International Journal of Crime, Law and Social Issues

Original Research Article

Received: 11 May 2022 **Revised:** 13 June 2022 **Published:** 13 June 2022

GOVERNMENT SECTOR'S RESPONSE IN COUNTER-CYBERTERRORISM IN THAILAND

Natthamon PETCHKLA[1] and Sumonthip CHITSAWANG[2]

1 Faculty of Political Science, Chulalongkorn University, Thailand; natthamon.p@chula.ac.th

2 Faculty of Political Science, Chulalongkorn University, Thailand; sumonthip.c@chula.ac.th

Handling Editor:
Professor Dr.Kittisak JERMSITTIPARSERT University of City Island, Cyprus

Reviewers:
1) Professor Dr.Attapol KUANLIANG Midwestern State University, USA.
2) Associate Professor Dr.Srisombat CHOKPRAJAKCHAT Mahidol University, Thailand
3) Associate Professor Dr.Wanaporn TECHAGAISIYAVANIT Mahidol University, Thailand

Abstract

Since the internet was invented, the global community has been rapidly changed by the advance of technology in cyberspace. A prominent issue now confronting society is the increase of cyberattacks which can be linked to cyber-terrorism. Individual countries in the world are now starting to address the concerns of cyberterrorism as a new means to achieve political goals. Thailand is one of these countries that has just started to pay this issue attention, but is not as advanced in dealing with the issue as some other nations are. In order to respond to the current cyberterrorism situation in Thailand and the situation that may occur in Thailand in the future, this presentation aims to review the definition of what cyberterrorism actually is, and the preparation plans of various governmental agencies which are at risk of cyberterrorism in order to evaluate the situation of cyber terrorism and the way to deal it in the future. Moreover, qualitative approaches which are documentary research and in-depth Interviews via in-person and online, will be used to develop the research solutions. In-depth interviews with more than 30 people from Thai policy analysts, technicians and international experts in cyber security have been undertaken and will be used in this research.

Keywords: Cyberterrorism, Counter-cyberterrorism, Government sector's Response, Fear of Cyberterrorism, Critical National Infrastructure

Citation Information: Petchkla, N., & Chitsawang, S. (2022). Government Sector's Response in Counter-Cyberterrorism in Thailand. *International Journal of Crime, Law and Social Issues, 9*(2), 1-11. https://doi.org/10.14456/ijclsi.2022.6

Introduction

Recently, through the media, society has been hearing more and more about Cyberterrorism and so has started to question how real the threat is to them and what any impact might be on them. The most important things for us to understand and then address are how real the threat is and what any likely impact on society will be, particularly because of Society's increasing reliance on technology. Here governments have a crucial role in understanding the risk so that they can employ proportionate and measured strategies at the appropriate time, to protect their citizens (Choi & Lee, 2018).

Cyber terrorism is caused by the change in the technology-driven social context but retains the traditional tactics of terrorism-the use of violence to create fear, targeting innocent people, causing the undermining of state credibility. These actions are largely attributed to political, religious, and racial interests (Fisher & Dugan, 2017). When traditional tactics are combined with modern technology, such as the use of terrorist technology attacking corporate networks of government agencies, especially the security agency and Industrial zones that affect the economy, destroying these entities will cause a huge impact at a national level. The use of cyber-attacks is one of the ways to attack the state's critical national infrastructure (CNI). Criminals must have a high level of computer skills in breaking through tightly secured systems, and the attacks require sophisticated and careful planning (Brickey, 2012).

