Legal Frameworks for Combating Dangerous Cyber Offenses in Vietnam

Nguyen Van Khoat

Ph.D in Law, Faculty of Criminal Law and Criminal Prosecution,
Hanoi Procuratorate University, Vietnam
Orcid: 0009-0007-6594-8942

Abstract

In recent years, Vietnam has witnessed a significant rise in cybercrime, posing serious threats to national security, economic stability, and individual privacy. The rapid digital transformation and increasing internet penetration have outpaced the development of effective legal frameworks to combat these dangerous cyber offenses. This study analyzed the existing legal frameworks in Vietnam concerning cybercrime, assessed their effectiveness, and identified gaps that hinder effective law enforcement. The study systematically examined relevant laws, regulations, and policies, including the Cybersecurity Law and the Penal Code, while also considering international best practices in combating cybercrime. Additionally, the study used specific cases and peer-reviewed journal articles on the subject of legal frameworks around cyber offenses to synthesize and compare the analysis from the laws. Findings indicate that while Vietnam has made strides in establishing a legal foundation for addressing cybercrimes, challenges remain, including vague definitions of cybercrimes, insufficient enforcement mechanisms, and a lack of public awareness regarding cybersecurity laws. This study emphasizes the urgent need for comprehensive reforms to strengthen Vietnam's legal frameworks, including clearer definitions of cyber offenses, enhanced collaboration between government agencies, and increased public education on cybersecurity. This study is relevant not only for policymakers and legal practitioners in Vietnam but also for scholars and international organizations seeking to understand the complexities of cybercrime legislation in emerging digital economies.

Keywords: Vietnamese Law, Cybersecurity law, Policy reform, High Tech crime investigation, Digital transformation.

1. Introduction

In the context of globalization and the ongoing Fourth Industrial Revolution (Bone, 2024), cyberspace has emerged as a critical component of economic, political, and social life in Vietnam. Nguyen et al. (2021) reveal that this rapid digital transformation has resulted in unprecedented opportunities for growth and innovation, propelling Vietnam to significant socio-economic achievements. However, Nguyen & Luong (2021) note that such achievement has equally given rise to a troubling increase in cybercrime. These crimes have been found to pose significant threats to national security, public safety, and the legitimate rights and interests of individuals and organizations (Luong et al., 2019). The evolution of cybercrime, as observed by Luong et al. (2019), shows that it is becoming equally complex, sophisticated, and transnational. For instance, offenders can operate from virtually anywhere in the world, engaging in a range of illegal activities. The criminal activities could entail the distribution of malware, hacking of control systems, theft of sensitive data, the spread of harmful content, and remote manipulation of devices that can inflict physical harm. This dynamic landscape presents formidable challenges for law enforcement agencies, as traditional methods of

detection and control are often inadequate in addressing the nuances of such cyber offenses. Given this pressing situation, the study and analysis of cybercrime in Vietnam is of urgent importance. It is essential to identify existing legal loopholes, analyze the challenges faced in enforcement, and propose feasible legal solutions to enhance Vietnam's capacity to prevent and combat cyber-related criminal offenses effectively. This article aims to clarify the nature and legal characteristics of crimes involving the illegal use of computer networks and telecommunications systems to commit dangerous acts. Furthermore, it will analyze the existing legal frameworks, evaluate the current status of enforcement, and recommend necessary legal reforms to improve the effectiveness of criminal law in this domain.

2. Overview of Computer Network Crimes

The landscape of cybercrime or cyber offense is characterized by its complexity and the evolving nature of threats. According to Lusthaus (2024), cybercrime entails criminal activities that exploit computer systems and networks to cause harm and/or inconvenience, targeting individuals, organizations, and governments. One of the most common types of cybercrime includes unauthorized access to systems, known as hacking. Deora & Chudasama (2021) reveal that hacking allows criminals to steal or manipulate sensitive data. Additionally, using a case example of remote control of automated devices, such as drones or 3D-printed weapons, Madzhumayev (2023) reveals that cybercriminals can exploit vulnerabilities in these technologies to cause harm or disruption from a distance. For instance, a hacked drone could be used to conduct surveillance or deliver harmful payloads, while compromised automated systems in manufacturing or transportation could lead to catastrophic failures and accidents.

Another prevalent form is malware distribution, where harmful software is spread to disrupt operations or extract information. The distribution of malicious software, or malware, is designed to gain unauthorized control over systems, destroy data, or spy on users and organizations. Malware takes the form of viruses, worms, and ransomware, each with its own destructive capabilities. Once embedded in a system, malware can compromise sensitive information, disrupt operations, and even hold data hostage for ransom (Macdonald & Frank, 2017). Such dynamics lead to significant financial losses and reputational damage.

