JURNAL CITA HUKUM (Indonesian Law Journal)
FSH UIN Syarif Hidayatullah Jakarta
Vol.13 No. 1 (2025), pp. 73-94, DOI: 10.15408/jch.v13i1.44612

Analysis and Recommendations for the Vietnam's Legal Framework on Cybercrime*

Nguyen Van Khoat[1]
[1]Hanoi Procuratorate University, Vietnam
10.15408/jch.v13i1.44612

Abstract
Cybercrime has emerged as a complex global threat that continuously evolves, posing challenges not only to states and law enforcement but also legal experts, computer professionals, and researchers. Despite its growing significance, there is no universally accepted definition of cybercrime, further complicating legislative and enforcement efforts. Vietnam, with one of the highest internet penetration rates in the world—over 80% of its population or approximately 80 million users, is particularly vulnerable to cybercrime. Recognising this risk, Vietnam enacted the Cybersecurity Law in 2018 and addressed cybercrime provisions in the amended Criminal Code of 2015 (revised in 2017). This article aims to analyse the effectiveness of Vietnam's legal framework on cybercrime and offer constructive recommendations for improvement. Utilising a qualitative research method through a literature-based and legal approach, the study conducts comparative legal analysis by examining relevant regulations and policies in Vietnam, Singapore, and the United States. The research reveals that although Vietnam has made significant strides in legislating cyber-related issues, its Cybersecurity Law 2018 places disproportionate emphasis on state control and lacks provisions that adequately protect individual rights or facilitate inter-agency cooperation. In contrast, countries like the U.S. emphasise robust information-sharing mechanisms among cybercrime investigation bodies, which enhances enforcement efficiency. The article concludes that Vietnam's legal framework would benefit from reforms that better balance national security and individual freedoms while fostering inter-agency collaboration and alignment with international best practices in cybersecurity governance.
Keywords: Cybersecurity Law; Vietnam; Cybercrime in Vietnam; Cybersecurity Law Singapore; Comparative Law

* Received: January 17, 2025; revised: February 22, 2025; accepted: March 15, 2025; published March 31, 2025.
[1] **Nguyen Van Khoat.** Faculty of Criminal Law and Criminal Prosecution, Hanoi Procuratorate University, Vietnam. Email: nguyenvankhoat@tks.edu.vn ORCID: https://orcid.org/0009-0007-6594-8942
**Corresponding author: nguyenvankhoat@tks.edu.vn

A. INTRODUCTION

Cybercrime is yet to be fully understood by researchers and law enforcement. UK government official data states that many victims of cybercrime do not report the incidents because they feel that the police are ill-equipped to deal with the crimes (Curtis & Oxburgh, 2023). Cybercrime has continued to cause unparalleled devastation to government agencies, economies, and individuals globally. According to Morgan (2024), cybercrime was projected to inflict damages totalling USD 9.5 trillion in 2024. To understand the magnitude of this estimated mind-boggling loss, if cybercrime were a country, it would be the third-largest economy globally, hot on the heels of the U.S. and China. According to Cybersecurity Ventures, these losses will rise to USD 10.5 trillion in 2025. Notably, global cybercrime losses were USD 3 trillion in 2015. To put these facts further in context, an analysis of 553 data breaches in 2023 targeting large organisations in 16 countries showed an average loss of USD 4.45 million per breach. The cost per breach rose 2.3% from USD 4.35 million in 2022 to 15.3% from USD 3.86 million in 2020. However, underreporting of cybercrime persists, with only 25% of cybercrime incidents reported to law enforcement globally. Further, according to the World Cybercrime Index published in 2024, the leading sources of cybercrime incidents in descending order were Russia, Ukraine, China, the U.S., Nigeria, and Romania. (Morgan, 2024)

Sweden was the first country globally to pass a data protection law -the "Swedish Data Act of 1973" to protect data from unauthorised access. The passing of the "Federal Computer Systems Protection Act of 1977" made the US the second country to pass a cybercrime law globally. The word cybercrime was coined in 1995 by Sussman and Heuston. Cybercrime is a broad phenomenon that involves illegal actions *"where a digital device or information system is either a tool or target or simply a combination of both"* (Sabillon et al., 2016). Murphy (2024) contends that there is no universally accepted definition of cybercrime. However, it can be understood as a crime involving the use of information technology to commit or aid in committing a crime. Cybercrimes fall under two broad categories: (i) Cyber-dependent crime- They target ICT systems such as computers and computer networks. They mainly use malware and hacking. (ii) Cyber-enabled crimes- everyday crimes that the use of information technology has scaled up. Cybercrimes are lucrative crimes, with the perpetrators making billions of euros annually. The nature of cybercrimes keeps evolving in scale, sophistication, and creativity. These crimes are perpetrated at all levels of society, and they can take any form, such as "investment fraud, phishing, identity theft, fake charities, etc. There are other prevalent crimes, such as cyberbullying, cyberstalking, harassment, and online grooming, among others (Murphy, 2024).

