

Analysis of the Impact of Transnational Cybercrime in Southeast Asian Countries on Global Social Development

Shuhan Zhang *

Bedes Senior School, Hailsham, United Kingdom

* Corresponding Author Email: mandy.zhang@bedes.org

Abstract. Recently, the frequent occurrence of cybercrime has brought a significant negative impact on the development of society. Based on the geographical location of Southeast Asia, where the Golden Triangle region is located, there have been frequent outbreaks of fraud crimes in recent times. Therefore, this article takes Southeast Asia as the research object and focuses on the discussion of criminal incidents in the region. At the same time, the article provides relevant issues brought about by transnational crime and its negative impact on social development. Finally, the article elaborates on illegal activities, the construction of legal frameworks, global economic and political impacts, and how to combat crime. The research in this article has important practical significance in clarifying the dangers and threats of cybercrime and building a good social environment.

Keywords: Transnational Cybercrime; Global; Southeast Asian Countries.

1. Introduction

1.1. Research Background and Significance

The growth of information and communication technology has revolutionized the world. With the expansion of internet penetration across the globe, societies have transformed into technologically dependent ones, with easier informational accessibility, such as the access to social platforms. According to Bankmysell '85.95% of the world's population owns a smartphone', which simultaneously provides opportunities for cyber criminals to exploit [1]. The expansion of internet accessibility has become the fundamental cause of the rise of cyber fraud, particularly in Southeast Asian countries such as Vietnam, Myanmar, Thailand, and China. This movement has not only resulted in an impact on individuals; it has become a threat to organizations, governments, and global security. The discussion today will delve into the complexities of fraudulent scams in Southeast Asian countries. The research in this article is of great practical significance in clarifying the hazards and threats of cybercrime and creating a favorable social environment.

1.2. Literature Review

BankMyCell provides global mobile usage information and provides the latest information on how many mobile connections are available in various countries. Vanes discussed the arms trade along the border between Myanmar and Thailand after the coup [2]. The annual report released by Interpol in 2022 provides relevant data collected by the government and experts in the field in collaboration with the United Nations. In recent years, this report has been cited and constructed by many experts [3]. Friend et al.'s research reviewed Ireland's experience in combating cybercrime and discussed the strengths and weaknesses of Irish cybercrime law [4]. Gerson discussed the urgent action of Thailand's Computer Crime Act, which was issued in 2016 and passed in 2007 [5]. Poulpunitha et al. used a series of data to support their argument and provided a detailed explanation of the information collection and funding process supported by the National Women's Commission [6] In 2019, the official agency of the US government, the Federal Bureau of Investigation, released information on international crime. Official organizations and experts in this field have collected a large amount of cited and frequently reviewed data to analyze the current situation [7]. However, there are still some illegal areas and extreme poverty areas that have not been included in the construction of the report.

Similar research has also been published in the European Organized Crime Review [8]. A DTA by Thuis, published by a doctoral student in the Journal of Law and Policy Transformation, takes India as a typical example to illustrate the trend of cybercrime, with data intensity that was recently published in official journals [9]. PwC officials also indicate the impact of crime on business [10].

1.3. Research Content and Framework

First, the study will start with cases of fraudulent activities in Southeast Asia, such as the typical case of the Golden Triangle. The second part of my main discussion will be the legal framework and social impact analysis, using the legal framework of other countries as an example. Then, the political and economic impacts of cybercrime, especially cyber fraud, will be discussed. Finally, methods to combat cybercrime are proposed.

2. The Transnational Cybercrime Activities in Association of Southeast Asian Nations

Recent rising in cross-border fraudulent activities in Southeast Asia have become a concern for the government. Bordering Southwest China, Thailand, Laos and Myanmar; the Golden Triangle is the centre of perpetrators of illicit fraud. It's known as the origin for numerous illicit transactions such as drugs and human trafficking. However, the rise in technology has unfortunately attracted the suppliers of the Golden Triangle to commit cybercrime, because it is more profitable than drug trafficking, while the risk of legal punishment and detection is lower than drug trafficking.

One of the cases 'bullets and weapons that have been confiscated by Thai law enforcement next to Myanmar's borderline' have again directly illustrated the nature of various transnational illegal markets and networks in the region [2]. This emphasizes the notion that transnational cybercrime activities cannot exist in a single country. In 2020, the COVID-19 epidemic triggered a digital transformation, and individuals, businesses and organizations were severely affected by the epidemic, which provided opportunities for cybercriminals to build new markets in cyberspace. Another reason for the high incidence of cybercrime is the high density of population in Southeast Asia countries. The growth of digital technology has caused a demand for internet accessibility. This reliance will become predominant of the rising number of internet security threats. According to INTERPOL's ASEAN Cyber Threat Assessment 'Cybersecurity experts project the total net cost of cybercrime to grow by 15 per cent per year over the next five years, reaching USD 10.5 trillion annually by 2025, up from USD 3 trillion in 2015' [3]. Examples of cybercrime include ransomware attacks, advanced persistent threat, phishing and social engineering and dark web marketplace.

