LEGAL RESPONSE IN THAILAND WHEN FACING CYBERCRIME

Korakod Tongkachok, Thaksin University
Krisda Apinawatawornkul, Thaksin University
Thongphon Promsaka Na Sakolnakorn, Silpakorn University

ABSTRACT

The objective of this research was to study the Thai cyber legal model when facing cybercrime. It was found that cyber security measures had a wide range of security systems due to the cyber threats associated with national security had been attacking infrastructure projects in the fields of state security, critical government services, banking finance, information technology and telecommunications, transportation and logistics, energy and utilities, and public health. These can have effects on the economy and society, as well as the stability and security of the country as a whole. Planning and collaboration between the public and the private sector was essential to maintain critical infrastructure. The cyber security of critical infrastructures currently in operation required the development of protection and protection policies by establishing a strategic plan, action plan, and cyber legal readiness plan to deal with various emergency situations by using an international framework of good practice.

Keywords: Cyber Security, Cybercrime, Cyber Law, National Security

INTRODUCTION

The development of information and communication technology systems had resulted in remarkable economic and social development. As applications and software have been developed that are highly efficient, common users can access information more easily, quickly, and save money. If users used information in a constructive way, it can be used to benefit the development and enhancement of the economy, society, and environment in various dimensions. On the other hand, technology can do a lot of damage as well. If a malicious person had developed modern tools to attack systems, steal, destroy, misrepresent, or deceive, it can result in interference and disruption of security at all levels such as the individual, the agency, country, and global. However, cyber security needed to take into account the protection of privacy and the convenience of accessing individual systems as well. A focus on national security may lead to a privacy breach (Grigore & Maftei, 2020). While aiming for the convenience of system access may also cause cyber security to become lax (Younies, 2020). Therefore, the responsible agency needed to balance cyber security, the protection of privacy, and the facilitation of access to the system properly, as they were key mechanisms for building trust and promoting the creation of trust which were important to use digital technology in all sectors of work with the law (Navaratna, 2020).

Currently, the provision of services or applications of computer networks, the internet, telecommunication networks, or the normal service of satellites was at risk of cyber threats that may affect the security of the state (Gunduz & Das, 2020) and domestic order. Therefore, in order to be able to prevent or deal with cyber threats in a timely manner, it was desirable to define the nature of mission or service as critical information infrastructure for both government and non-governmental organizations that must be prevented, countered, and reduce the risk of cyber threats without affecting the security in various fields. In addition, there should be an agency to be responsible for coordinating the actions of both the public and private sectors in general situations or situations that were seriously detrimental to security. They also should establish a unified and continuous action plan and measures for cybersecurity that will make it effective in preventing and dealing with cyber threats. As cyber security was a major problem for each country, it was imperative to manage cyber security through cyber security law enforcement in Thailand. Therefore, this research examined Thailand's cyber legal handling patterns when confronted with cybercrime (Asia Pacific Regional Internet Governance Forum, 2020).

RESEARCH METHOD

This research is a knowledge management process by collecting scattered information in the form of documents, statistics, investigative reports, and cybercrime laws. IT personnel and staff who have roles or are involved in cyber operations or development as tools. The samples used in this research were experts who were selected to provide information for their actions against cybercrime. Sample selection that covers as much diversity in the population as possible is the best method of sampling, as the coexistence of sample diversity is of great interest and value to research.

The first group is four people who are involved in cyber operations or development and are using cyber development as a development tool in Thailand. The second group is 6 people with knowledge and expertise in the technology strategy in the government sector, consisting 2 people of the Ministry of Digital Economy and Society, 1 person of the National Security Agency, 2 people of the Royal Thai Police, and 1 person of the Thai army.

Data analysis whereby the researcher collects data along the way to obtain the correct and complete information on the desired subject. After that, the researcher used data analysis by classifying the data. In the classification of information, the framework is classified by issues relating to cyber advancement, cyber threats, and the implementation of cyber law as a tool for the prevention of cybercrime in Thailand.

LIRATURE REVIEW

The concept of cybersecurity as many countries are transitioning to the digital age or entering the digital economy (Turina, 2020). Everyone is related to the internet in some way even if not a direct internet user in a new cyber approaches (Plazas, 2020). The basic idea of the cyber approach is that the Internet reduces the link between social reality and politics, issuing a sovereign state (Zhuravskaya, Petrova, & Enikolopov, 2020). Cyber is different from the real world and requires a different governance model in terms of cyber thought law (De Benedetti, 2020).