Broadhurst et al. (2019) identify phishing as a significant concern, involving deceptive attempts to acquire sensitive information by masquerading as trustworthy entities. The impact of cybercrime on society is profound, posing serious risks to national security and public safety. According to Junger (2018), victims of cybercrime face financial losses, reputational damage, and emotional distress due to these offenses. In close relation to phishing is financial fraud. According to Nicolls et al. (2021), cybercriminals have thrived by organizing large-scale schemes through fake websites, social media scams, or malware-infested applications. These fraudulent activities can lead to significant financial losses for individuals and businesses, eroding trust in online transactions and digital platforms.

The above findings underscore the multidimensional impact of cybercrime, highlighting its reputational, financial, and emotional impacts on victims. This insight exposes the complexity of cybercrimes as not only a technological issue, but also a societal issue that affects people on different scales. Additionally, while these findings confirm that the crimes are exclusively digital, their consequences can manifest as physical, psychological, and financial harm to individuals, institutions, and the state. Therefore, the interconnectedness of computer and telecommunications networks implies that a single cyber incident can have ripple effects, impacting not just the immediate victims but also the broader community and economy. Understanding the nature of these dangerous acts and their implications is crucial for developing effective legal frameworks and enforcement strategies to combat cybercrime and safeguard the digital landscape.

2.1 Definition of Computer Networks, Telecommunication Networks, and Illegal Use

To comprehend and tackle issues of cybercrime, understanding the basic functionality of computers and Telecommunications networks is a prerequisite. A computer network is a system of interconnected devices that communicate with one another to share data, resources, and services. These networks can vary in size and complexity, ranging from small local area networks (LANs) that connect a few devices within a limited geographic area, to extensive wide area networks (WANs) that span large distances and connect multiple

networks across cities, countries, or even continents (Wan & Zhang, 2021). The observed connectivity reveals that the primary purpose of a computer network is to facilitate communication and collaboration among users, enabling them to access shared resources such as files, applications, and internet connectivity.

On the other hand, a telecommunications network encompasses the technologies and infrastructure that enable the transmission of information over distances. This includes communication methods, such as voice calls, video conferencing, and data transfer, utilizing electromagnetic signals, fiber optics, and satellite systems (Agzamovich & Hikmatulla, 2021). Looking at the above definitions, it is evident that these networks form the backbone of global communication, supporting everything from personal conversations to critical business operations and emergency services.

Nevertheless, the prevalence of illegal use of computers and telecommunications networks in modern day has threatened the obvious benefits of such technologies and infrastructure. As a result, scenarios have not only violated legal statutes but also undermined the integrity and security of the networks involved, posing significant risks to individuals, organizations, and society as a whole. It is worth noting that as technology continues to advance and the interconnectedness of networks increases, the potential for cybercrime is expected to grow equally. As a result, the evolution of legal countermeasures is equally expected to be of the same measure in order to address these challenges effectively. Understanding the definitions and implications of computer networks, telecommunications networks, and their illegal use is crucial for developing comprehensive strategies to combat cybercrime and protect the integrity of digital communication systems.

2.2 Characteristics of High-Tech Crimes

One of the most significant characteristics of cybercrime is the anonymity it affords offenders. Many cybercriminals utilize virtual private networks (VPNs), the dark web, and various encryption tools to conceal their identities and locations (Proulx, 2022). This anonymity could make it exceedingly difficult for law enforcement agencies to trace the origins of cyberattacks or identify the perpetrators, creating a significant barrier to effective prosecution and deterrence. Additionally, Cybercriminals leverage on the cross-border nature of cybercrime by initiating attacks from abroad, targeting victims within Vietnam's territory (Nguyen & Luong, 2021). This transnational aspect complicates jurisdictional issues and enforcement, as different countries may have varying laws and levels of cooperation in addressing cybercrime. As a result, a crime committed in one jurisdiction can have profound implications for victims in another, necessitating international collaboration and legal harmonization to combat these threats effectively. Another defining feature of cybercrime is its low cost combined with high impact. Minimal tools like laptops, internet bundles, and readily available software are used by cybercriminals to launch cyberattacks that inflict enormous damage (Van Nguyen, 2022). This accessibility lowers the barrier to entry for potential offenders, allowing a wider range of individuals to engage in cybercriminal activities, from amateur hackers to organized crime syndicates.