3. Legal Framework and Social Impact Analysis

3.1. Legislative Framework Against Cybercrime

The legislative framework against cybercrime varies in different countries. One successful case is the Review of Irish experience on fighting cybercrime [4]. This article first looked at the primary cyber related criminal legislation in Ireland, which is part of the Criminal Damage Act 1991. This only has a limited understanding of intent on modern technology and barely had a sense of cybercrime when first constructed. However, in a more recent study, Irish cybercrime legislation has been reimplemented. Thailand's Computer Crimes Act addresses unauthorized access, data damage and related offences while passing the Personal Data Protection Act to regulate personal data processing [5]. Another research published by S. Poulpunitha in 2021 on the 'strategies to prevent and control of cybercrime against women and girls' states that due to gender inequality only women and girls are associated with cybercrime in India, the IT Act 2000 have enacted by the government in order to combat against cybercrimes, and the act includes punishment on "hacking, publishing of obscene materials on the net, tampering the data" [6]. Although the countries enacting Act to protecting vulnerability groups, there's still concerns for woman been actively involved, showing that there's

still loopholes in the law enforcement and legislation framework, further state that official organizations need to improve and refine the legislative framework as quick as possible. While countries like Ireland, Thailand, India have begun to combat and improving their legislative framework against cybercrime, the Europol's cybercrime center have also brought up their actions. They created an administrative framework to prioritize the transitional cybercrime organization and focusing on exploitations on children. The benefit of their system is that they enable countries across the Europe to join the investigation of the new platform to take actions against the national crime [8]. In comparison to these countries, Myanmar and Vietnam's legislative framework is still incomprehensive. Therefore, is important to leaning from experience of other countries and enhancing the fight against cybercrime. At the same time, it's essential to aware that the effectiveness of the laws is dependent on their enforcement and international cooperation, especially in transnational crime organizations when strengthen the legislative framework.

3.2. Global eEconomic and Political Impact

The report of INTERPOL's ASEAN Cyber Threat Assessment has presented that data breach incidents and cyberattacks during the year of 2020 caused large numbers of financial losses and disrupt the dynamic and stability of economic systems worldwide [3]. According to the 2019 FBI Internet crime report 'the total financial losses across the globe for the past 5 years have reached \$27.6 billion' [7]. At the same time, the growing number of cybercrimes is also causing concerns in national security. It can be used as a tool for political manipulation, and terrorism. State-sponsored cyber-attacks can target other nations' infrastructure, military systems, and sensitive government information, which will also cause public panic while successfully provoking the government and worsening the international relationship. The prevailing socio-economic instability within the Golden Triangle stands as a foundational factor driving the escalation of inequality and unlawful undertakings in the region. Given that the Golden Triangle remains beyond the governance of any singular nation or authority, it has become a fertile ground for lucrative enterprises such as illegal drug production and human trafficking, which generate substantial profits while diverting resources from the legitimate market. Consequently, a growing number of individuals with lower incomes are increasingly drawn towards engaging in this high-profit sector, which has again reinforced the presence of an illicit economy in the area. While cybercrime brings a significant impact to larger society, it also impacts over businesses [9]. "46% of organizations reported experiencing fraud or financial crime over the last 24 months; 70% of those organizations that did encounter it experienced new incidents of fraud as a result of COVID-19 disruptions" [10]. The research has claim that cybercrime over business will consequence a fall in revenue for firms which is a huge problem for firms, especially for small firms, they're having less economies of scale and limited money to invest, therefore cybercrime will badly effect the productivity of the industry. In addition, large companies may lose their commercial secret due to data hack, which can be a big threat to companies in a greater scale.

4. Combating of Transnational Cybercrime

4.1. Set up Anti-cybercrime Unit in Southeast Asia Countries

Previous claims that most countries in Southeast Asia do not have a minister or a specific department in charge of the cybercrime unit, it may be inferring that the official government may not have yet realized the negative impact and tremendous effect of cybercrime. Therefore, it is essential for Southeast Asia countries' official organization and the government to aware the impacts and address the issue with specialized approach. Establishing these units will bolstering national cybersecurity and develop and enforce legislation, regulation, and other cyber security policies. Most importunately, it can foster international bunding and cooperation with the recent information and showing the close bunding between Southeast Asia countries, which also ensures the international bunding relations.

4.2. Provide Education in order to Increase the Public Awareness.

Another crucial strategy in combating cybercrime is to prioritize public education and awareness. By providing education to the general population, governments will empower individuals of various forms of cybercrime, includes online fraud, phishing attacks, and identity theft. By raising public awareness, communities will be more resilient to cyberattacks, as public are better equipped to detect the suspicious activities. However, this can be a huge cost to government in LIC and NEEs, as the education requires labor and technologies, but overall informed individuals with the knowledge and skills will protect themselves against several consequence of cyber crime

4.3. Developing the New Legislative Framework in ASEAN Countries

The existing of legal framework often lags behind the rapid development of cybercrime, therefore laws must be adapted and modernized to effectively prosecute cybercriminals. Each country may have a different legislative framework with different approaches and aspects, but it is important to ensure that countries can work together and provide the support to law enforcement agencies operating domestically or across the borders. By structuring a legislative framework, government will strengthen the protection on public's digital right and discourage the fierce criminal to harm individuals, organizations and greater society.