Therefore, the world society has set the concept of internet governance. The idea of organizing this internet society (Vakil & Norouzpour, 2020) has been discussed extensively at various international conferences such as the World Summit on Information Society: WSIS (Klein, 2004) held in Geneva, Switzerland, in December 2003, and the 2nd time in Tunis, Tunisia, in June 2005 (Berry, 2006). The working group on internet governance (Servaes, 2020) defined Internet governance as “Internet governance is when the public, private, and civil society sectors take into account common rules and regulations, traditions, decision-making processes, and programs to shape the direction of the evolution and utilization of the Internet” (Asia Pacific Regional Internet Governance Forum, 2020).

RESULTS & DISCUSSION

In 2020, it was found that several types of cyber threats have been identified from abusive content and the threats that arise from the use of disseminating false or inappropriate information (Abusive Content) to destroy the credibility of individuals or institutions, to incur unrest, or unlawful information such as obscene, obscene, defamatory, and to advertise products by email that the recipient does not intend to receive the advertising information (Spam).

Attack on the availability of the system was a threat resulting from an attack on the availability of the system to render the services of the system from operating normally. This had the effect of a delay in the response of the service to the failure of the system to continue to service. Threats may arise from direct system service attacks, such as various DOS (Denial of Service) attacks, or attacks on service-supported infrastructure such as buildings, facilities, power systems, and air conditioning systems.

Cyber threats in foreign countries, cloud jacking, were likely to be one of the most prominent cyber threats in 2020 due to increasing dependence on cloud businesses. If it was misconfigured, most attack events were reported by (Sophos, 2020) Threat Report.

Over the past year, Thailand has had several forms of cyber threats against government and private agencies and organizations as follows:

Fraud was a threat arising from fraud that can occur in a variety of ways, such as unauthorized use of systems or information resources for their own benefit or exploitation, or sell pirated goods or software (Whitty, 2019).

Information Gathering was a threat arising from an attempt to gather information about a malicious attacker's system (Scanning) by running services that may be open on the system, such as information about the operating system (Do, Martini & Choo, 2018).

Unauthorized access or alteration of information security was a threat that was caused by an unauthorized access or unauthorized modification (Eldem, 2020).

Intrusion attempts were threats posed by intrusion/hacking attempts, either through CVE Common Vulnerabilities and Exposures (Kolev & Nikolova, 2020).

Intrusions were threats to the system that had been intrusions/successfully hacked, and the system was occupied by unauthorized persons (Egloff, 2020).

Malicious code was a threat that was generated by a program or software that was developed in order to cause undesirable effects on the user or the Malicious code to cause malfunction or damage to the system, program or software (Bi, Yang, Liu & Huang, 2020).

For Thailand's threats tracked by data reported by ThaiCERT (2020), threats had been shown to continue to increase, especially in 2018-2020 where the threat rate was lower, but more damage to an organization or entity. (ECSIRT.net project on cooperation and common statics) Threats arising from fraud were still more deterrent than other types of threats in 2018 and 2019. Even though there were more numbers in 2020 than others, it was still high. The rising rate of threats was the use of the Malicious code was a threat posed by a program or software that had been developed to produce undesirable results which contain viruses, worms, and Trojans for the purpose of damaging systems or stealing information. These virus programs may have techniques for attacking.

In addition, the latest cyber security report for the fourth quarter of 2019 of the antivirus company was Kaspersky. The analysis of web-based attacks, common threats, and threat sources were found that Kaspersky had been able to block more than 2.7 million web-based cyber threats in Thailand over three months (Bangkokbiznews, 2020). In view of the problem of cyber security in Thailand, the Office of the National Security Council had developed the National Cyber Security Strategy 2017 - 2021. They had put in place measures before the implementation of cyber laws to become Thailand's first national policy for securing cyber security to fully embrace the digital age of society in the future. The main goal was to build the readiness of Thailand to deal with the escalating cyber threats to cover all aspects of the environment, facilitate, and strengthen Thailand's capabilities by focusing on having a central mechanism for management, national cybers ecurity, protection of infrastructure, raising awareness in all sectors, and building cooperation with foreign countries.

Cyber security Act, B.E. 2562 of Thailand aimed to enhance the security of the Critical Information Infrastructure (CII) to be effective, and had measures to prevent, respond, and reduce the risk of cyber-attacks that may affect the security of the state, economy, and peace within the country. This applied to government agencies or non-governmental organizations that operated in eight groups of critical information infrastructure services: government security, critical government services, banking, information technology and telecommunication, transport and logistics, energy and utilities, public health, and other areas as further announced by the Commission.