The aim of this article is to explore the current situation of cyberterrorism in Thailand. It will also look at the cyber security policies of the more than 15 Thai government agencies in responding to cyber terrorism namely National Security Council, National Cyber Security Committee, Ministry of Digital Economy and Society, Bank of Thailand, National Intelligence Agency, Ministry of Defence, Royal Thai Air Force, Royal Thai Army, Technology crime suppression division, Ministry of Justice, Ministry of Public Health, Electricity Generating Authority of Thailand, National Broadcasting and Telecommunication division, National Institute of Development Administration, University of Sheffield and Chulalongkorn University. Moreover, it will study the development of policies and strategies for the prevention and response of future cyber terrorism. So as to consider the current cyber-terrorism situation in Thailand and the situation that may occur in Thailand in the future, this article shall review cyber-terrorism incidents in foreign contexts and the preparation plans of various governmental agencies which are at risk of cyber-terrorism. The Thai government has a preparation against cyber terrorism in the form of defensive action. The policy is to establishment the Office of the National Cybersecurity Commission (NSC) as a main agency for countering-measures and preventing cyber- terrorism in particular which the official launch date is August 2021 (Goel, 2020). As well as, the military also has a plan to protect the critical national infrastructures that vulnerable to attack by technical experts actively respond 24 hours (Heinl, 2014).

In this study, qualitative approaches, which are documentary research and in-depth interviews will be used to develop the research solutions. First, this research will use documentary research. This can be obtained from the study of academic documents and information from various sources both domestic and international related to cyber terrorism concepts and theories. Second, in-depth interviews with more than 30 people from Thai policy analysts, technicians, and international experts in cyber security have been undertaken and will be used in this research. Interviewees were selected by using a purposive random sampling method. The researcher selected participants who would be able to contribute to the objectives of the research such as policy makers, qualified practitioners, government officers who are dealing with cyber threats, and cyber experts. In order to resolve the research problem, the information received from this process will be analyzed using existing terrorism theories, to allow new conclusions to be drawn.

The rest of the article is set out as follows. First, it sets out a detailed study on cyber terrorism specifically focusing on the definition. Second, it outlines the current cyber situation in

Thailand and then reviews some of the policies that Thailand uses to respond to cyber terrorism and also its military strategies in cyberspace. Before then going on to compare the Thai Cyber-responding model to other nations' models. Finally, the article concludes by considering interviews with cyber-experts outlining how to respond to cyberterrorism in the future including.

What is Cyberterrorism?

"Cyberterrorism" is the complex interaction between two existing and well-defined concepts. That of "cyber," which relates to and means what is happening in cyberspace, and then "terrorism" which means an action that causes a huge damage at population involved with political motivation (Denning, 2000). So, what we end up with is the playing out of terrorism in the virtual world. All the existing motivations that drive terrorists to commit their acts of terrorism remain the same, but the realm in which they undertake these is vastly different from the 'real' world. Cyber terrorism is hard to define because of its complex and evolving nature. Multiple definitions are possible, and in fact, experts in security are yet to agree on a common definition. Symantec, however, has used the approach mentioned above as a template to define "pure Cyberterrorism" (Gordon & Ford, 2006). Authors will take this approach and so use the definition that it is groups or individuals with motivations for terrorism using information technology networks to realise their objectives.

The various information technology networks now allow the terrorists multiple avenues of opportunity. For example, using computer viruses which may hack into or disable a system. They can attack company websites or undertake denial of service attacks (DoS). Perhaps even simply use communication methods such as email to issue threats to their targets. Essentially, they make use of various telecommunications infrastructure, computer networks, and systems where they can share information between themselves or carry out threats on individuals and organisations via electronic means. Despite all of this opportunity and the fact that the media covers stories about exactly this type of thing, it is still frequently claimed that these attacks amount to nothing more than just computer hacks or malicious attacks. It is often argued that these attacks cannot be classed as terrorism in the purest sense, and so there is no such thing as cyber terrorism (LaFree, 2015). They argue that using the definition of terrorism that creates fear, significant physical damage, or death, means that firstly, it is very unlikely that this could be carried out online. Secondly, the programmes and processes we now have in place to protect computer networks and systems mean that it is even more unlikely. (LaFree & Dugan, 2015).