Finally, cybercriminals' rapidly evolving techniques further complicate the landscape of cybercrime. Continuous advancements in technologies such as artificial intelligence, blockchain, and deepfake technology (Bone, 2024) enable offenders to develop new methods to outpace conventional detection systems. Logically, as these technologies become more sophisticated, so too do the tactics used by cybercriminals, making it imperative for legal frameworks to adapt and respond to the dynamic nature of cyberspace. These characteristics collectively render cybercrime particularly dangerous and challenging for traditional criminal justice systems. The need for legal frameworks that are responsive to the evolving nature of cyberspace is more critical than ever.

3. Cybercrime Legislation in Vietnam

Following rapid technological development and the ongoing Fourth Industrial Revolution, Nguyen et al. (2021) acknowledge that Vietnam’s legal system has equally recognized the growing threat of cybercrime and the misuse of digital networks. This recognition has been affirmed by the incorporation of cyber offenses into specific provisions within its criminal law framework. Efforts to address cybercrime started off back in

1999 under the 1999 Penal Code of Vietnam. Specific articles, such as article 143 of the Penal Code, sought to address the destruction or deliberate damage of property, which could encompass acts like damaging computer systems or data. Articles 230-239 of the Penal Code also cover illegal activities related to weapons, explosives, radioactive elements, and toxins, which could extend to the misuse of technical means or devices in cybercrime. However, due to a lack of specific provisions on the categories of cybercrime, which exposed significant gaps in addressing cyber offenses, there was a need to amend the 1999 Penal Code.

The 2015 Penal Code came as a remedy to the limitations of the 1999 Penal Code. Specifically, Article 285 addressed the misuse of information technology systems. Eventually, technical errors as well as the need to expound on the legal framework for cyber offenses led to the amendment of the 2015 Penal Code in 2017. Furthermore, these amendments captured the gaps in the alignment of Vietnam's legal framework on cybercrimes to the international standards and improved the justice administration associated with cybercrime offenses.

Article 288 of the 2015 Penal Code, amended in 2017, specifically remains the important legal reference point on cyber crimes in Vietnam. The article criminalizes the illegal provision or use of information on computer networks or telecommunications networks. This provision encompasses a range of harmful activities, including disseminating false information, offenses against individual honor and dignity, incitement to violence, and distorting the truth. Targeting and criminalizing these specific behaviors ensures that individuals and society are protected from the damaging effects of misinformation and online harassment, which can have serious repercussions in both personal and public spheres.

Another critical provision is Article 289, which addresses illegal access to computer networks, telecommunications networks, or electronic devices belonging to others. This article criminalizes unauthorized access for harmful purposes, thereby reinforcing the principle that individuals and organizations have the right to secure their digital assets. Unauthorized access can lead to data breaches, identity theft, and other forms of cybercrime, making this provision essential for safeguarding personal and organizational information. Article 290 focuses on the obstruction or disruption of the operation of computer or telecommunications networks. This provision penalizes acts such as introducing malware, interrupting operations, or sabotaging digital infrastructure. The purpose of this provision is to maintain the ethics, functionality, and reliability of critical digital services, which are vital for the economy and public safety.

Additionally, Article 291 addresses the creation and distribution of malware, specifically targeting those who design or spread software intended to damage data or systems. This provision recognizes the significant threat posed by malicious software, which can lead to extensive damage and financial loss for individuals and organizations. The law aims to deter the development and dissemination of harmful software by holding offenders accountable for their actions in this area. Beyond the 2015 Penal Code, Vietnam has a complementary law called the Cybersecurity Law, which was enacted in 2018. This law provides comprehensive regulations on cybersecurity protection, prevention of cyberattacks, and safeguarding national security in cyberspace.

While these provisions provide a legal basis for criminal prosecution in cybercrime cases, they primarily cover technical violations or economic crimes. However, the scope of the current legal framework may not adequately address more dangerous acts, such as cyberterrorism, the manipulation of critical infrastructure, or the incitement of mass violence through digital networks. These complex and evolving threats require a more nuanced understanding and more precise delineation within the legal terminology and scope. As cybercrime continues to evolve, Vietnam's legal system must adapt and expand its provisions to encompass a broader range of cyber offenses. This includes developing specific laws that address emerging threats and ensuring that law enforcement agencies are equipped to handle the complexities of cybercrime effectively.

3.1 Comparative analysis

Vietnam's current approach to addressing cybercrime can be effectively compared with international legal standards and best practices, particularly those established by countries such as the United States, the

members of the Council of Europe, and China. This comparative analysis highlights the strengths and weaknesses of Vietnam's legal framework about global norms and practices in combating cybercrime.

