Jurnal IUS Kajian Hukum dan Keadilan
Volume 10, Issue 2, August 2022, E-ISSN 2477-815X, P-ISSN 2303-3827
*Nationally Accredited Journal, Decree No. 158/E/KPT/2021*
*open access at : http://jurnalius.ac.id/ojs/index.php/jurnalIUS*

# *POLICIES, LAWS AND STRATEGIES FOR RESPONDING TO CYBERTERRORISM IN THAILAND*

**Natthamon Petchkla[1], Sumonthip Chitsawang[2]**
[1]PhD Student at the Faculty of Political Science, Chulalongkorn University, Thailand
Email: natthamon.p@chula.ac.th
[2]PhD student at the Faculty of Political Science, Chulalongkorn University, Thailand,
Email: sumonthip.c@chula.ac.th

*Received: 2022-06-30; Reviewed: 2022-07-30; Accepted: 2022-08-24; Published: 2022-08-24*

**Abstract**

*This article explains the policies and strategies currently used in Thailand for responding to terrorism. This study uses in-depth interviews with technicians and policy analysis experts in the area of cyber-attack, including more than 30 people in 15 governmental agencies. Specifically, the study begins by exploring the definition of cyberterrorism. Moreover, the study uses document research in both Thai and English and concludes that Thailand's governmental agencies understand the concept of cyberterrorism and have already established policies and strategies for responding to it in the future.*

***Keywords: Cyberterrorism; Cyberterrorism Policies; and Strategies for Responding Cyberterrorism.***

## 1. INTRODUCTION

It is essential to avoid cyber-attacks in this era of frequent attempts. Thailand is one of the countries in which the government provides information about cyber security breaches. This article is an original study conducted for the purpose of exploring recent cyberterrorism in Thailand and the strategies used to respond. This research clearly defines cyberterrorism to help the government create response policies. The term of using violence attacking national critical infrastructures causing huge damages to the innocent people via cyber space in order to achieve political issues will applied while analysing[1]. The research is organized with two main purposes. First, to identify areas of agreement, disagreement, and ambiguity related to the concept of cyberterrorism. Second, to review recent academic research in the area of cyberterrorism, including how to create policies and strategies for responding cyberterrorism in the future.

## 2. ANALYSIS AND DISCUSSIONS

### Concepts and Controversies in the area of Cyberterrorism

After discussing the studies on government responses to cyberterrorism in Thailand, the study analyses data from 15 government agencies. The analysis clearly shows that Thai governmental agencies are concerned about cyber-attacks but do not recognise

[1] Schmid, Alex P and Jongman, Albert J. (2008). Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, & Literature (updated edn). (New Burnswick, NJ: Transaction, 2008). Pg.5-7

DOI: http://dx.doi.org/10.29303/ius.v10i2.1095

them as cyberterrorism. The fundamental issue is the definition of cyberterrorism. The definition of cyberterrorism needs to be clear to explain the situation and the possible means to counter terrorism in Thailand.

Two issues in particular define cyberterrorism from Thai governmental officers' perspectives. First, the definition of cyberterrorism is related to financial crimes, fraud, and exploitation at the organizational level and results in significant damage. However, the second definition is related to the use of technology and the results of the attack. Most governmental officers who work in the area of broadcasting, telecommunications, and the military sector believe that cyberterrorism is an activity which focuses on basic information utilities such as monitoring movements in social media. Cyberterrorism aims to attack national institutions, harming the reputation of the nation and provoking civilians to oppose the government. Thus, cyberterrorism is linked to policies that take primary responsibility for protecting the nation from opposed civilians[2]. Thailand's anti-cyberterrorism agencies need to use cyber surveillance to prevent cyber intrusion or aggression. cyberterrorism may result in physical integration that would be a problem for cybersecurity stability of the country such as assuming civilian as cyber-terrorists[3].

**The definitions of cyberterrorism according to three different types of national agencies.**

This article has drawn information from people who work in the government sector and have more than three years of cyber-related experience. The National Agencies of Thailand are divided into three different categories:

1. **Policy and Regulations Sector:** National Security Council, National Cyber Security Committee, Ministry of Digital Economy and Society, Bank of Thailand, National Intelligence Agency.
2. **Military Defence Sector:** Ministry of defence, Royal Thai Air Force, Royal Thai Army, Technology Crime Suppression Division.
3. **The national agencies most at risk from cyberterrorism:** Ministry of Justice, Ministry of Public Health, Electricity Generating Authority of Thailand, National Broadcasting and Telecommunication Division.

- **The Policy and Regulations Sector's perspective towards cyberterrorism**

  Security regulators define cyberterrorism by three features. First, the use of computers to attack governmental agencies such as inoperable attacking or intruding the system which targeted in only cyber space. Second, the attack must be related to political issues and aim to distort the image of the government. Third, the attack causes severe damage to innocent people.