Cybercrime is a global menace that is leading to many losses. Chen et.al. (2023) note that cybercrimes are a global threat to the economy, security, stability, and individual interests. Citing Ghafur et.al. (2019) and Chen et al. (2023), they give an example of the WannaCry ransomware attack 2017. The WannaCry ransomware attack harmed over 230,000 computers in over 150 countries, leading to approximately 4 billion USD in losses. According to Cloudflare (2024), the WannaCry ransomware attack occurred on 12th May 2017, spreading to more than 200,000 computers daily. Major companies such as FedEx, Honda, Nissan, and the UK's National Health Service (NHS) were affected. *"Ransomware is malicious software that locks up files and data via encryption and holds them for ransom."* In the case of the NHS, the attack had life-threatening consequences for some patients, and they had to divert some of their ambulances to private hospitals (Cloudflare, 2024). Chen et al. (2023) also established that most cybercrime-related IPS were in North America and Europe. They also noted that high-income regions had more cybercrime incidents than low-income regions.

The Convention on Cybercrime (ETS No.185) is the first international treaty on cybercrimes. It was opened for signatures on 23/11/2001 in Budapest, Hungary. According to EUR-Lex (2023), the Convention deals with "crimes that can only be committed through the use of technology, where the devices are both the tool for committing the crime and the target of the crime, and crimes where technology has been used to enhance another crime, such as fraud." The Convention entered into force on 1 July 2004.

The Council of Europe member states noted in the preamble (among other things) of the Convention cybercrime a need to protect society from cybercrime, computer networks, and electronic data may be used for criminal purposes, the need for states and the private sector to work together in combating cybercrime and, an effective fight against cybercrime required international cooperation. The Convention on Cybercrime ETS No. 185 identified "Offences against the confidentiality, integrity, and availability of Computer data and systems in Chapter II (Article 2-8). Chapter II (Articles 2-8) deals with legislation that member states have to pass in their countries against cybercrime, and they include Illegal access- Article 2; Illegal interception- Article 3; Data interference- Article 4; System interference- Article 5, Misuse of devices- Article 6; Computer-related forgery- Article 7; Computer-related fraud- Article 8. In addition, there are offences related to child pornography - Article 9, copyright infringement and related rights- Article 10, Attempt and aiding and abetting- Article 11.

The Council of Europe Member states agreed on the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a

racist and xenophobic nature committed through computer systems- ETS No. 189. They opened it for signatures on 28th January 2003 at Strasbourg, France. This additional protocol recognised that computer systems were being used for racist and xenophobic-related crimes and came into force on 1st January 2006. On 12th May 2022, the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No. 224) was opened for signatures. The second additional protocol was based on the nature of cybercrimes, where electronic evidence could be stored in "foreign, multiple or unknown jurisdictions."

The Second Additional Protocol to the Convention on Cybercrime (ETS No. 185) formed a legal basis for disclosure of domain name registration information and direct co-operation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal data protection safeguards. (Council of Europe, 2022)

The United Nations General Assembly Committee agreed on a draft "United Nations Convention against Cybercrime" (document A/78/96 that will be opened for signatures in Hanoi in 2025 and later at the UN Headquarters until 31 December 2026 (United Nations, 2024a). The draft document resulted from three years of negotiations by the Committee established by the UN General Assembly to work on the Convention on Cybercrime. The draft of the cybercrime convention resulted from five years of work by UN member states, civil society, the private sector, and academic institutions (United Nations, 2024b). The primary purpose of the Draft United Nations Convention against cybercrime is "*Strengthening international cooperation for combating certain crimes committed using information and communications technology systems and for the sharing of evidence in electronic form of serious crimes".* (United Nations, 2024c)

The Draft United Nations Convention Against Cybercrime- A/AC.291/L.15 (2024) has noted in the preamble that despite information and communications technologies presenting massive potential for development, they pose novel risks and opportunities for cybercriminals that may have adverse effects on states, enterprises and the well-being of individuals and societies. The Convention has also stressed the need for states to cooperate in all relevant ways to combat cybercrime; has acknowledged the ever-increasing cybercrime incidents; sought to prevent, detect, and suppress cybercrime, etc. In Chapter I (General provisions), Article 1 contains the convention's statement of purpose.

Article 1:

(a) Promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively;

(b) Promote, facilitate, and strengthen international cooperation in preventing and combating cybercrime.

(c) Promote, facilitate, and support technical assistance and capacity-building to prevent and combat cybercrime, particularly for the benefit of developing countries.

Gojali (2023) notes that cybercrime has increased in Indonesia's corporate sector. Government data revealed that in 2019, Indonesia recorded 290 million cyberattack incidents and losses of more than 34.2 billion U.S. dollars. Indonesia has legislated on cybercrime in response to the rise in the vice. Cyber warfare and espionage are significant threats to Indonesia's institutions and organisations. The primary law on cybersecurity in Indonesia is the Electronic Information and Transactions (ITE) Law, which is used alongside the Indonesian Criminal Code.