The United States' legal framework for addressing cybercrime is primarily governed by the Computer Fraud and Abuse Act (CFAA). This legislation criminalizes hacking and the transmission of malicious code, imposing severe penalties for offenses that significantly damage human life, public health, or national security. The CFAA is a robust deterrent against cybercriminal activities, reflecting a proactive stance toward protecting critical infrastructure and public safety. Additionally, the same act enacted in 1986, has undergone several amendments up until 2018. This shows the coherence and consistency in improving the legal structures. Vietnam could learn from this by constantly improving and developing a specific legal framework, for instance, the cybersecurity law, making it a one-stop shop for legal dynamics of cyber offenses, as opposed to having multiple provisions in other laws, just mentioning limited aspects of cybercrime. However, it is also essential to acknowledge that CFAA remains to be a work in progress as outlined by Soulier (2023). This acknowledgment confirms that cybercrime is a dynamic field and legislation frameworks ought to be dynamic too to be able to counter cyber offenses effectively.

The Council of Europe's Budapest Convention on Cybercrime represents a significant international benchmark for defining cybercrime and establishing procedures for cooperation among nations. The Convention emphasizes the importance of cross-border collaboration, lawful interception, and the preservation of data, providing a comprehensive framework for addressing cybercrime on a global scale (Campina & Rodrigues, 2022). The member states under this convention commit to harmonizing their legal frameworks and enhancing collaboration in investigating and prosecuting cyber offenses. While Vietnam has ratified several international treaties related to cybercrime and cybersecurity, it has not yet acceded to the Budapest Convention. This absence limits Vietnam's ability to engage in international cooperation fully and may hinder its effectiveness in combating transnational cybercrime, which often requires collaborative efforts across jurisdictions.

China's Cybersecurity Law, effective from 2017, establishes a comprehensive legal framework that prioritizes national security, public order, and the use of network technologies to combat terrorism and incitement. This law reflects China's approach to cybersecurity as a matter of state security, emphasizing the need for strict regulations and oversight of network activities. The Cybersecurity Law includes provisions for data localization, user identification, and the monitoring of online content, a mechanism to prevent the misuse of digital networks for harmful purposes. While Vietnam's legal framework addresses various aspects of cybercrime, it may benefit from adopting a more rigorous approach similar to China's, particularly in prioritizing national security and public order in its cybersecurity strategy.

3.2 Gaps in the Current Legal Framework

Despite the presence of criminal provisions aimed at addressing cybercrime in Vietnam, several significant issues hinder the effectiveness of the legal framework. One of the primary concerns is the vagueness of definitions within the legal texts. Terms such as "dangerous acts" (in article 109), "illegal use" in article 318, and "incitement" (in article 117) are not consistently defined or interpreted in the 2015 Penal Code, amended in 2017. This lack of clarity creates room for legal uncertainty, making it difficult for law enforcement agencies, legal practitioners, and the judiciary to apply the law uniformly. The ambiguity surrounding these terms can lead to varied interpretations, which may result in inconsistent enforcement and prosecution of cybercrime cases. This inconsistency undermines the rule of law and can erode public trust in the legal system.

Furthermore, an overlap of articles provisions within the 2015 Penal Code is another legal gap. Certain behaviors may fall under multiple criminal clauses, leading to confusion regarding which article should be applied in a given case. According to Van Nguyen et al. (2022), such overlaps have resulted in inconsistencies in indictment or sentencing, as different courts or prosecutors choose to pursue other charges for similar offenses. Such discrepancies can create a perception of unfairness in the legal process and may ultimately weaken the deterrent effect of the law.

Additionally, the lack of categorization of cybercrime, a very important aspect in cybersecurity within the 2015 Penal Code poses a challenge. The current legal framework does not clearly distinguish between low-level technical violations and high-risk acts that endanger national security or public safety. This failure to categorize offenses appropriately could lead to inadequate responses to serious threats, as less severe violations may be treated with the same level of scrutiny as more dangerous acts. A more refined categorization system would enable law enforcement and the judiciary to prioritize resources and responses based on the severity and potential impact of the offenses.

Finally, Bui and Lee (2022) observes that the current legal framework in Vietnam has had the tendency of being more reactive than preventive. Existing laws are primarily designed to punish harm after it has occurred, rather than enabling proactive detection and deterrence of cybercrime. This reactive approach limits the effectiveness of the legal system in preventing cyber offenses before they escalate into more serious incidents. A shift toward a more preventive stance would require the development of strategies and tools that empower law enforcement to identify and mitigate potential threats before they materialize.