[2] Silke, Andrew. (2004). "The Road Less Travelled: Recent Trends in Terrorism Research", in Andrew Silke (ed.) Research on Terrorism: Trends, Achievements and Failures (Abingdon: Routledge), 186-213, 193-194. Pg.205-208.

[3] Noguchi, M., & Ueda, H. (2019). An analysis of the actual status of recent cyberattacks on critical infrastructures. NEC Technical Journal, Special Issue Cybersecurity, 12(2), 19-24. Pg. 19-20.

- **The Military Defence Sector's perspective on cyberterrorism**

Cyberterrorism is defined as applying terrorist tactics to current technology systems to breach government security, causing severe damage to civilians and deterioration of the image of Thailand. Terrorist's acts can be carried out either as a group or as an individual. Cyber-attacks are borderless, and can originate with within or outside Thailand.

- **The national agencies most risk for cyberterrorism and their perspectives on cyberterrorism.**

Cyberterrorists aim to damage governments for their own gains. Their attacks are conducted via a computer and the Internet. The terrorist's purposes are to destroy the target's computer system and distorted information of the opposing party. The terrorists also threaten the government to achieve their political goals. Currently, most of the methods used destroy the government's computer system and render it inaccessible to the public sphere.

Combining the definitions of experts working in all three different national agencies can be summarised as follows. The agencies define terrorism as the use of terrorist methods to achieve political goals such as the destruction of innocent people, undermining the credibility of the government, and misrepresenting information through the use of technology and cyber devices causing severe damage[4]. This definition summarises the nature of cyberterrorism in Thailand.

The Definition of Cyberterrorism


[4] Noguchi, M., & Ueda, H. (2019). An analysis of the actual status of recent cyberattacks on critical infrastructures. NEC Technical Journal, Special Issue Cybersecurity, 12(2), 19-24 Pg.19-20 and Kugler, R. L. (2009). "Deterrence of cyberattacks", Cyberpower and national security, 320, 309-340. Pg. 327-328.

**Policies for Responding to Cyberterrorism.**

There are several perspectives appropriate for analysing possible responses to cyberterrorism. This section focuses on two main issues: the legal perspective and the strategic perspective.

**1. Legal Perspective**

The legal perspective explains how the government defines cyberterrorism as an armed attack and recognises it as a self-defence issue[5]. If an attack occurs in any form, all states must react in a way based on their experience, their specific knowledge related to the attack, and the laws related to retaliation[6]. Traditional attacks and cyber-attacks elicit different responses because cyber-attacks are unpredictable and the sources are unidentified[7]. Cyber-attacks can be more violent than traditional attacks. Thus, the question as to whether a country has the right to use cyber weapons for self-defence purposes. Will the attacked country be justified? No one has yet been able to come to a conclusion[8].

Thailand has established a policy to respond to cyberterrorism in the form of defensive action. This policy, launched in August 2021, involved establishing the Office of the National Cybersecurity Commission (NSC) as the main agency for counter measures and prevention of cyberterrorism in particular[9]. Based on the office's core mission, the Office of the National Cybersecurity Commission is an agency that monitors and responds to threats promptly through ThaiCERT which has technical experts constantly ready to respond[10]. The Office of the National Cybersecurity Commission is both policymaker and operator and its policies apply to all departments to implement and create standards for all operating units. The Commission's duties do not include the prosecution of the offenders which is a duty for the judicial branch[11].

What the Office of the National Cybersecurity Commission is able to increase digital research and collect statistics from various agencies[12]. The Commission then analyses those statistics that predict the future and determines the planned response. Thailand should have a strategic position to respond to each type of threat[13]. Therefore, the following section identifies the tools that are used by attackers and the strategies or methods that should be used to deal with them.

[5] Nakayama, S. (2012). Govt Claims Cyberdefense Right/Says International Laws Should be Applied to Computer Infiltration. Yomiuri Shimbun, p.17.

[6] Segal, A. (2011). Cyberspace Governance: The Next Step. Council on Foreign Relations Press. Retrieved from http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397.

[7] Ayala, L. (2016). Detection of Cyber-Attacks. In Cybersecurity for Hospitals and Healthcare Facilities (Pg. 53-60). Apress, Berkeley, CA.

[8] Dever, J., (2013). Cyberwarfare: attribution, preemption, and national self-defense. JL & Cyber Warfare, 2, Pg.25.

[9] Goel, S. (2020). National cyber security strategy and the emergence of strong digital borders. Connections, 19(1), 73-86. Pg. 73-75.