B. METHODS

This article is grounded in a comprehensive analysis of secondary data collected through a library research approach. Recognising cybercrime's dynamic and rapidly evolving nature, the author aimed to develop an insightful and up-to-date discussion by relying on the most recent and relevant data. To support the research, the author carefully examined various credible sources, including peer-reviewed journal articles, annual cybercrime threat reports, government publications, institutional press releases, and expert analyses from cybersecurity organizations. This broad and diverse range of literature provided a rich foundation for understanding the multifaceted nature of cyber threats in both national and global contexts. Additionally, the author adopted a comparative study methodology, focusing specifically on the cybersecurity environments of Vietnam, Singapore, and the United States. This approach allowed for an in-depth examination of the similarities and differences in legal frameworks, policy responses, and strategic priorities across these countries, offering a more nuanced understanding of best practices in combating cybercrime.

C. RESULTS AND DISCUSSION

1. Cybercrime in Vietnam: Challenges and International Legal Comparisons

In recent years, Vietnam has emerged as a rapidly digitizing economy driven by technological advancements and widespread internet adoption. However, this progress has increased cybercrime, presenting significant challenges to law enforcement, businesses, and policymakers. Cybercriminal activities range from financial fraud and data breaches to the proliferation of malware and hacking campaigns. The rise of cybercrime in Vietnam underscores the urgent need for robust legislative measures and international cooperation.

Vietnam ranks among the most internet-connected nations in Southeast Asia, with over 70% of its population online. While enabling economic growth, this connectivity has made the country a target of cyberattacks. The Vietnam Information Security Association (VNISA) reported a sharp increase in cyber incidents in recent years, with financial institutions, e-commerce platforms, and government systems being the primary targets.

Typical forms of cybercrime in Vietnam include:

1. **Phishing Attacks**: Scams that steal personal and financial information via fake websites and emails.
2. **Data Breaches**: Compromising sensitive data, often sold on the dark web.
3. **Ransomware**: Malicious software used to extort money by encrypting victims' data.
4. **Online Fraud**: Includes fake online marketplaces and fraudulent investment schemes.

Online scams are increasing in scale and severity with technological advances globally. Vietnam is no exception to this worrying trend. Vietnam's deputy director of the Cybersecurity and High-Tech Crime Prevention Department, Major General Nguyễn Văn Giang, noted that online scammers keep coming up with novel ways to scam people. Their Modus Operandi includes fake job advertisements, phishing emails, brand counterfeiting, account hijacking, love scams, and online lending, among others, aimed at defrauding their victims of their money. In 2023, Vietnamese citizens lost to online scams rose by 50% compared to 2022, when the total was startling VND10 trillion (USD 394 million). Online scammers have also been using fake websites and phishing emails to steal sensitive personal information from their hapless victims. In this regard, Vietnam is engaging multinational platforms such as Google and

Facebook to revamp its policies on personal data protection to curb further data losses. (Viet Nam News, 2024)

Luong and Ngo (2024) state that there is a rise in pig-butchering scams in Southeast Asia due to the high use of digital technology and online financial transactions. Pig-butchering scams are cryptocurrency investment scams, so named after the process of fattening pigs before they are butchered. In these scams, unwary victims are lured into investing their money in seemingly legitimate high-yield investments. The scammers promise fraudulent high returns within a short period. Once the unsuspecting victims are hooked, the scammers disappear without a trace, leaving them high and dry. In 2022, pig-butchering scams caused an estimated USD 2.57 billion loss. (Trend Research, 2024)

Online scammers perhaps find Vietnam lucrative because of the high internet penetration. Luong and Ngo (2024), citing Nguyen (2024b) and Nguyen (2024a), note that the internet was formally launched in Vietnam in 1997, and by 2023, about 80 million (80%) Vietnamese were using the internet. Also, Vietnam had a 30 billion USD internet-based economy, the largest in South Asia. Further, Luong and Ngo (2024), citing the Global Anti-Scam Alliance (GASA 2024), reported that Vietnam recorded the second-highest scams globally in 2023; the worst-hit country was Kenya. In 2023, Vietnam lost 3.6% of its GDP to fraudsters, about VND 391.8 trillion (about USD 16.23 million). In a study on the prevalence of scams in Vietnam, Luong and Ngo (2024) reported that Text/SMS messages and phone calls were used mainly for the scams, accounting for 57% and 80%, respectively. The survey established that 70% of the respondents encountered scam attempts at least once a month. In addition, scammers prefer Facebook and Gmail as the most popular online platforms. 71% of the respondents reported having experienced scam attempts on these platforms. The other platforms used by online scammers in Vietnam were Telegram (28%), Google (13%), and TikTok (13%). The study also reported that investment scams (pig-butchering) were the highest scams. (Luong & Ngo, 2024)