3.3 Practical Enforcement and Case Studies in Vietnam

3.3.1 Recent Prosecution Trends and Statistical Overview

According to Trinh (2024), Vietnam has witnessed a significant rise in cybercrime prosecutions, particularly targeting phishing attacks, online fraud, and breaches of government systems. In 2023 alone, nearly 14,000 cyberattacks were reported—a sharp and consistent upward trend, reflecting the evolving interplay of technological advancements, social dynamics, and increasingly sophisticated criminal tactics. This escalation highlights critical gaps in Vietnam's legal framework, including the need for clearer cybercrime categorization and a shift toward preventive rather than reactive countermeasures. Addressing these shortcomings would enable the government to allocate sufficient resources to combat cyber threats more effectively. Furthermore, enhancing public awareness of cybersecurity and cybercrime dynamics remains essential for building resilience against emerging digital threats.

3.3.2 Notable Cybercrime Cases in Vietnam

The first notable case is that of a cyberattack on Vietnam’s Aviation Systems in July 2016. Deutsche Welle. (2016, July) reported that Vietnam experienced a significant cyberattack that targeted its aviation systems, specifically the Vietnam Airlines website and the information systems of Tan Son Nhat International Airport. The hackers, allegedly linked to the Chinese group 1937CN, replaced screen displays with political messages related to territorial disputes in the South China Sea. This attack disrupted flight schedules, disseminated hostile propaganda, and raised alarms about the security of critical infrastructure in the country. This incident exposed the vulnerabilities of Vietnam’s digital landscape, particularly concerning essential services that rely on technology for their operations. Taking on a reactive countermeasure, Vietnam developed stronger cyber defense measures and policy adjustments to protect critical infrastructure, as observed in the amendments of the 2015 Penal Code and the establishment of the Cybersecurity Law in 2018.

The second notable case is that of a disinformation Campaign During the COVID-19 Pandemic. According to a report by UNESCO (2020), the COVID-19 pandemic presented a unique challenge for governments worldwide, and Vietnam was no exception. During this critical period, several individuals exploited social media platforms to spread disinformation regarding various aspects of the crisis, including death tolls, lockdown measures, and vaccine side effects. The government implemented strict regulations to combat disinformation, including Decree No. 15/2020/ND-CP, which imposed penalties for spreading false information online. Authorities also monitored digital spaces to prevent misleading narratives that could disrupt public health measures (Thiện, 2024).

Reports by the U.S. Department of State (2025) revealed that in 2021, Vietnam faced a serious cybercrime case involving the online distribution of terrorism-related materials. A group operating anonymously through encrypted messaging platforms disseminated bomb-making manuals and incited violence against

public officials. The materials, translated from foreign extremist sources, specifically targeted vulnerable youth in remote areas, raising concerns about online radicalization and recruitment into extremist ideologies. Authorities arrested the suspects and charged them under cybercrime and national security laws, reflecting the gravity of their actions. However, the prosecution encountered challenges in proving direct intent and establishing a clear link between online activities and real-world threats. This case underscored the complexities of prosecuting cybercrime, particularly when extremist content does not lead to immediate physical harm but poses a long-term threat to national security.

3.3.3 Challenges in detection and investigation

Despite Vietnam's strengthened legal actions, the country continues to face significant challenges in investigating and prosecuting cybercrimes. One of the primary obstacles is attribution, as identifying cybercriminals remains difficult due to anonymization tools and international data routing, which obscure the identities of perpetrators. Additionally, Deora & Chudasama (2021) note that the volatility of digital evidence, which can be quickly deleted, encrypted, or altered, makes timely seizure and preservation critical for successful prosecutions. However, such dynamics have exposed the vulnerabilities of the existing legal procedures in Vietnam, as reported by Nguyen et al. (2021).

A further complication is the lack of technical expertise among law enforcement and judicial officials. According to Van Nguyen et al. (2022), many personnel lack the advanced forensic skills necessary for investigating cybercrime, limiting the effectiveness of prosecutions. Moreover, jurisdictional conflicts arise in cross-border cases, where slow international cooperation, especially in the absence of mutual legal assistance treaties or membership in global frameworks like the Budapest Convention, hampers enforcement efforts. In response, Vietnam has implemented several initiatives to strengthen its cybersecurity capabilities. An article by Tilleke & Gibbins (2024) reveals that establishing the Cybersecurity and High-Tech Crime Prevention Department (A05) within the Ministry of Public Security marks an institutional effort to address cyber threats. Additionally, the government has promoted cyber literacy campaigns to enhance public awareness and improve online security. According to Interpol (2021), Vietnam has also engaged in regional and international cooperation, partnering with INTERPOL and ASEAN to bolster cyber defense strategies.