[10] Heinl, C. H. 2014. Regional cybersecurity: moving toward a resilient ASEAN cybersecurity regime. Asia policy, (18), 131-160 Pg. 158-160. and Tantawutho, T. (2017, January). The computer crime incidents and the future of countermeasures in Thailand. In 2017 Third Asian Conference on Defence Technology (ACDT) (Pg. 97-103). IEEE.

[11] *Ibid*, Goel, 2020 Pg. 73-75.

[12] *Ibid*, Tantawutho, 2017 Pg. 97-103

[13] Jirawannakool, K., Sanglertsilapachai, N., & Siwamogsatham, S. (2009). Computer Security Incident Handling and Phishing Cases in Thailand. In Global E-Governance (Pg. 194-201). IOS Press.

**2. Strategic Perspective**

Military actions are necessary are to protect the nation and critical infrastructures that are vulnerable to cyber-attack [14]. This section examines the tools that are used by attackers and the strategies or methods that should be used to respond.

a. Hackers

Hackers are people highly skilled in computers and in using them in illegal ways, such as stealing information via the network or modifying computer programs[15]. They can find vulnerabilities in computer systems. In this case, a hacker is identified as an individual or a group of individuals working together who share the same goals[16]. To combat hackers, we must learn as much about cyber-activity as possible, especially in technical areas to prevent access to governmental resources via software control[17].

**Tools:** Viruses and Worms, Backdoor: Trojans and Rootkits, Botnets

**Methods and Tactics:** DoS Attacks, Infiltration techniques, data logging, snooping, data collection, anonymization techniques.

**Counter-measures:** The government should be aware of professional hackers that can breach the system[18]. The government should have a list of suspected hackers so the government can follow up, adapt, and trace hacking to the source[19]. If these hackers are caught, they can bring their knowledge passed on to governmental staffs in the organization for the benefit of the government[20].

b. Cracker

Crackers are people who use their knowledge of hacking to commit crimes or manipulate people, such as stealing identity, destroying data, or even taking over someone else's computer[21]. There are two types of crackers: black hats and grey hats. Black hats engage in illegal cyber threat activities[22]. Attacks by a group of black hats include illegal activities and cyber harassment[23]. Grey hats are in the middle and aim for maximum benefit[24].

---

[14] Abdulmana, S., & Saleh, B. (2014). Coordinate negative content filtering and threat detection in Thailand on the Internet infrastructure. In The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M) (Pg. 1-5). IEEE.

[15] Gaia, J., Sanders, G. L., Sanders, S. P., Upadhyaya, S., Wang, X., & Yoo, C. W. (2021). Dark Traits and Hacking Potential. Journal of Organizational Psychology, 27(3). Pg.23-46.

[16] Sun, L. (2021). Discussion on computer network security prevention based on big data era. In Journal of Physics: Conference Series (Vol. 1848, No. 1, p. 012103). IOP Publishing. (Pg. 1-5)

[17] Schneier, B. (2021, July). Invited Talk: The Coming AI Hackers. In International Symposium on Cyber Security Cryptography and Machine Learning (Pg. 336-360). Springer, Cham. Pg. 338-340

[18] Perlroth, N. (2021). This Is How They Tell Me the World Ends: The Cyberweapons Arms Race. Bloomsbury Publishing USA. Pg. 420-432

[19] *Ibid*, Schneier, 2021, Pg. 338-340

[20] Mahoney, C. W. (2021). Corporate Hackers. Strategic Studies Quarterly, 15(1), 61-89.

[21] Richet, J. L. (2013). From young hackers to crackers. International Journal of Technology and Human Interaction (IJTHI), 9(3), Pg.53-62.

[22] Richet, J. L. (2013). From young hackers to crackers. International Journal of Technology and Human Interaction (IJTHI), 9(3), Pg.53-62.

[23] Gandhi, F., Pansaniya, D., & Naik, S. (2022). Ethical Hacking: Types of Hackers, Cyber Attacks and Security. International Research Journal of Innovations in Engineering and Technology, 6(1), p.28.

[24] *Ibid*, Gandhi, Pansaniya, & Naik, 2022, p.28

**Tools:** Viruses and Worms, Backdoors: Trojans and Rootkits, Botnets

**Methods and tactics**: DoS attacks, infiltration techniques, data recording, spying, data collection, anonymity techniques.

**Counter-measures:** This group has expertise similar to hackers but with different ideologies[25]. What the government needs to clearly identify the different types of hats to legally judge each party's responsibility. Even if some parties have good intentions, the method is still illegal. It is important to categorize the groups and identify the purpose of each group and their skills.

c. Script Kiddies

Script kiddies are novice hackers who lack skill in hacking computers[26]. Script kiddies usually use hacking programs developed by highly skilled hackers. They penetrate the computer system that they are interested in or attempt to access the system with their own knowledge, but they do not have the same level of skills as a hacker[27].