One of the significant problems related to cybercrimes is cyberattacks. Trinh (2024) notes that Vietnam has the 12th-largest internet user population globally. However, since 2011, Vietnam has been facing a series of cyberattacks, mainly from Chinese hackers. For example, a Vietnamese hydrographic research vessel's cable system was damaged by Chinese vessels, triggering cyberspace warfare between Chinese and Vietnamese hackers. In 2023, there were 13,900 reported cyber-attack incidents in Vietnam. According to the Vietnam National Cyber Security Technology Company, in 2023, cyberattacks increased by 9.5%

compared to 2022. According to Asia Business Law Journal (2024), continuous cyber-attack incidents have prompted Vietnam's Prime Minister to issue a directive to the relevant government agencies to review Vietnam's cybersecurity. Vietnam has 72 million internet users, yet many are ignorant of cybersecurity concerns. Also, there is a gap in the coordination between government agencies and the private sector. Since March 2024, Ransomware attacks have been reported in major enterprises, including "financial advisory company VnDirect, fuel service station chain PVOil and a telecommunications service provider." Also, in Vietnam, phishing, scam calls, and data breaches are a concern. According to Bkav Corporation (a cybersecurity software company), an assessment conducted in December 2023, computer viruses caused losses of approximately VND 17.3 trillion (USD 716 million) to Vietnamese users in 2023. (Asia Business Law Journal, 2024)

Singapore has its share of cybercrimes and cyberattacks, too. Khan (2024) states that cybercrime accounted for 70% of reported crime incidents in Singapore in 2023. Romero (2024) reports that the Singapore Cybersecurity Agency (CSA) has recorded increased cybercrimes such as phishing, ransomware, and scams. Data reveals that phishing, employment, and e-commerce-related fraud are the most frequent. Online fraudsters frequently use messaging and social media platforms like Telegram, Instagram, and Facebook. In 2022, Singapore recorded losses amounting to 21.3 million Singapore dollars through e-commerce fraud. Khan (2024), in underscoring the ever-growing threat of cybercrimes in Singapore, quotes Singapore Police Force (SPF) data. SPF data shows that 2011 cybercrimes were not considered a significant threat and were not categorised as standalone crimes. Instead, cybercrimes were lumped together with commercial crimes and accounted for a paltry 12.1% of the crimes. However, fast forward to 2021, the cybercrime landscape has changed entirely, and cybercrime accounted for 50% of the crimes reported in Singapore annually.

Singapore Police Force (2024). Mid-Year Scams and Cybercrime Brief 2024 reported an increase in cybercrimes compared to 2024. From January to June 2024, the number of scams and cybercrime incidents increased by 18.0% to 28,751 incidents compared to 24,367 incidents within the same period in 2023. Further, the Singapore police data showed that 92.5% of the 28,751 incidents were scams. Scams rose by 16.3% to 26,587 incidents in the first half of 2024, compared to 22,853 incidents in the same period in 2023. Regarding financial loss, a minimum of $385.6 million was lost in the first half of 2024 compared to $309.4 million in the first half of 2023. A further analysis of the reported incidents by the Singapore Police Force showed that, on average, an estimated $14,503 was lost per scam between January and June 2024, which is a 7.1% increase compared to an average

of $13,541 lost per scam in the same period in 2024. However, it should be noted that in the first six months of 2024, 59.8% of scams resulted in losses less than or equal to $2,000. In 86% of these scams, the perpetrators did not gain direct control of their Victims' accounts. Instead, through various complex scam methods and social engineering, the victims were duped into effecting monetary transfers to the scammer's accounts.

Singapore Police Force reports 3,447 phishing scams in Singapore between January and June 2024, causing losses of an estimated $13.3 million. The scams were perpetrated using emails, text messages, calls, or advertisements. During the period under review, 44.4% of the phishing scam victims were aged between 30 and 49. Singapore's popular online marketplace, Corousell, Facebook, and SMS are the most used avenues for contacting scam targets.

Investment scams (Pig-fattening) were also recorded in Singapore between January and June 2024. Three thousand three hundred thirty investment fraud cases were reported, causing an estimated $133.4 million in losses. Investment fraud perpetrators enticed their unwary targets into making investments in 'easy high-profit investments.' Targets were approached through online friends, internet searches, and even unsolicited messages from scammers. In some cases, they receive initial 'small profits' from their investments, which entices them to invest larger amounts of money only to realise, after a while, that they cannot withdraw either their 'investment capital or their profits.' 44.7% of the victims of this scam were between 30 and 49 years old, and they were contacted mainly through Facebook, WhatsApp, and Telegram.

The Singapore Police Force Mid-Year Scams Brief 2024 also states that Singapore has been working with Foreign Law enforcement agencies such as the Royal Malaysia Police and INTERPOL because of the transnational nature of cybercrime. As a result of this cooperation, in the first half of 2024, we took down nine transnational scam cells, three fake friend call syndicates, four money laundering syndicates, one phishing syndicate, and one investment scam syndicate. In this operation, more than 100 people based outside Singapore, involved in more than 320 fraud incidents, were arrested.