Roles of directors, executives, operators of the Regulatory Body/Regulators that directed the regulated entities to meet the needs of stakeholders in accordance with the Cybersecurity Act were as follows:

- Responsibility: The person performing duties with knowledge, ability and potential/ assigned by the director or the chief executive from the regulatory body/regulators of the agency.
- Accountability: The person with the highest level of decision-making duties and responsibilities in accordance with the Cybersecurity Act or the agency, such as setting vision, mission, policy, strategy, risk appetite, related plans, performance balanced with compliance with laws, standards, announcements, orders, and conformances, including duties and responsibilities to evaluate, direct, and monitor to achieve the overall objectives of the organization.
- Consulted: The person who was responsible for advising on data-intensive processes, information, cybersecurity, data processing processes and procedures, cybersecurity, and outcomes and benefits.
- Informed: The person who used data to make decisions or made use of data, information, cybersecurity, as well as continuous work development to create equilibrium value for relevant stakeholders.

The results of the research revealed that the eight major information infrastructure agencies were government security, critical government services, banking finance, information technology and telecommunication, transportation and logistics, energy and utilities, and public health must comply with cybersecurity, which was divided into four areas: policy and plan, management, critical information infrastructure, and cybersecurity operations.

The Cybersecurity Act was a law that has been established to provide Thailand with protective measures to cope and mitigate the risks from cyber threats affecting the state security and domestic order, which had been in effect since May 28, 2019. The essence was an approach to cyber management, prevention, response, and mitigation through collaboration between stakeholders, developing the competence of personnel and experts, including education and awareness for cyber threats as well.

In the Cybersecurity Act B.E. 2562, there were three committees established as follows:

1) National Cybersecurity Committee (NCSC) was chaired by the Prime Minister. They were responsible for proposing policies, formulating master plans, setting standards and guidelines for promoting development, enhancing staff skills, coordinating collaboration with agencies, and monitoring and evaluating the implementation of the established policies.
2) Cybersecurity Regulating Committee (CRC) chaired by the Minister of Digital Economy and Society. They were responsible for overseeing and taking action to address critical cyber threats, establish

guidelines for government and information infrastructure agencies, and define measures for risk assessment, response, and cope with the threat arises.

3) Office of the National Cybersecurity Committee, chaired by the Minister of Digital Economy and Society. They were in charge of general administrative tasks.

The three committees will oversee eight essential IT infrastructure, namely state security, critical government services, finance and banking, information technology and telecommunications, transportation and logistics, energy and public utilities, public health, and other areas as further announced by the Commission.

The Cybersecurity Act empowered government officials to review computer information of those who may have information related to the threat, and imposed penalties for those who violate or fail to cooperate with fines and imprisonment. At the same time, there were penalties for critical information infrastructure agencies that dropped off to perform their duties. For example, If the agency failed to report the threat without reasonable cause, there was a fine not exceeding 200,000 baht, etc.

Maintaining cybersecurity was a priority of every organization and action must be taken to cover the people-process-technology element which AC Infotech is ready to serve your organization in all the following elements.

People component: Organize cybersecurity awareness training for employees, cyber health check for employees, and phishing simulation test.

Process component: Analyze the consistency of the organization's operations against various laws and regulations (Gap Analysis), audit and report on the performance of corporate cybersecurity, audit and report the performance of supply chain cybersecurity (Supply Chain Audit), provide consulting on the implementation of international standards for information security and cybersecurity such as ISO 27001, NIST CSF.

Technology component: Measure the cybersecurity level of the organization as a whole (Cybersecurity Health Rating), perform a vulnerability assessment/penetration testing, provide a search for vulnerabilities by a bug Bounty, organize cyber exercise test.

Problems of cyber security will continue to grow with more modern technology. Government agencies will remain a prime target in cyberattacks from malicious people, both from attacks to trick the public's trust of government agencies and attacks to destroy the credibility of the agency caused by whether it is to show the power of a group of people who oppose government policies, defamations, harassment, or even an attack to test the attacker's own ability. In the future, cyberattacks will become more or more violent, as attack tools can be easily obtained from the internet and underground, which will allow new hackers to emerge easily. The government must focus on cyber security in a concrete way with the Cybersecurity Act promulgated through public hearings to gain positive views and acceptance from the private and public sectors. More importantly, people, especially government personnel at all levels, must be aware of the importance of monitoring and implementing the organization's cybersecurity measures to protect themselves and the agencies safe from attacks. In addition, monitoring the cybersecurity situation is vital to help them prepare for the latest threats that arise.