**Tools:** Virus and Worms, Backdoor; Trojans and Rootkits

**Methods and Tactics:** DoS Attacks, Data Entry, Spying, and Data Collection

**Counter-measures:** This group may be less professional than normal hackers, and sometimes pose no harmful threats to state. However, the state should pull these script kiddies out of the professional hacker network or out of large organizations dedicated to committing cybercrime[28]. Developing these new script kiddies' skills through training from the government could benefit the government in the long term.

d. Cyber vigilantes

This group is anonymous and acts with anti-government purposes to achieve their political goals[29]. On the other hand, some groups may be involved in illegal activities such as money laundering. Cyber vigilantes breach the privacy of the targets who being unlawful with the goal of protecting the rights and liberties of innocent people[30]. However, cyber vigilantes who lack proper political motivation can eventually turn into terrorists that oppose the state[31].

**Tools:** Virus and Worms, Backdoor: Trojans and Rootkits, Botnets

**Methods and Tactics:** DoS Attacks, Infiltration Techniques, Social Engineering, Data Entry, Snooping, Data Collection, Invisible Techniques

**Counter-measures:** Compared to the three aforementioned groups, cyber vigilantes have the strongest ideology and structural inclusion. This group tries to

[25] Kumar, S., & Agarwal, D. (2018). Hacking attacks, methods, techniques and their protection measures. International Journal of Advance Research in Computer Science and Management, 4(4), Pg.2253-2257.

[26] Holt, T. J. (2020). Computer hacking and the hacker subculture. The palgrave handbook of international cybercrime and cyber-deviance, Pg.725-742.

[27] Bhardwaj, A., & Goundar, S. (2020). Keyloggers: silent cyber security weapons. Network Security, 2020(2), Pg.14-19.

[28] Ibid, Holt, 2020, Pg.725-742.

[29] Silva, 2018, Pg. 21-36

[30] Tan, W. L., & Khader, M. (2022). Impact of justice-related dispositions on support for cyber vigilantism: The mediating effect of perceived severity of transgression. Legal and Criminological Psychology, 27, Pg. 234-246.

[31] *Ibid*, Tan, & Khader, 2022, Pg. 234-246.

achieve their goals by using formidable tactics, combining psychology and technology[32]. Therefore, the government should give power to the National Cybersecurity Commission to watch this group and follow them to identify any potential movement before expanding their idea and ideology in the future.

e. Non state actors with Political Agendas

Non-state actors may more easily access a country's Internet network because they are anonymous groups using cyber-tools to fight for their state's political goals[33]. However, these activities may not always impact innocent people because they are more likely to intimidate or coerce the state rather than attack people[34]. It is possible for this group to achieve their goals faster because cyber-tools are readily available anywhere and anytime and the associated costs are not high. Vice versa they can produce effective results[35]. More importantly, should these groups gain more members to become more powerful, political revolution can result[36].

The attack starts with their desire to confront, uproot, and increase their power using website to damage to discredit the government information system by changing content information[37].

**Tools:** Virus and Worms, Backdoor: Trojans and Rootkits, Botnets

**Methods and Tactics:** DoS Attacks, Infiltration Techniques, Social Engineering, Data Entry, Snooping, Data Collection, Techniques for invisibility

**Counter measures:** It is difficult for governments to identify or accuse non-state actors as terrifying groups of cyber terrorists[38]. Moreover, non-state actors are sometimes supported by states whether their financial, technology or accessing to information. Some states may have to protect these groups for their own benefit. However, some non-state actors are groups of trainees who might simply want challenges[39]. Most of the methods and strategies used are based on the ideology of their organizations. Strong support from a powerful state makes it easier to form an anonymous group (Kobia, 2021). Thus, states should create strong defence and offense systems to prevent non-state actors from accessing information systems or attacking non-state actors. It is difficult to find a list of those involved, but what can be done is to track the hackers' behaviours[40]. As these hackers allow themselves to trace their roots or use these spies to infiltrate non-state actors[41]. States need to build recovery teams,

[32] McDonald, C. (2021). Friends, rivals, foes: The private sector and online vigilantism impact on police cyber capabilities. Pg.2-86

[33] Klein, J. J. (2018). Deterring and dissuading cyberterrorism. Air & Space Power Journal-Africa and Francophonie, 9(1), Pg.21-35.

[34] Dayem, L. (2018). The Ethics of Cyber Warfare. Illini Journal of International Security, 4(1), Pg.5-20.