3.3.4 Legal and Practical Challenges in Enforcement

One of the significant challenges facing Vietnam's legal framework is the difficulty in defining what constitutes a “dangerous act” in cyberspace. While Articles 288 to 291 of the 2015 Penal Code provide some legal grounding, they primarily focus on the methods of committing these acts, such as illegal access or malware. This narrow focus overlooks the broader implications, such as the potential to incite mass panic or threaten national security. As a result, the ambiguity surrounding the definition of dangerous acts leads to inconsistent application of the law, making it challenging to distinguish between criminal offenses and violations of administrative or ethical norms in the online environment.

Another pressing issue is the limited forensic capabilities within Vietnam’s criminal justice system. Currently, Van Nguyen et al. (2022) reveal that the Vietnamese system relies heavily on confession-based procedures, which are often inadequate for addressing the complexities of digital crimes. According to Tran et al. (2025), effective cybercrime enforcement requires advanced forensic laboratories capable of analyzing digital devices, specialized training for cybercrime units, and tools to trace blockchain transactions and encrypted communications. Unfortunately, many local police units lack these essential resources, hindering their ability to combat cybercrime effectively. International cooperation presents yet another challenge. Vietnam's non-membership in the Budapest Convention restricts its full participation in global evidence-sharing and coordination frameworks. This limitation results in slow and complex mutual legal assistance requests, ultimately diminishing the effectiveness of cross-border investigations into cybercrime.

Moreover, approximately 50% of its population is active internet users (Internet World Stats, 2018), and Vietnam is already exposed to cybercriminals. Luong et al. (2019) refer to this kind of dynamic as a two-in-one phenomenon. First, there is a positive energy of embracing technology and applying it for economic revolution, and second, there’s an increasing risk of being harmed by this technology. As a result, taking a

reactive approach, despite having the Vietnamese government on the front line of the regulation of online platforms, such efforts have been proven futile. Although Vietnam has imposed obligations on global platforms like Facebook and YouTube under the Cybersecurity Law of 2018, observations from Nguyen (2024) reveal that enforcement remains weak. Harmful content often circulates for days or weeks before being removed, particularly when hosted on servers abroad. The lack of transparency in platform algorithms and delays in content moderation further complicate efforts to prevent or respond to coordinated online campaigns that involve dangerous or criminal messaging.

Lastly, there is a concerning overlap between cybercrime and national security laws. In some cases, cybercrime offenses may be prosecuted under broad national security provisions, such as "conducting propaganda against the State" or "abusing democratic freedoms." A study by Nguyen-Pochan (2021) showed that while the government has remained proactive in supporting technological advancements for economic gains, it has also viewed this as an avenue for political instability. As a result, efforts to address cybercrimes emanating from social media have been tackled politically and not using proper legislative instruments. While this approach allows for swift action, it raises significant concerns about the delicate balance between addressing criminality and protecting freedom of expression, especially when online activities involve political discourse or criticism.

4. Recommendations and Legal Direction

Vietnam must adopt a comprehensive legal reform strategy to combat cybercrime effectively. This involves clarifying legal definitions in the 2015 Penal Code, distinguishing between technical cybercrimes such as hacking and purpose-driven offenses such as cyberterrorism, and establishing harm thresholds to ensure proportionality in prosecution. Alternatively, Vietnam could have the Cybersecurity Law of 2018 clarify in-depth specifications on cybercrime to address the current prevailing ambiguity. To strengthen enforcement, Vietnam needs specialized laws on cyberterrorism, addressing threats such as attacks on infrastructure, digital incitement, and hybrid cyber-physical crimes.

Additionally, improving digital evidence handling is critical, modernizing forensic procedures, investing in cyberforensics labs, and creating a national digital evidence management system will enhance the integrity of investigations. Capacity building is another priority. Vietnam should introduce specialized training programs for law enforcement, judiciary officials, and cybersecurity professionals while fostering collaboration between government agencies and private sector firms. Expanding education in cyber law and digital investigation will also support long-term expertise. On the international front, Vietnam should ratify the Budapest Convention to facilitate cross-border cooperation in cybercrime cases. Strengthening bilateral and multilateral agreements within ASEAN and beyond will help Vietnam engage in real-time investigations and information sharing. Regulating social media platforms more effectively is also crucial, ensuring swift responses to government takedown requests and promoting content moderation that aligns with national laws. However, it is imperative for Vietnam to strike a balance between such regulatory measures and freedom of expression safeguards to prevent overreach. Finally, a national strategy on cyberethics and digital responsibility will help address the behavioral roots of cybercrime through public awareness campaigns, online radicalization prevention programs, and collaboration with educational institutions.