4.4. International Cooperation

Most importantly, cybercrime often occurs across national borders such as places like the golden triangle, therefore making international collaborations a cornerstone in the global battle against transnational cybercrime organization. Most of the cybercriminals and organization operate across national borders in places like the golden triangle, making domestic police more difficult to capture. By sharing information and resources the Southeast Asian country can tracking and apprehending criminals in different jurisdictions, ensuring that they face consequences for their actions. Therefore, countries should work together through international agreements and organizations like INTERPOL and UN to share information and expertise to solve the cybercrime issue fundamentally.

5. Conclusion

The purpose of this study is to discover the growing threat of cybercrime to global security, the author begins by presenting examples of transnational cybercrime activities in Southeast Asian countries followed by a discussion of legislative frameworks of each country and the global political and economic impact and conclude by suggesting ways to address and combat this serious crime. The result of the study show that cybercrime is no longer a minor problem, with a gradual increase in the number of people being scammed and involved in illegal activities. The general population across the globe should pay attention to this research, as it shows how cybercrime can severely affect the future of individuals, businesses and organizations. This research is essential to remind people cybercrime is everywhere around you, is important for government to work together to combating against this serious issue. The limitation of this dissertation is that the topic is too dangerous and sensitive for the collection of primary data, therefore most of the information is cited by other articles.

References

- [1] BankMyCell. <https://www.bankmycell.com/blog/how-many-phones-are-in-the-world>, last accessed 30/08/2023
- [2] News, V. Myanmar border gun seizures stoke fears of illicit post-coup arms trade. Voice of America (VOA News). https://www.voanews.com/a/east-asia-pacific_myanmar-border-gun-seizures-stoke-fears-illicit-post-coup-arms-trade/6206939.html 2021, June 12, last accessed 02/09/2023
- [3] ASEAN cyberthreat Assessment 2021, <https://www.interpol.int> 2021, last accessed 03/09/2023

- [4] Friend, C., Grieve, L. B., Kavanagh, J., & Palace, M. Fighting cybercrime: A review of the Irish experience. Zenodo. <https://zenodo.org/record/4766528>, last accessed 03/09/2023
- [5] Gerson, K. (n.d.). Thailand: Grave concern over Thai Computer Crimes Act. <https://www.amnesty.org/en/wp-content/uploads/2021/05/ASA3949442016ENGLISH.pdf>, last accessed 03/09/2023
- [6] Poulpunitha, Dr. S., Manimekalai, Prof. K., & Veeramani, Dr. P. Strategies to prevent and control of cybercrime against women and girls. *International Journal of Innovative Technology and Exploring Engineering*, 2020, 9(3), 609–612.
- [7] FBI releases the internet crime complaint center 2019 internet crime report. https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf, last accessed 03/09/2023
- [8] Marcena Hunter, The European Review of Organised Crime , Innovation in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce(J-CAT) https://d1wqtxts1xzle7.cloudfront.net/39045137/08_ReitanoEtAl_pp142-154-libre.pdf?1444248713=&response-content-disposition=inline%3B+filename%3DInnovations_in_International_Cooperation.pdf&Expires=1694215390&Signature=CFdayn-LrZPx-88s5TjhLi5Za3XY9nFvheh3q~7fQlhpP8Pmv4sHBtSo9uzAL3lhFeR-8O0If7QLwmmow6utkA6o5aucCZOFA3u8PjQnFePVvtJj-9Jcp3swT5NnTDapr-FBIW5nnRpU39Yg69JZajaPWYwnv1TDgEtHu-WOyjd4jzYZkgZS5c2M4Wn9a8OKvZ~mlCZ9IXWdcGJJDObIns-BLJjU95S~lnHAu9M-SrktMw2zlerBUPq0XjLQQcFoXq2Tf-6G1O694O1U7OZOr0ykrvNAn8FWXnAgS2Y5fFU~EXVt0rgdJuo8fs1qJtZu4z4EfqlfsS5d2DXhzaYrQA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA last accessed 06/09/2023
- [9] Tanya Gupta, Emerging trends of cybercrime in India: A contemporary review, *Journal of Law and Policy Transformation*, <https://journal.uib.ac.id/index.php/jlpt/article/view/7839/3323>, last accessed 07/09/2023
- [10] PwC Cybercrime poses biggest threat to businesses – as the impact of hackers becomes more destructive, <https://www.pwc.com/bm/en/press-releases/pwcs-global-economic-crime-and-fraud-survey-2022.html#:~:text=The%20survey%20of%201%2C296%20business%20leaders%20from%20across,common%20crimes%20experienced%20by%20organisations%2C%20regardless%20of%20revenue>, last accessed 10/09/2023