[35] McDonald, C. (2021). Friends, rivals, foes: The private sector and online vigilantism impact on police cyber capabilities. Pg.2-86

[36] *Ibid*, McDonald, 2021, Pg.25-29

[37] *Ibid*, McDonald, 2021, Pg.13-14

[38] Taneski, N. (2021). Transformation of war–use of conventional military forces against no-state actors. The Annual of the Faculty of Philosophy in Skopje, 74, Pg.467-477.

[39] *Ibid*, Taneski, 2021, Pg.467-477.

[40] *Ibid*, Taneski, 2021, Pg.467-477.

[41] *Ibid*, Taneski, 2021, Pg.467-477.

including collaborating with international cyber organizations and seek help when needed.

**Future Cyber Attack Response**

From the above analysis, the lessons and solutions recommended for the Thai government are as follows.

**1. Cyber Warfare Using Botnets**

Cyber war that aims to attack all national critical infrastructures mostly occurs by using botnets. Therefore, the National Cybersecurity Commission must cooperate with ThaiCERT to monitor the situation[42].

In addition, ThaiCERT must have a network with other countries whether private or the state itself to be able to help or send signals in time[43]. Learning to prepare a backup system is also important for use in restoring the country's critical infrastructures when they are attacked. Most of the developed countries are pressing ahead with Internet networks which means all critical infrastructures may rely on online systems, while the developing countries have not yet come to rely on technology[44].

Without relying on technology, Thailand still has a backup and can maintain the country's critical infrastructure operations. However, the Thai government should prepare and cooperate with the National Cybersecurity Commission and the ThaiCERT team, increasing training for each national agency or enabling ThaiCERT staff to work with each national agency. Cyber interruption may cause people to panic. Therefore, governments need to create cyber awareness campaigns to reduce panic and enable people to live with the chaos of the situation should it occur.

**2. Cyber warfare from state actors**

An attack on behalf of the name of the state is clear and has a definite purpose[45]. The Thai government can therefore respond through the head of the government. Diplomatic negotiations could provide a solution. But if the opposing country does not accept the proposal, the Thai government may have to reconsider its approach. Regarding the cyber ability of the state, the strategy in war depends on the government's ability to negotiate with the enemies (Ibid). Thailand must protect its important utilities depending on the extent of the damage. One such strategy is theft or cyber guerrilla techniques disguised in the cyber army of the opposing country. If that country has inferior technology, the Thai government can attack using an offensive strategy aimed to stop the attack. Other options are using international laws to determine the rules of negotiation for both parties and asking for help from the international community.

[42] ThaiCERT. (2018). Cybersecurity strategy for critical information infrastructure in Thailand. Bangkok: Electronic Transactions Development Agency. Pg.1-28

[43] *Ibid*, ThaiCERT, 2018, Pg.1-28

[44] Norris, P., (2003). "Digital divide? Civic engagement, information poverty & the Internet in democratic societies," at http://ksghome.harvard.edu/ ~ .pnorris.shorenstein.ksg/book1.htm, accessed 5 February 2004.

[45] Yeo, S., Birch, A. S., & Bengtsson, H. I. J. (2019). The Role of State Actors in Cybersecurity: Can State Actors Find Their Role in Cyberspace?. In National Security: Breakthroughs in Research and Practice (Pg. 16-43). IGI Global.

**3. Cyber-attacks associated with internal warfare**

This form of war is often accompanied by cyber guerrilla tactics[46]. Thus, the government must be especially careful when using online channels to reach people. For example, insurgents in the three southernmost provinces will use cyber-channels to unite. Moreover, this can involve financial attacks such as bank account hacking, phishing emails, or various forms of money fraud. Insurgents may use this money in continue to support terrorism. This form of money making is motivated by international terrorist groups such as North Korea[47]. To deal with this situation, the government can cooperate with financial institutions to control all local banks such as the National Bank of Thailand. The local branches need to cooperate with the government to exchange information and raise awareness of using online channels.

Intrastate wars are easy to deal with because national-state laws can be used to apprehend perpetrators to trace the origins of the funds used from the sources of terrorism (Wenhong, 2020). However, most of what terrorists want comes in the form of Bitcoin, not the traditional currency. Therefore, electronic currency may be relevant if a ransom is demanded. Second, the state should have use publicity and control online channels because various messages that are posted via online platforms persuade people who do not have the basic knowledge to deal with the attacks.

**4. Cyber warfare from non-state actors**

In the case of non-state actors, cyber-attacks have political purpose; internal politicians have a mutual cyber-related interests with non-state groups. Attacks from non-state actors can come in the form of pressures to change an information infrastructure. Such pressures can induce technology consumers or users of the Internet to change their political perception[48]. An attack from a non-state agent will create a problem for the nation state because states may not be able to use national laws to arrest the attackers. More importantly, a non-state actor cooperating with a state actor are still cautious because it is impossible to predict which country is behind the scenes of this attack.

