H0VE

The Human Right Watch. (2016), "Thailand: Cyber Crime Act Tightens Internet Control". https://www.hrw.org/news/2016/12/21/thailand-cyber-crime-act-tightens-internet-control