5. Conclusions

The illegal use of computer networks and telecommunications to commit dangerous acts poses a significant and complex challenge for Vietnam, especially as the country undergoes digital transformation and increasingly relies on online platforms. While Vietnam has made progress in recognizing and prosecuting cybercrimes, its current legal and institutional responses are fragmented and reactive. The existing legal frameworks, such as the Penal Code of 2015 amended in 2017 and the Cybersecurity Law of 2018, provide a foundation but lack the specificity and integration needed to tackle emerging threats like cyberterrorism and digital disinformation. Enforcement agencies face ongoing challenges in digital forensics, jurisdictional coordination, and evidence handling, which are compounded by the rapid pace of technological change and

the anonymous nature of the Internet. To create a safer digital environment, Vietnam must adopt a more proactive and collaborative legal model. This includes clarifying criminal definitions, enhancing institutional capabilities for digital investigations, aligning domestic laws with international standards, fostering a culture of digital awareness and ethics, and strengthening accountability for online platforms while safeguarding fundamental freedoms. As Vietnam becomes more interconnected, its legal system must effectively balance innovation with protection and freedom with security. Achieving this will require not only technical upgrades and legal reforms but also a fundamental shift in how cyber behavior is understood and governed. With a sustained commitment to these goals, Vietnam can develop a robust legal framework that protects its citizens from cyber threats and ensures that cyberspace serves as a catalyst for progress rather than a source of danger.

Author Statements:

Ethical approval: The conducted research is not related to either human or animal use.

Conflict of interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

Acknowledgement: The authors declare that they have no company or person to acknowledge.

Author contributions: The authors declare that they have equal rights to this paper.

Funding information: The authors declare that there is no funding to be acknowledged.

Data availability statement: The data supporting this study's findings are available on request from the corresponding author. However, due to privacy or ethical restrictions, the data are not publicly available.

References

1. Agzamovich, U. U., & Hikmatulla, N. (2021, November). Exchange of messages in the telecommunication network with different types of communication channels. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE. DOI: 10.1109/ICISCT52966.2021.9670173
2. Bone, J. (2024). Globalization, the ‘New’Labour Market, AI and the 4th Industrial Revolution. In The Great Decline (pp. 117-137). Bristol University Press.
3. Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2019). Phishing and cybercrime risks in a university student community. International Journal of Cybersecurity Intelligence & Cybercrime. 2(1), 4-23. https://www.doi.org/10.52306/02010219RZEX445
4. Bui, N. S., & Lee, J. A. (2022). Comparative cybersecurity law in socialist Asia. Vand. J. Transnat'l L., 55, 631.
5. Campina, A., & Rodrigues, C. (2022, January). Cybercrime and the council of europe Budapest convention: prevention, criminalization, and international cooperation. In Abstract Book-7th International Zeugma Conference on Scientific Researches (Vol. 1, No. 1, p. 381). IKSAD.
6. Deora, R. S., & Chudasama, D. (2021). Brief study of cybercrime on an internet. Journal of communication engineering & Systems, 11(1), 1-6. DOI: 10.37591/JoCE
7. Deutsche Welle. (2016, July). Hackers target Vietnam's airports. https://www.dw.com/en/hackers-target-flight-info-screens-at-vietnams-airports/a-19437977
8. Government of Vietnam. (2018). Cybersecurity Law (No. 24/2018/QH14). Hanoi: National Assembly of Vietnam.
9. Government of Vietnam. (1999). Penal Code (No. 15/1999/QH10). Hanoi: National Assembly of Vietnam.
10. Government of Vietnam. (2017). Penal Code (Amended) (No. 12/2017/QH14). Hanoi: National Assembly of Vietnam.
11. INTERPOL. (2021). ASEAN cyberthreat assessment 2021: Key cyberthreat trends outlook from the ASEAN Cybercrime Operations Desk. INTERPOL. https://www.interpol.int

12. Internet World Stats. (2018). World Internet Users and 2018 Population Stats. The Big Picture.

13. Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. Crime science, 7(1), 1-15. https://doi.org/10.1186/s40163-018-0079-3

14. Luong, H. T., Phan, H. D., Van Chu, D., Nguyen, V. Q., Le, K. T., & Hoang, L. T. (2019). Understanding Cybercrimes in Vietnam: From Leading-Point Provisions to Legislative System and Law Enforcement. International Journal of Cyber Criminology. 13(2).