**5. Cyber warfare against private actors under state support**

This type of cyber war can be complicated as it is indistinguishable from conflicts among corporations under the state or among private corporations with opposing national interests[49]. Therefore, it is difficult to detect the true objectives of the actors. Dealing with private companies involves companies that are not supported by any state because if they are, it will cause even more violence and can easily become a war between states. If Thailand encounters this situation, the Thai government must enlist technologically advanced agencies to suppress private companies or cooperate with private companies

[46] Kim, S. K., Cheon, S. P., & Eom, J. H. (2019). A leading cyber warfare strategy according to the evolution of cyber technology after the fourth industrial revolution. International Journal of Advanced Computer Research, 9(40), Pg.72-80.

[47] Rauta, V. (2020). Towards a typology of non-state actors in 'hybrid warfare': proxy, auxiliary, surrogate and affiliated forces. Cambridge Review of International Affairs, 33(6), Pg.868-887.

[48] *Ibid* Norris, 2003

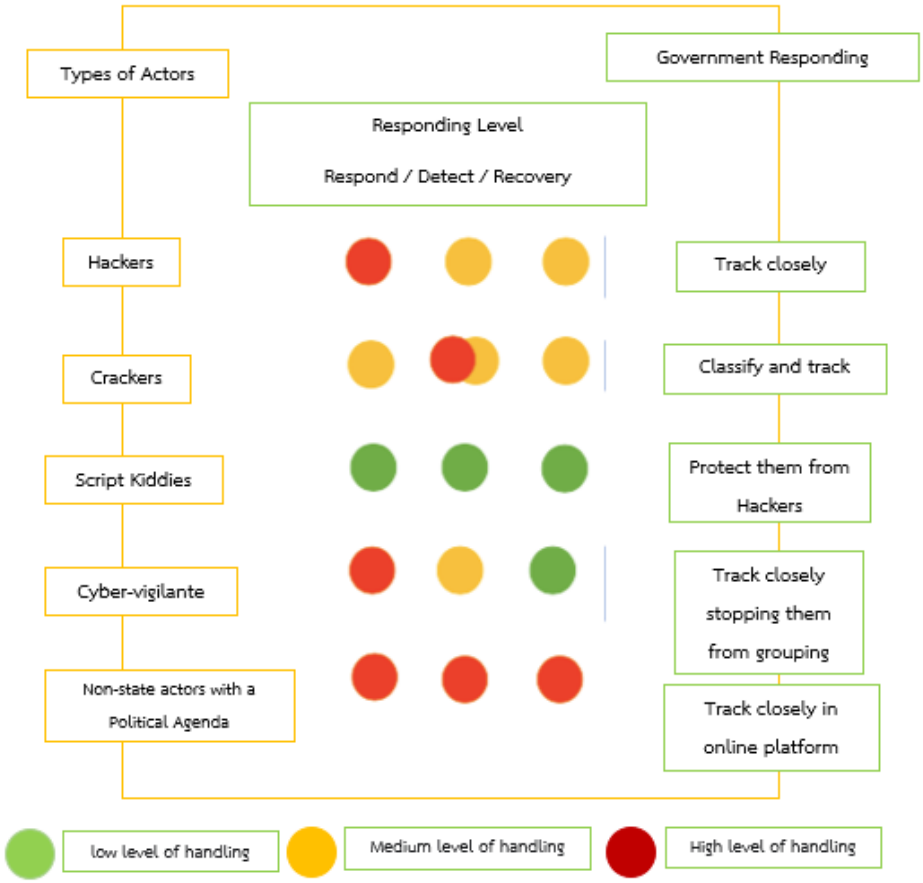
[49] Kostyuk, N., & Zhukov, Y. M. (2019). Invisible digital front: Can cyber-attacks shape battlefield events?. Journal of Conflict Resolution, 63(2), Pg.317-347.

under the control of the state itself, because they have personnel with the knowledge and ability to deal with private companies.

**6. Cyber warfare versus nuclear weapons warfare**

Thailand can learn from the Iranian response to the cyberwarfare of the US-Iran Stuxnet incident that used a complex virus with real physical effects[50]. Even though Thailand does not have its own nuclear power plant, nuclear plants could be built in Thailand or reach underground the ocean pipelines which can be targets for cyber-terrorists. The best way for dealing with this situation is to prevent a complex Trojan virus from attacking the system. Next, Thailand needs to build a shelter for people in the vicinity of power plants to minimise losses[51]. Thailand has no refuge or sanctuary. Therefore, creating these shelters will benefit people in the future during various disasters that occur unexpectedly. Military nuclear deterrence strategies cannot be applied to cyber warfare because of a non-border[52]. The lethality of a weapon affects its intimidation power, as in the case of nuclear weapons. Therefore, Thailand should use continuous cyber surveillance.