According to the U.S. Government Accountability Office (GAO) (2023a), Cybercrimes are criminal activities targeting computers or computer networks to collect data or steal information. Also, cybercrime includes the use of computers for criminal activities. It is challenging to investigate cybercrimes because the internet allows anonymity of the perpetrators, the perpetrators can operate remotely, and technology makes it possible to commit international crimes. This then calls for cooperation with other states and international agencies in

cybercrime. Cybercrimes have led to the loss of Billions of dollars in the U.S. and threaten public safety and economic security. GAO (2023b) notes that there is no consistent definition for cybercrime in the U.S., and hacking and ransomware attacks have led to the loss of billions of dollars. In the U.S., 12 agencies investigate cybercrime. According to Petrosyan (2024), more than 880,000 cybercrime incidents were reported in the U.S. in 2023. The reported incidents involved phishing, spoofing, and personal data breaches. By 2023, more than 605 per cent of Americans had encountered credit card fraud. In the U.S., the 2013-2014 Yahoo data breach was the worst reported incident in the U.S. It remains the worst reported data breach in global history.

The U.S. Federal Bureau of Investigation (2023, pp. 7- 8) reported that its Internet Crime Complaint Centre (IC3) has received 758,000 complaints annually for the past five years. Between 2019 and 2023, IC3 has received 3.79 million complaints, leading to USD37.4 billion losses. In 2019, there were 467,361 complaints and USD 3.5 billion in losses; in 2020, there were 791,790 complaints and USD 4.2 billion in losses; in 2021, there were 847,376 complaints and USD.6.9 billion in losses; in 2022, 800,944 complaints and USD 10.3 billion in losses; and in 2023, there were 880,418 complaints and USD 12.5 billion in losses. Within the same period, the top cybercrime incidents were Tech Support, Extortion, Non-payment/ Non-delivery, Personal Data Breach, and phishing. Further, the Federal Bureau of Investigation (2023, p. 11) reported that 2023 the IC3 recorded 21,489 Business Email Compromise (BEC) incident reports, leading to USD 2.9 billion Losses.

BEC is a sophisticated scam targeting both businesses and individuals who transfer funds. It is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorised fund transfers.

There was a spike in Investment fraud (pig-fattening) in 2023, and the IC3 reported that investment scams were the most frequent incidents. Victims are lured into fraudulent investment schemes promising quick, high returns. In 2022, investment fraud led to USD 3.31 billion losses. In 2023, the losses from investment fraud rose by 38% to USD 4.57 billion. Cryptocurrency-related investment fraud has been increasing notably in the U.S. In 2022, cryptocurrency-related investment fraud led to losses of USD 2.57 billion. In 2023, cryptocurrency-related investment fraud increased by 53%, resulting in USD 3.96 billion in losses.

Ransomware attack complaints in 2023, according to IC3, were 2,825, culminating in USD 59.6 million losses. Ransomware is a type of malicious

software, or malware, that encrypts data on a computer, making it unusable. In addition to encrypting the network, the cyber-criminal will often steal data off the system and hold that data hostage until the ransom is paid. If the ransom is not paid, the entity's data remains unavailable. (Federal Bureau of Investigation, 2023, p.13)

Within the same period, there were 1,193 ransomware attacks targeting Critical Infrastructure sectors. According to IC3, of the 16 Critical Infrastructure Sectors in the US, 14 experienced ransomware attacks, and at least one member fell victim to the attack. The primary ransomware variants USD in the 2023 attacks against Critical Infrastructure were Lockbit, ALPHV/Blackcat, Akira, Royal, and Black Basta.

2. Vietnam's Legal Framework on Cybercrime Compared to Singapore and the U.S.

Vietnam's primary legal response to cybercrime is the **Law on Cybersecurity**, enacted in 2018. It mandates strict regulations on data storage and requires foreign companies operating in Vietnam to localise their data. Additionally, the **Penal Code of 2015 (amended in 2017)** criminalises various forms of cyber offences, including illegal data access and distribution of malware.

Regarding the prevention and combating cyberattacks, the Vietnam Law on Cybersecurity 2018 Article 19 states that (1) Acts comprising cyberattacks (a)

Article 19. Prevention of and combating cyberattacks
1. Acts constituting a cyberattack and cyberattack-related acts comprise:

(a) Distributing informatics programs that cause harm to a telecom network, the Internet, a computer network, an information system, an information processing and control system, a database or a facility;

(b) Hindering, disordering, paralysing, interrupting or stopping the operation of, and/or illegally preventing the transmission of data by a telecom network, the Internet, a computer network, information system, information processing and control system, database or e-facility;

(c) Infiltrating, harming or appropriating data stored or transmitted on a telecom network, the Internet, a computer network, information systems, information processing and control systems, a database or an e-facility;

(d) Infiltrating, creating or exploiting security vulnerabilities or weaknesses and system services in order to appropriate information and/or to earn illicit profit;

(e) Producing, purchasing and selling, exchanging or donating tools, devices [equipment] and software with the function of attacking a telecom network, the Internet, a computer network, information system, information processing and control system, database or e-facility in order to use such objects [tools, devices and software] for illegal purposes;

(f) Performing other acts that affect the regular operation of any telecom network, the Internet, computer network, information system, information processing and control system, database, or e-facility.