That being said, there is a well-supported argument that cyber terrorism is most effective and has the greatest impact when combined with an attack in the real (physical world) (Fisher & Dugan, 2017). Essentially using electronic means in the cyber realm to carry out an attack that has consequences and impacts on the real world. This could, for example, be achieved by carrying out an attack in the real world where multiple civilians are injured and require medical attention or damage that requires attendance by the fire brigade services. The terrorist group could amplify the impact of this by then attacking the IT networks that deliver the emergency operational response, so hampering the ability to respond to it. Additionally, cyber technology such as the internet allows terrorist organisations to share information anonymously and help prevent detection as might be the case in more traditional forms of communication. This allows them to plan in secret, raise funds and share propaganda across borders and reach all sides of the world instantaneously. This was picked up by the Director of the Central Intelligence Agency (CIA) in 2000, in the Director of the Central Intelligence Agency's statement on global security threats, he specifically mentioned how well-known terrorist groups such as Hezbollah, Hamas, and Al-Qaeda, were using encrypted messaging in files and emails to manage the running of their organisations. We know that one of the key figures in the attacks of 9/11, Ramzi Yousef, used encrypted files to hold details of how the attacks on the aircraft should be

conducted. These were not found until after the attacks and when it was too late because they were held on his computer (Tenet, 2004).

In this area, three main areas of concern for the future. The first is intelligence gathering, this is where actors, who may represent another state or other organisation, are able to harvest valuable data from their target by gaining access to their IT networks and systems, whilst remaining undetected (Aronson, 2005). The second is hacking, where networks can be disrupted once access has been gained by the perpetrator, where they can take control or cause the system to malfunction. The third is cyber warfare. Aronson uses Von Clausewitz's concept of war and says that it is played out digitally in a cyber realm. Here, rather than in a physical battlefield, two states battle each other and try to remove the defence capability of the opposite side by engaging in a digital war that seeks to knock out the defence capabilities via computer networks that control them (Aronson, 2005).

Moreover, cyber-terrorism is a new attack strategy which creates huge devastation and expands serious damages in many dimensions and arena. Just when some government's computers turn on and connect to internet world, the cyber-terrorists can access their computer and install some software programs to transfer confidential information, and at the same time, they can upload a virus into government's computers or other electronic machines (Wilson, 2008). Alongside all of these things, the terrorist groups are able to undertake mass recruitment and issue propaganda on a truly global scale. They have used the tactics of the large corporations in undertaking public relations and 'selling their brand' so that they can reach a mass audience and influence people across the world in their ways of thinking and justifying their cause. The fact that the cyber realm eliminates any sort of border between nations, means that a global reach is easily achievable and can be done without the usual laws and regulations that may stymie their work when using traditional forms of communication. The internet crosses borders and allows the groups to carry out cyber-attacks whilst not being identified. They no longer need to be at the site of an attack in order to undertake it, and could in effect be on the other side of the world, safe from the local authorities (Mazari et al., 2018). This means that the ability to carry out an attack using these cyber systems is already an increasingly attractive proposition for terrorist groups. But the fact that it also requires fewer people and costs less than traditional attacks, makes it an even more viable option for an increasing number of different groups (Mazari et al., 2018). In fact, there is a growing acknowledgement that multiple previous terrorist attacks can already be linked with having at least some cyber element. And there is a growing concern that weaknesses in existing computer programmes and systems, may make government and critical infrastructure systems alluring targets for any future cyber-attacks.

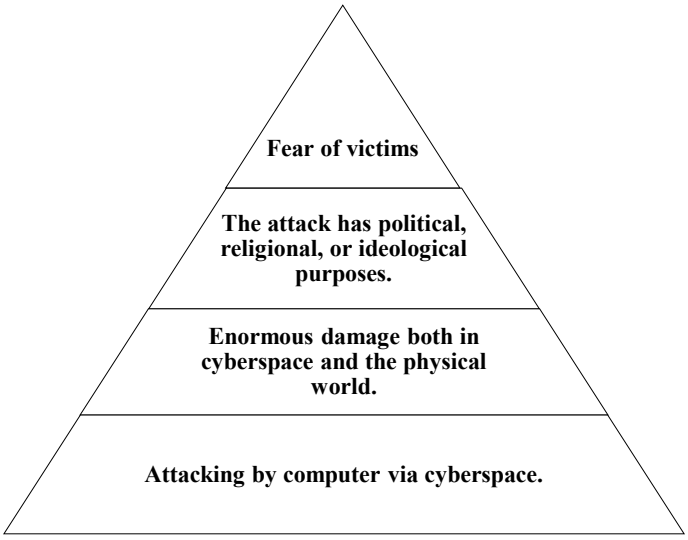

Figure 1 The Definition of Cyber Terrorism
Source: Denning (2000)