Types of Cyber Attackers and The Government Respons




[50] Gompert, D. C., & Libicki, M. (2019). Cyber war and nuclear peace. Survival, 61(4), Pg.45-62.
[51] Futter, A. (2018). Hacking the bomb: cyber threats and nuclear weapons. Georgetown University Press. Pg.111-115
[52] *Ibid*, Futter, 2018, Pg.111-112

**7. The Future of Cyberterrorism**

- Cyberterrorists are more likely to attack banking networks and financial transactions. International exchange baskets attack will make people in the country lose their confidence in the country's economy. Whether this action will affect large organizations is not yet known. The large international financial corporations will be able to intercept this problem in time before it causes structural damage. However, anonymous hackers from any country can temporarily bring an economy to a standstill, which leads to a destruction of security in the future.
- Cyberterrorists are more likely to attack air traffic control systems. A clear example is failure of a system control sensor in the captain's room, which can be accomplished hacking the system.
- Cyberterrorists are able to replace drugs in pharmaceutical factories and damage them. This is a very severe form of cyber-terror and cannot be predicted.
- Cyberterrorists can change the pressure level of gas pipelines causing system failure, explosion, and fire.
- Terrorists can switch information in the immigration system to facilitate immigration illegally.
- Terrorists can hack prison systems and can open all the doors of prisons across the country at the same time. This will create chaos that will be difficult to control.
- Inability to use mobile devices can make people panic because so much now depends on mobile devices and an Internet connection. If the system crashes, it will cause an interruption of people' lives. When using online money transfer systems, various security systems on personal mobile devices can be hacked so passwords from private data can be stolen.
- Using Artificial-Intelligence (AI) to gain power over people, AI can instruct people to make mistakes. If most people believed in AI working, for example, AI might direct a child to use a finger to pull a plug, since a child may not have much knowledge. If the AI tells them to do anything, they will follow that order.
- Social media will be the main channel for attacking companies through the use of bots to collect customer information. Attackers will use the information for their own benefit. Social media could be an important channel to create viruses asking for ransom from companies by using customer data as the hostage.

## 3. CONCLUSION AND SUGGESTION

This article focuses on strategic and tactical methods to combat cyberterrorism. The study is based on in-dept interviews with key informants from national agencies in Thailand that are divided into three different groups. This article has provided a definition of cyberterrorism and also attempted to divide cyber attackers into different categories based on their type. Finally, the paper suggests methods to help predict the risk of particular cyber-attacks in the future along with ways of responding to these

attacks. Cyber-attacks can be understood and responded to most effectively when the Government knows who is orchestrating the attacks, and what their purposes are.

## REFERENCES


Abdulmana, S., & Saleh, B. (2014). Coordinate negative content filtering and threat detection in Thailand on the Internet infrastructure. In The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M). IEEE.

Ayala, L. (2016). Detection of Cyber-Attacks. In Cybersecurity for Hospitals and Healthcare Facilities. Apress, Berkeley, CA.

Bhardwaj, A., & Goundar, S. (2020). Keyloggers: silent cyber security weapons. Network Security, 2020(2).

Dayem, L. (2018). The Ethics of Cyber Warfare. *Illini Journal of International Security*, 4(1).

Dever, J., (2013). Cyberwarfare: attribution, preemption, and national self-defense. *JL & Cyber Warfare*, 2, 25.

E Silva, K. K. (2018). Vigilantism and cooperative criminal justice: is there a place for cybersecurity vigilantes in cybercrime fighting?. *International Review of Law*, Computers & Technology, 32(1).

Futter, A. (2018). Hacking the bomb: cyber threats and nuclear weapons. Georgetown University Press.

Gaia, J., Sanders, G. L., Sanders, S. P., Upadhyaya, S., Wang, X., & Yoo, C. W. (2021). Dark Traits and Hacking Potential. *Journal of Organizational Psych*ology, 27(3).

Gandhi, F., Pansaniya, D., & Naik, S. (2022). Ethical Hacking: Types of Hackers, Cyber Attacks and Security. *International Research Journal of Innovations in Engineering and Technology*, 6(1).

Goel, S. (2020). National cyber security strategy and the emergence of strong digital borders. Connections, 19(1).

Gompert, D. C., & Libicki, M. (2019). Cyber war and nuclear peace. Survival, 61(4), 45-62.

Heinl, C. H. (2014). Regional cybersecurity: moving toward a resilient ASEAN cybersecurity regime. *Asia policy*, (18).

Holt, T. J. (2020). Computer hacking and the hacker subculture. The palgrave handbook of international cybercrime and cyberdeviance.