The Criminal Code of Vietnam N0.11/2015/Q13 of November 27, 2015 (amended 2017) deals with spreading software programs harmful to computer networks, telecommunications networks, or electronic devices in Article 286. Article 286 (1) Deliberately spreading malicious software program to harm computer networks, telecommunication networks, or electronic devices attracts a VND 50,000 to a maximum of VND 200,000,000 or 03 years community sentence of 6-36 months custodial sentence if this type of crime results to (a) The perpetrator making an illegal profit between VND 50,000,000- VND 200,000,000; (b) Damage to property worth between VND 50,000,000 to 300,000,000; (c) If the malware infected between 50-199 electronic devices or harmed a network with 50-19 users; (d) The offender had incurred civil liability previously or has a record for a crime of the exact nature that has not been expunged.

Article 286 (2) stipulates offences that carry a VND 200,000,000 to VND 500,000,000- or 03-07-year jail term. The offences include (a) offences committed by an organised group; (b) The proceeds of the crime are between 200,000,000 and 500,000,000; (c) the crime results in damage of property between VND 300,000,000 and VND 1,000,000,000; (d)The malware infects between 200 and 499 electronic devices or a network of 200-499 user; (dd) The offence entails dangerous recidivism. Article 286 (3) has stipulated a 07 to 12 years jail sentence without the option of a fine for the following offences: (a) a crime against any system containing classified data or a system used for national defence and security; (b) Crimes that target national information infrastructure; national grid control information system; banking or finance information system; traffic control information system; (c)The proceeds of the crime are or surpass VND 500,000,000; (d) The crime results in damage to property of or more than VND 1,000,000,000.

The malware infects 500 or more electronic devices or harms a network of 500 or more users. Article 286 (4) provides that the perpetrator of the crimes outlined in Article 286 (1)-(3) might be fined VND 30,000,000 to 200,000,000 or forbidden from holding specific jobs for 01-05 years. While the cybersecurity law has strengthened the legal framework, critics argue it prioritises state control over individual privacy and is only marginally aligned with global best practices. Furthermore, enforcement challenges persist due to limited technical expertise and insufficient resources in law enforcement agencies. Singapore offers a helpful comparison as a regional neighbour. The Cybersecurity Act (2018) includes detailed provisions for protecting critical information infrastructure and incident reporting obligations. Singapore's framework promotes public-private partnerships and international cooperation, leading Southeast Asia's fight against cybercrime.

According to Khan (2024), Singapore's Ministry of Home Affairs has two approaches to cybercrimes: (i) Traditional crimes that existed before the age of computers or can be committed without computers. Criminals have leveraged the existence of computer technology to exploit new frontiers for their criminal acts. (ii) Crimes that depend on computers and can exist without computers, such as denial of service attacks. Singapore Cybersecurity Act 2018 provides for the designation of a computer or computer system as critical infrastructure. In the designation of a computer or computer system as critical infrastructure, Singapore's Cybersecurity Act 2018 states in Section 7(1)

The Commissioner may, by written notice to the owner of a computer or computer system, designate the computer or computer system as a critical information infrastructure for the purposes of this Act, if the Commissioner is satisfied that:

(a) The computer or computer system is necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore; and

(b) The computer or computer system is wholly or partly in Singapore.

In ensuring cybersecurity, owners of critical information infrastructure must report all cybersecurity incidents to the Commissioner in the prescribed form and manner - Section 14(1). Section 14 (1) requires the cybersecurity incident to be reported (a) the specific incident regarding the critical infrastructure; (b) the cybersecurity incident about any computer or computers under the owner's control that/are connected to or communicate with the critical infrastructure.

Section 14(2) requires owners of critical information infrastructure to establish mechanisms for detecting cybersecurity threats to critical infrastructure in compliance with the code of practice. Section 14(3) If the owner of a critical infrastructure, without a reasonable explanation or excuse, contravenes Section 14(1) stipulations, is liable to a fine not exceeding $100,000 or a prison term of not more than two years or both.

Singapore's Computer Misuse Act 1993 (2020 Revised edition) is detailed in its approach to cybercrimes and the corresponding penalties. In Part 2, Section 3, regarding unauthorised access to computer materials, Subsection 1 has proscribed unauthorised access to a computer and its data. For this crime, the penalties are 3(a) a fine of not more than $5,000 or a two-year imprisonment or both. 3(b) for repeat offenders, a fine not exceeding $10,000 or imprisonment for a period not exceeding three years or both.

Subsection 2 stipulates that if damage occurs as a result of the crime in section 3, then if the perpetrator is found guilty, they may be fined not more than $50,00 or imprisoned for not more than seven years or both.