CONCLUSION

Currently, the provision of services or applications of computer networks, the Internet, telecommunication networks, or the normal service of satellites poses a risk of cyber threats that may affect national security and domestic order. Therefore, in order to be able to prevent or respond to cyber threats in a timely manner, both government and non-government organizations must prevent, respond, and mitigate the risks of cyber threats from affecting the security in various aspects, whether in general situations or situations which are serious security threats.

Therefore, it is imperative to enact the Cyber security Act 2019, which without this law will cause cyber danger in Thailand. Although this law is only enforced for one year, it works in both public and private entities that they must strictly perform all the processes or actions necessary to keep the organization free from the risks and damages that affect the safety of the government Information in all forms, including protection against crimes, attacks, sabotage, espionage, and errors, should take into account the three fundamental elements of information security, or the 3 CIA that are Confidentiality, Integrity, and Availability.

REFERENCES

Asia Pacific Regional Internet Governance Forum (APrIGF). (2020). Asia Pacific Regional Internet Governance Forum (APrIGF).

Berry, J.W. (2006). The World Summit on the Information Society (WSIS): A global challenge in the new Millennium. *Libri, 56*(1), 1-15.

Bi, J., Yang, X., Liu, W., & Huang, D.W. (2020). A cost-effective algorithm for selecting optimal bandwidth to clear malicious codes. *IEEE Access, 8*, 19900-19910.

Bangkok biznews. (2020). 'Thailand' ranks fifth highest target for cyber threats in the region.

Do, Q., Martini, B., & Choo, K.K.R. (2018). Cyber-physical systems information gathering: A smart home case study. *Computer Networks*, *138*, 1-12.

De Benedetti, M. (2020). Bruno Leoni’s concept of law and representation in the cyber age: A cybernetic model. *Open Political Science*, 3(1), 56-65.

Eldem, T. (2020). The governance of turkey’s cyberspace: Between cyber security and information security. *International Journal of Public Administration*, *43*(5), 452-465.

Egloff, F.J. (2020). Public attribution of cyber intrusions. *Journal of Cybersecurity*, *6*(1), 1-12.

ECSIRT. (2020). Project on cooperation and common statics.

Gunduz, M.Z., & Das, R. (2020). Cyber-Security on smart grid: Threats and potential solutions. *Computer Networks, 169*, 107094.

Grigore, A.N., & Maftei, A. (2020). Exploring the mediating roles of state and trait anxiety on the relationship between middle adolescents’ Cyberbullying and Depression. *Children*, *7*(11), 240.

Klein, H. (2004). Understanding WSIS: An institutional analysis of the UN World Summit on the Information Society. *Information Technologies & International Development, 1*(3), 3-13.

Kolev, A., & Nikolova, P. (2020). Instrumental equipment for cyber-attack prevention. *Information & Security, 47*(3), 285-299.

Ministry of Digital Economy and Society. (2019). A five-year operation plan: Ministry of digital economy and society.

Navaratna, D. (2020). Laws in sri lanka to prevent cyber-attacks: Analysis of laws in Sri Lanka to prevent cyber-warfare in the future.

Plazas, C. (2020). Information crossroads: Intersection of military and civilian interpretations of cyber-attack and defense.

Servaes J. (2020). *Communication for Development and Social Change: In Search of a New Paradigm*. In: Servaes J. (Ed.), Handbook of communication for development and social change.1, 15-27. Springer: Singapore.

Sophos. (2020). *Threat Report*.

Thailand Computer Emergency Response Team : Thai CERT (2020). Crime statistics.

Turina, A. (2020). The progressive policy shift in the debate on the international tax challenges of the digital economy: A “Pretext” for overhaul of the international tax regime? *Computer Law & Security Review*, *36*, 105382.

Vakil, A., & Norouzpour, H. (2020). Multi-Stakeholder internet governance and international law: Common concepts or new approach? *Public Law Researsh*, *21*(66), 107-140.

Whitty, M.T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime, 26*(1), 277-292.

Younies, H., & Na, T. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime*, *27*(4), 1089-1105.

Zhuravskaya, E., Petrova, M., & Enikolopov, R. (2020). Political effects of the internet and social media. Annual Review of Economics, *12*, 415-438.