According to this thesis, it has proposed four factors of cyber-terrorism. By comparing the definition with other academics, the most comprehensive and closest definition of cyber-terrorism is divided into four components as follows:
1) Attacking by computer via cyberspace
2) Causing huge damage to life and property, both in cyberspace and the physical world.
3) The attack has political, religious, or ideological purposes.
4) Causing intimidation within a population or at the government level, and potentially influencing their behaviour through applying pressure.
When these four elements combine, there are the primary objectives of cyberterrorism. Physical damage caused by computer attacks can make people fear and agree to follow the guidelines of terrorists. It is mostly about politics, society, religion, and the ideology of the group. An example that can be applied with this cyberterrorism definition is the Single Gateway incident. This incident occurred in July 2016 by a group of people who disagreed with the government policy, the Single Gateway. They brough down the government website by pressing the F5 all together at the same time. This situation is different from the other cyber-attacks because the attackers had a political purpose. Even though, the result of this incident was not a huge impact, it recognized as a starting point that could be developed in the future. This is the reason why the government should focus on the cyberterrorism and ready to respond it.

The Cyberterrorism Situation in Thailand

In Thailand, cyber terrorism is predominantly targeting the general public by attempting to manipulate the views of groups of people using misinformation. Cyber-attackers directly target people who are from different social, racial, and religious groups, where they can create fear in a similar way. These fears will easily ingrain in people's minds, which criminals do not need to use advanced skills to attack. Creating a virus to attack the public is not complicated. Therefore, un-skilled criminals can do it. As a result, the governments need to develop approaches to countering cyberterrorism techniques by harnessing news and social media channels to control the situation. On the other hand, the attack on the country's critical infrastructure, terrorists must have high-skilled at attacking. Otherwise, they are usually done in the form of networks and organizations. As the impacts of the attack are hugely damaging,

governments need to study more about these new approaches and evolving attack patterns while finding defensive measures including organizational awareness (Goel, 2020).
In 2021, there were 2,250 cyber-attacks in Thailand. classified into the top-fourth rank types of threats. First, 30.5 percent of all threats (687 cases) were generated by programs or software developed to deliver undesirable results to users or systems (Malicious Code). Second, 25.6 percent (576 cases) was Fraud. Third, 20.9 percent (471 cases) were minor threats posed by vulnerability. Followed by 18.6 percent (173 cases) were threats arising from intrusions (Thaicert, 2021).
Thailand is one of the countries that is most aware of cyber threats, as evidenced by the Cyber Security Act 2017 (Sombatpoonsiri, 2017). Thailand is well prepared for cyber threats in the form of both state policies and laws. In addition, the Ministry of Digital Economy and Society is the primary regulator or all cyber-related missions. The Cyber Security Act is a mechanism to monitor, prevent, tackle and mitigate cyber threats for the critical information infrastructure. However, the Cyber Security Act has been implemented in Thailand to provide an appropriate response to cyberterrorism. So as to study the effectiveness of this Act, the researchers then chose to study agencies that are at risk of being targeted by cyber-terrorists, including the Ministry of Digital Economy and Society, Ministry of Justice, National Security Council, Ministry of Public Health, Provincial Electricity Authority, Bank of Thailand. Therefore, studying these agencies' responses to counter-cyberterrorism can help demonstrate the level of preparedness for cyberterrorism (Thaicert, 2021).