Section 4 of Singapore's Computer Misuse Act 1993 (2020 Revised edition) deals with Access with intent to commit or facilitate the commission of an offence. Section 4 Subsection 1 deals with accessing a computer to procure a programme or data in the computer with criminal intent. 4(2) Crimes related to property, fraud, dishonesty, or leading to physical harm attract a prison term of not less than 2 years. 4(3) Anyone found guilty of an offence under Section 4 of the Act shall be fined no more than $50,000 or imprisoned for 10 years or both.

Section 5 has focused on the unauthorized modification of computer material. 5(1) prohibits intentionally performing actions that would cause unauthorized modification of a computer's contents. 5(1)(a) First-time offenders, if found guilty, shall be fined not more than $10,000 or imprisoned for not more than 3 years or both. 5(1)(b) Repeat offenders shall not be fined more than $20,000 or imprisoned for not more than 7 years or both. Section 5 (2) If the offences committed under this section cause damage, the guilty person shall be fined not more than $50,000 or imprisoned for not more than 7 years or both.

Section 6 is about the unauthorized use or interception of computer services. Section 6 (1) (a)Unauthorized access of a computer to directly or indirectly secure any computer service; 6(1)(b) Unauthorized interception of a computer function using electromagnetic, acoustic, mechanical, or other device; 6(2)(c) Anyone who or commits or makes crimes in either (a) or (b) or both to be committed shall be 6(1)(d) fined not more than $10,000 or imprisoned for not

more than three years or both; 6(2)(e) For repeat offenders they shall be fined not more than $20,000 or imprisoned for not more than 5 years or both. Section 6(2) For damages arising from crimes under this section, the guilty person shall be fined not more than $50,000 or imprisoned for not more than 7 years or both.

Section 7 focuses on unauthorised obstruction of the use of a computer. Section 7(1) intentional unauthorized or lawful (a) interference, interruption or obstruction of a computer from being used (b)impediment or prevention of access, or affects the usefulness or performance of any data stored in a computer negatively or a computer programme is proscribed. For such offences, Section 7(1)(c) For first offenders, the guilty person shall be fined not more than 10,000 or imprisoned for not more than 3 years or both; 7(1)(d) For repeat offenders, they shall be fined not more than $20,000 or imprisoned for not more than 5 years both. Section 7(2) For any damage occurring due to offences under this section, the offender shall be fined not more than $50,000 or imprisoned for not more than 7 years or both.

United States Code Title 18, Section 1030, the Computer Fraud and Abuse Act (CFAA), was enacted in 1986 as an amendment to the first federal computer fraud law. The Act has been reviewed progressively in response to the ever-changing computer crime landscape. CFAA has proscribed "intentionally accessing a computer without authorisation or accessing beyond the authorised limit." However, it has fallen short of defining what "without authorisation" means (NACDL, nd). According to the U.S. Department of Justice, Justice Manual 18 U.S.C. §§ 1030(a)(1), (a)(2), (a)(3), (a)(4), and (a)(5)(B)-(C) a defendant will be charged with the offence of "without authorisation" if the defendant at the time of accessing the computer.

(1) the defendant was not authorised to access the protected computer under any circumstances by any person or entity with the authority to grant such authorisation; (2) the defendant knew of the facts that made the defendant's access without authorisation; and (3) prosecution would serve the Department's goals for CFAA enforcement. Further, the U.S. Department of Justice, Justice Manual, three paragraphs of section 1030- 18 U.S.C. §§ 1030(a)(1), (a)(2), and (a)(4). deal with 'exceeding authorised access'. The department will charge defendants with this crime if, at the time of the defendant's actions.

(1) a protected computer is divided into areas, such as files, folders, user accounts, or databases; (2) that division is established in a computational sense, that is, through computer code or configuration, rather than through contracts, terms of service agreements, or employee policies; (3) a defendant is authorised to access some areas, but unconditionally prohibited from accessing other areas

of the computer; (4) the defendant accessed an area of the computer to which his authorised access did not extend; (5) the defendant knew of the facts that made his access unauthorised; and (6) prosecution would serve the Department's goals for CFAA enforcement.

Regarding whether prosecution would serve the Department's Goals for CFAA enforcement, the U.S. Department of Justice's position is informed by the primary goal of the CFAA, that is *"upholding the legal right of individuals, network owners, operators, and other persons to ensure the confidentiality, integrity, and availability of information stored in their information systems."*

The U.S. also deals with cybercrime through the Cybersecurity Information Sharing Act (CISA) enacted in 2015. According to Hanna (2024), the Cybersecurity Information Sharing Act (CISA) allows U.S. and non-governmental agencies to share information when investigating cyberattacks. For agencies not part of the government, sharing information is voluntary. However, some of the U.S. government regulations hamper the sharing of information between agencies. A case in point is where a hospital in the U.S. is attacked; the hospital administrators could be barred from sharing information with government investigative agencies because of the privacy regulations in the Health Insurance Portability and Accountability Act (HIPAA). Further, updates have been made to CISA to ease information sharing while maintaining Confidentiality. The revamped regulations require the Director of National Intelligence and the federal departments of Homeland Security, Defence, and Justice to collaborate in formulating procedures for sharing information on cybersecurity threats.