15. Lusthaus, J. (2024). Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?. Annual Review of Law and Social Science. 20(1), 369-385. https://doi.org/10.1146/annurev-lawsocsci-041822-044042

16. Macdonald, M., & Frank, R. (2017). The network structure of malware development, deployment and distribution. Global Crime. 18(1), 49-69. https://doi.org/10.1080/17440572.2016.1227707

17. Madzhumayev, M. M. (2023, August). High-Tech Means and Implements of Crime: Challenging the Security of Sustainable Urban Development. In International Conference on Intelligent and Fuzzy Systems (pp. 780-787). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-39777-6_91

18. Nguyen-Pochan, T. T. P. (2021). State management of social media in Vietnam. The Russian Journal of Vietnamese Studies, 5(1S), 23-33. DOI : 10.54631/vs.2021.s-23-33

19. NGUYEN, Q. M. N. (2024). Legitimizing the Vietnam's Cybersecurity Law: Media Narratives and System Justification. Doctoral Thesis

20. Nguyen, D. P., Vo, X. V., Nguyen, V. C., Mai, X. D., & Duong, Q. K. (2021). Sustainable development for Vietnam's economy in the context of globalization and Industrial Revolution 4.0. Sustainability and Environmental Decision Making. 281-310. DOI https://doi.org/10.1007/978-981-15-9287-4_15

21. Nguyen, T., & Luong, H. T. (2020). The structure of cybercrime networks: transnational computer fraud in Vietnam. Journal of Crime and Justice, 44(4), 419–440. https://doi.org/10.1080/0735648X.2020.1818605

22. Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. Ieee Access. 9, 163965-163986. DOI: 10.1109/ACCESS.2021.3134076

23. Proulx, K. (2022). Anonymity Online and the Perfect Environment for Cybercrime (Master's thesis, Utica University).

24. Soullier, B. A. (2023). Decriminalizing Trivial Computer Use: The Need to Narrow the Computer Fraud and Abuse Act (CFAA) After Van Buren. Fed. Comm. LJ, 76, 239.

25. Standing Committee of the National People's Congress. (2016/2025). Cybersecurity Law (Amended) (PRC Cybersecurity Law, Draft Amendment 2025). Beijing: National People's Congress.

26. Thiện, H. (2024, May). Inside Vietnam's top-down disinformation campaign. Fair Planet. https://www.fairplanet.org/story/inside-vietnams-top-down-disinformation-campaign/

27. Tilleke & Gibbins. (2024, March). Vietnam to conduct first PDPD compliance investigation. https://www.tilleke.com/insights/vietnam-to-conduct-first-pdpd-compliance-investigation/

28. Tran, D. V., Nguyen, P. V., Le, L. P., & Nguyen, S. T. N. (2025). From awareness to behaviour: understanding cybersecurity compliance in Vietnam. International Journal of Organizational Analysis, 33(1), 209-229. https://www.emerald.com/insight/content/doi/10.1108/ijoa-12-2023-4147/full/html

29. Trinh, V. D. (2024). Vietnam's struggle with cyber security. EastAsiaForum. https://eastasiaforum.org/2024/03/20/vietnams-struggle-with-cyber-security/

30. UNESCO. (2020, April). In Viet Nam, UNESCO calls to end fake news and disinformation and highlights the importance of quality media coverage. https://www.unesco.org/en/articles/viet-nam-unesco-calls-end-fake-news-and-disinformation-and-highlights-importance-quality-media

31. United States Congress. (1986, last amended in 2018). Computer Fraud and Abuse Act (18 U.S.C. § 1030). Washington, DC: U.S. Government Publishing Office.

32. U.S. Department of State. (2025, January). 2021 Country Reports on Human Rights Practices: Vietnam. https://2021-2025.state.gov/reports/2021-country-reports-on-human-rights-practices/vietnam/

33. Van Nguyen, T. (2022). The modus operandi of transnational computer fraud: a crime script analysis in Vietnam. Trends in Organized Crime. 25(2), 226-247. https://doi.org/10.1007/s12117-021-09422-1

34. Van Nguyen, T., Truong, T. V., & Lai, C. K. (2022). Legal challenges to combating cybercrime: An approach from Vietnam. Crime, Law and Social Change, 77(3), 231-252.

35. Wan, H., Liu, G., & Zhang, L. (2021, October). Research on the application of artificial intelligence in computer network technology. In Proceedings of the 2021 5th International Conference on Electronic Information Technology and Computer Engineering (pp. 704-707). https://doi.org/10.1145/3501409.3501536