Thai's Policies on Responding to Cyberterrorism

The National Agencies of Thailand

Policy and Regulation Sector	Military Defense Sector	Targeted Agencies
- National Security Council - National Cyber Security Committee - Ministry of Digital Economy and Society - Bank of Thailand - National Intelligence Agency	Ministry of Defence Royal Thai Air Force Royal Thai Army Technology crime suppression division	Ministry of Justice Ministry of Public Health Electricity Generating Authority of Thailand National Broadcasting and Telecommunication division

Figure 2 The National Agencies of Thailand on Responding Cyberterrorism

Based on in-depth interviews with staff from the agencies above, this thesis has structured the national agencies of Thailand responding to cyber-terrorism into three categories: Policy and Regulation, Military Defence Sector, and Valuable Targets Agencies. Since there are many different missions among those sectors, it is easier to understand each sector's perspectives and policies through cyberterrorism.
According to in-depth interviews with the government agencies officers, all key informants have a consensus agreement that there is no real cyberterrorism in Thailand according to the thesis definition. However, there are some cases that move closer to the definition, according to an interview with an NCSC officer. The first example from 2015 stemmed from an apparent protest against plans by the state to limit access to websites which they defined and deemed as inappropriate. This proposal became known as the 'Great Firewall of Thailand' (Laungaramsri,

2016), and appeared to gain support from at least 10,000 Thai citizens. The form of the attack was to make Government sites (such as the main thai.go.th site) inaccessible through distributed-denial-of-service (DDoS) attacks. Even the site for the Ministry of information, communications, and technology (ICT) was targeted. Interestingly, those responsible saw what they did as a form of civil disobedience, rather than an attack and certainly not a form of cyberterrorism. This situation is an example of what the Thai Government would say falls within the definition of cyberterrorism. However, even though there was a political aim behind this activity, the impact of this situation did not cause huge damage to life or property enormously. It was minor computer networking damage which indirectly resulted in dis-credit of the government, said the senior cyber officer from the Ministry of Digital Economy and Society. There are not many cases that can be identified as cyber terrorism. However, a ransomware attack on Saraburi hospital in 2021, and when hackers linked to a hotel in Bangkok threatened Sony Pictures employees via email in 2014, are good examples of cyberterrorism that were provided by the interviewees.

Thai Cyber-responding Model Compared to Other Nation's Models

Based on a researched documentary method, most powerful nations have different responses to cyber threats. These can be summarized as set out in the table 1 (Kerschischnig, 2013).

Whilst this Cyber Security Maintenance Act is thorough and comprehensive in certain aspects, it is incomplete overall. This is because it makes no mention specifically of Cyberterrorism. It talks about the processes in place needed to help prevent or reduce the risks posed by cyber threats to state agencies through maintenance, management, and resolution following a cyber incident. It includes and references areas concerning security on a national and economic level, along with references to the military. The main body associated with overseeing this is the NCSC, which is the "National Cyber Security Committee" (translated). The members of this group show the high level of importance that this issue is given in Thailand, as it is chaired by the Prime Minister and contains prominent ministers (such as for Defense), and Permanent Secretaries (such as for Justice). As well as key prominent stakeholders from bodies such as the Royal Thai Police and National Security Council. There is a range of members from a range of disciplines (such as IT, science, engineering, and law, among others) who bring a wide range of expertise to ensure that when considering the threats posed, all are considered and thought through as fully as possible. As also mentioned elsewhere in this paper, the Thai Computer Security Incident Response Team (which follows a similar model to that used in the EU) provides a point of contact for the Thai internet community to report any cyber incidents (Chang, 2017).

Prominently, Thailand has made remarkable progress in cyber security such as creating a strong network among internal state agencies to exchange and share knowledge in order to protect their organizations from hackers. The cooperation can be recognized as a strength for Thailand. However, the government still lacks of international co-operational or joining in cyber community with the other powerful states. Therefore, the government needs to encourage Thailand to adopt international laws and implement them efficiently. Regarding to the tactic for countering cyberterrorism, the royal Thai army should adopt a tactic so-call cyber-surgery, which can be identified the cyber attackers into different categories such as Hacker, Cracker, non-state actor or state actor. Thus, Thai military officers can track each type of attackers and keep an eye on them.