Jirawannakool, K., Sanglertsilapachai, N., & Siwamogsatham, S. (2009). Computer Security Incident Handling and Phishing Cases in Thailand. In Global E-Governance. IOS Press.

Kim, S. K., Cheon, S. P., & Eom, J. H. (2019). A leading cyber warfare strategy according to the evolution of cyber technology after the fourth industrial revolution. *International Journal of Advanced Computer Research*, 9(40).

Klein, J. J. (2018). Deterring and dissuading cyberterrorism. *Air & Space Power Journal-Africa and Francophonie*, 9(1).

Kobia, R. (2021). International Inter-Agency Coordination of State and Non-State Actors in Combating Global Cyber threat: Case Study of Kenya and Zambia (Doctoral dissertation, University of Nairobi).

Kostyuk, N., & Zhukov, Y. M. (2019). Invisible digital front: Can cyber-attacks shape battlefield events?. Journal of Conflict Resolution, 63(2), 317-347.

Kugler, R. L. (2009). "Deterrence of cyberattacks", *Cyberpower and national security*, 320.

Kumar, S., & Agarwal, D. (2018). Hacking attacks, methods, techniques and their protection measures. International Journal of Advance Research in Computer Science and Management, 4(4).

McDonald, C. (2021). Friends, rivals, foes: The private sector and online vigilantism impact on police cyber capabilities.

Mahoney, C. W. (2021). Corporate Hackers. Strategic Studies Quarterly, 15(1).

Nakayama, S. (2012). Govt Claims Cyberdefense Right/Says International Laws Should be Applied to Computer Infiltration. Yomiuri Shimbun.

Noguchi, M., & Ueda, H. (2019). An analysis of the actual status of recent cyberattacks on critical infrastructures. NEC Technical Journal, Special Issue Cybersecurity, 12(2).

Norris, P., (2003). "Digital divide? Civic engagement, information poverty & the Internet in democratic societies," at http://ksghome.harvard.edu/ ~ .pnorris. shorenstein.ksg/book1.htm, accessed 5 February 2004.

Perlroth, N. (2021). This Is How They Tell Me the World Ends: The Cyberweapons Arms Race. Bloomsbury Publishing USA.

Rauta, V. (2020). Towards a typology of non-state actors in 'hybrid warfare': proxy, auxiliary, surrogate and affiliated forces. Cambridge Review of International Affairs, 33(6).

Richet, J. L. (2013). From young hackers to crackers. International Journal of Technology and Human Interaction (IJTHI), 9(3).

Rugge, F. (2018). Confronting an" Axis of Cyber"?: China, Iran, North Korea, Russia in Cyberspace. Ledizioni-LediPublishing.

Schmid, Alex P and Jongman, Albert J. (2008). Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, & Literature (updated edn). (New Burnswick, NJ: Transaction, 2008).

Schneier, B. (2021, July). Invited Talk: The Coming AI Hackers. In International Symposium on Cyber Security Cryptography and Machine Learning. Springer, Cham.

Segal, A. (2011). Cyberspace Governance: The Next Step. Council on Foreign Relations, Policy Innovation Memorandum, (2), 1.

Silke, Andrew. (2004). "The Road Less Travelled: Recent Trends in Terrorism Research", in Andrew Silke (ed.) Research on Terrorism: Trends, Achievements and Failures (Abingdon: Routledge), 186-213.

Smith, A. D., & Rupp, W. T. (2002). Issues in cybersecurity; understanding the potential risks associated with hackers/crackers. Information Management & Computer Security.

Sun, L. (2021). Discussion on computer network security prevention based on big data era. In Journal of Physics: Conference Series (Vol. 1848, No. 1, p. 012103). IOP Publishing.

Tan, W. L., & Khader, M. (2022). Impact of justice-related dispositions on support for cyber vigilantism: The mediating effect of perceived severity of transgression. Legal and Criminological Psychology.

Taneski, N. (2021). Transformation of war–use of conventional military forces against no-state actors. The Annual of the Faculty of Philosophy in Skopje, 74.

Tantawutho, T. (2017, January). The computer crime incidents and the future of countermeasures in Thailand. In 2017 Third Asian Conference on Defence Technology (ACDT). IEEE.

ThaiCERT. (2018). Cybersecurity strategy for critical information infrastructure in Thailand.

Bangkok: Electronic Transactions Development Agency. Pg.1-28

Wenhong, X. (2020). Challenges to cyber sovereignty and response measures. Mirovaia ekonomika i mezhdunarodnye otnosheniia, 64(2).

Yeo, S., Birch, A. S., & Bengtsson, H. I. J. (2019). The Role of State Actors in Cybersecurity: Can State Actors Find Their Role in Cyberspace?. In National Security: Breakthroughs in Research and Practice. IGI Global.