Table 1 Cyber-Responding Models

United States of America	Russia	China
- USA launched a cyber defense plan, "Comprehensive National Cybersecurity Initiative" that provided more military means to protect CII. It also supported the development of public-private partnerships, education, and the workforce in cyberspace. - USA had a strategy for cyber defense policy and admitted an offensive element. - The National Security Agency (NSA) was launched to deal with signal intelligence.	- Russia is developing its cyberwarfare capabilities. - Russia has a secret service called FSB which coordinates with the internal security of the state, against terrorism and organized crime. However, it is the Foreign Intelligence Service that manages its response to espionage originating from other states, - Home of massive knowledge and initiative hackers.	- Encouraging ICT infrastructure and the use of cyberspace in economic goals. - Maintaining strict control over free speech on political issues. - Monitoring the internet traffic of over 400 million users. -Building up an offensive cyber strategy which can promote its superpower in the cyber world. - China is also accused as being part of using cyber espionage through private proxies.
EU Countries	**North Korea**	**Thailand**
- In 2009, the European Commission launched a project to protect CII. - Emphasizing cybersecurity measures and cooperation among international countries. - The UK takes a human security approach known as security of people and also encourages a muti-stakeholder approach. - France built national authority for cybersecurity as a national strategy in 2011. - Germany established a national agency for cyberspace as a national agenda.	- North Korea is known as a country which has a cyber-operation with the task of spying. - North Korea has the capability to wage a cyberwar. - However, due to a lack of realisable evidence, it is hard to confirm that North Korea is a powerful country in cyberspace.	- Thai government has recognised the Cyber-attack as a threat since it launched the Computer Crime Act in 2007 aim of protecting the computer systems from violations - The government has developed the legal framework until it launched the Cyber Security Maintenance Act, 2019. - Establishing the "National Cyber Security Committee" called "NCSC" and ThaiCERTs which is the Computer Security Incident Response Team for Thailand.

What Thailand Should Respond in the Future

The Thai Government responds to any incidents that it regards as cyber-terrorism using a model that is comparable to that used in the European Union (EU). The EU makes use of its experts in IT security, who come together from across their main bodies and institutions (Kerschischnig, 2013) to form CERT-EU, which stands for 'Computer Emergency Response Team'. They provide a coordinated response across the agencies and bodies contained within the EU. At a Governmental level, CERTs provide the overall coordination when responding to large-scale incidents-such as attacks on critical infrastructure. It also ensures all relevant

stakeholders are involved, which includes their counterpart teams in other countries with whom they share experiences and information.

The Thai government needs to learn and prepare to deal with cyber-terrorism from a legal perspective by increasing the legal framework to cover all the areas of cyber action and co-operate with international law to deal with cyber-terrorists in the future. As we know that international law is not enough to control cyber terrorism, because there is no law more powerful over the sovereignty of each state. Thus, Thailand has to co-operate and share information with the cyber-community alliances and also develop its own legal system efficiently enough to deal with cyber-terrorists on Thai soil. In order to deal with them, the government needs to use the operation so-call cyber-surgery, which can be identified the cyber attackers' purposes, means, and supporters. The important tactic is to start from a small point and induct to the whole point at the end. Therefore, it may be easy for the Thai government to tackle this problem.

Moreover, it can be clearly seen that most of the Thai government officers have insufficient skill in technology including, cyber security awareness according to the data collected from an in-depth interview. A quarter of the interviewees said that there are lot of minor cyber-attacks caused by the exploitation of their own officers, who were socially engineered by skilled hackers. Thus, the government should pay attention to how to provide more knowledge in cyber security to government officers and always update all important data in different portal accesses. Regarding the re-habitation process from the Department of Correction, there are 304 inmates who were arrested under offences of the Computer Misuse Act 2017 that have been treated in a similar way to the other prisoners. This issue should be recognized by the government that those offenders have computer skills which can be useful for the government's cyber security in the future. Thus, they should have a specific re-habitation program to address this, that is different from the other prisoners.

Conclusion

Cyberspace is a new dimension where the threat is more real than many people realize. Cyberweapons can be a powerful method to attack national power and intimidate state citizens. The article has suggested the government needs to be more resilient and robust than the cyber theories have predicted. Moreover, the government needs to clearly define the meaning of cyberterrorism in policy or legal acts which will then help them with the power required to control and punish cyberterrorists in the future. There are several models of responding to cyber-terrorism from different countries which the Thai government could consider. For example, the single gateway used in China. This method is effective because it controls all cyber activity across the country. However, this is not a model that could be easily replicated in Thailand because it would violate the rights of its citizens' freedom. There is a trade-off to be considered between the rights of individuals, and public security. It should however consider the skills and education it can provide, to ensure that individuals can protect themselves and the wider population from the threat of cyberterrorism.

Acknowledgement

I would like to express my special thanks of gratitude to the National Research Council of Thailand (NRCT), the Royal Golden Jubilee PhD, and the Thailand Research Fund (TRF) for giving me the golden opportunity to do this project.

References

Aronson, J. (2005). *Causes and consequences of the communication and Internet Revolution. The Globalization of World Politics: An Introduction to International Relations*. 3rd ed. Oxford: Oxford University Press.

Brickey, J. (2012). Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace. *CTC Sentinel, 5*(8), 4-6.

Chang, L. (2017). Cybercrime and Cyber Security in ASEAN. In *Comparative Criminology in Asia* (pp.135-148). Zürich: Springer.

Choi, K., & Lee, C. (2018). The Present and Future of Cybercrime, Cyberterrorism, and Cybersecurity. *International Journal of Cybersecurity Intelligence & Cybercrime, 1*(1), 1-4.

Denning, D. (2000). *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*. Retrieved from http://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm.

Fisher, D., & Dugan, L. (2017). Criminological Explanations for Terrorism. In B. Huebner. (ed). *Oxford Bibliographies* (pp. 1-14). Oxford: Oxford University Press.

Goel, S. (2020). National Cyber Security Strategy and the Emergence of Strong Digital Borders. *Connections: The Quarterly Journal, 19*(1), 73-86.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2*, 13-20.

Heinl, C. (2014). Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime. *Asia Policy, 18*(4), 131-160.

Kerschischnig, G. (2013). Cyberthreats and International Law. *Merkourios-International and European Law, 29*(76), 106-108.

LaFree, G., & Dugan, L. (2015). How Has Criminology Contributed to the Study of Terrorism since 9/11?. *Sociology of Crime, Law and Deviance, 20*, 1-23.

LaFree, G. (2015). Criminology, Terrorism, and Serendipity. In M. Maltz & S. Rice (eds). *Envisioning criminology* (pp. 119-126). Cham: Springer.

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

Mazari, A., Anjariny, A., Habib, S., & Nyakwende, E. (2018). Cyber Terrorism Taxonomies: Definition, Targets, Patterns, Risk Factors, and Mitigation Strategies. In M. Khosrow-Pour. (ed). *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications* (pp. 608-621). Pennsylvania: IGI Global Published.

Sombatpoonsiri, J. (2017). *Growing Cyber Activism in Thailand*. Retrieved from https://carnegieendowment.org/2017/08/14/growing-cyber-activism-in-thailand-pub-72804.

Tenet, G. (2004). *The Worldwide Threat 2004: Challenges in a Changing Global Context*. Retrieved from https://irp.fas.org/congress/2004_hr/022404tenet.pdf.

Thaicert. (2021). *Statistics*. Retrieved from www.thaicert.or.th/statistics/statistics-en2021.html.

Wilson, C. (2008). *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. Retrieved from https://apps.dtic.mil/sti/citations/ADA477642.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Conflicts of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.