Vietnam's Cybersecurity law has addressed the challenge of cyberattacks in Article 19. Cyberattacks such as ransomware are a global problem and keep increasing in scope and devastation. A significant weakness noted in Vietnam's Law on Cybersecurity is its focus on the state, overlooking the obvious threats that cybercrimes pose to non-government agencies, citizens, and privately owned businesses. The law should borrow a leaf from Singapore's Computer Misuse Act 1993 (2020 revised edition). Singapore's Computer Misuse Act 1993 (2020 revised edition) details cybercrimes and the associated penalties. The law can be said to be dynamic in its approach to computer-related crimes.

In Vietnam, Penalties for Cyberattacks have been stipulated in the Criminal Code of Vietnam No.11/2015/Q13 of 2015 (Amended 2017). The specific penalties, depending on the severity of the crime, are given in Article 286 of the criminal code. In Singapore, the Cybersecurity Act 2018 mandates that owners of computers designated as Critical Infrastructure Installation (CII) take all the

relevant steps to secure them. Also, all incidents involving attacks on CII must be reported as prescribed. The Cybersecurity Act has allowed the Cybersecurity Agency to investigate cybersecurity incidents.

The nature of cybercrimes is constantly evolving, and in many cases, a multi-agency approach is required to tackle them. Unlike the Case of the US, where data sharing among cybercrime investigating agencies has been legislated in the Cybersecurity Information Sharing Act (CISA) -2015, the same is not seen in Vietnam. Vietnam should adopt this concept in fighting cybercrime because it touches many sectors, and the seamless sharing of data will assist in tackling cybercrime. The U.S. has a more comprehensive approach to cybercrime than Vietnam, through legislation such as the Computer Fraud and Abuse Act (CFAA) and the Cybersecurity Information Sharing Act (CISA). These laws emphasise criminalising hacking and encouraging collaboration between private entities and the government for threat intelligence sharing. Unlike Vietnam, the U.S. focuses heavily on fostering a secure digital environment while balancing privacy concerns.

Cybercrime transcends borders, and Vietnam's challenges cannot be addressed in isolation. Participation in international agreements, such as the Budapest Convention on Cybercrime, could strengthen Vietnam's capabilities through knowledge sharing and technical support. Although Vietnam is not a signatory, joining such initiatives would align its legal framework with global standards and enhance its ability to combat transnational cybercrime.

D. CONCLUSION

As Vietnam continues to advance in its digital transformation journey, driven by rapid technological adoption, e-commerce expansion, and increased government digitisation, cybercrime is emerging as a significant and persistent hurdle. From data breaches and online scams to state-sponsored attacks and ransomware threats, the digital environment in Vietnam is becoming increasingly complex and vulnerable. These cyber threats risk undermining public trust in digital services and threaten national security, economic stability, and the privacy of individuals and organizations alike. To address these growing concerns, Vietnam must invest in building a robust and resilient cybersecurity ecosystem. This effort should begin with aligning national cybersecurity laws and frameworks with internationally recognised standards, such as those promoted by the Budapest Convention or the ASEAN cybersecurity cooperation frameworks. Legal harmonization will enhance cross-border cooperation in

combating cybercrime and attract foreign investment by ensuring a safer digital environment.

In addition to legal reform, fostering greater collaboration between government agencies, private sector players, academic institutions, and international partners is essential. Such multi-stakeholder engagement can promote knowledge sharing, enhance incident response capabilities, and support the development of a skilled cybersecurity workforce. However, while bolstering digital security, Vietnam must ensure that policies do not compromise fundamental rights and freedoms. The right balance between national security, economic innovation, and individual privacy will be key to sustainable digital growth. As Vietnam navigates the complexities of the digital age, a thoughtful, inclusive, and forward-thinking cybersecurity strategy will be crucial for building trust and resilience in its digital future.

Recommendations

1. **Enhance Legal Protections**: Amnesty International (2018) noted that Vietnam's Cybersecurity had granted the state far-reaching powers and could interfere with citizens' rights, particularly the right to expression. Vietnam should amend its cybersecurity law to balance state control with privacy rights and international norms.
2. **Capacity Building**: Vietnam faces many challenges in dealing with cybercrime. However, this challenge is not unique to Vietnam; it is a global issue. The ever-changing nature of technology and cybercrime exacerbates this. Investment in technical training for law enforcement and the judiciary is crucial to tackle cybercrime effectively.
3. **Public Awareness Campaigns**: Many people in Vietnam fall victim to cybercrime because of ignorance. Many Vietnamese are not aware of cyber-related risks and the threats they pose. Educating citizens and businesses on cyber risks and best practices can reduce vulnerabilities.
4. **International Engagement**: Signing and implementing global treaties like the Budapest Convention will bolster Vietnam’s ability to fight cybercrime collaboratively. Because cybercrimes are international, this would particularly come in handy when sharing information with international investigating agencies such as INTERPOL or even other states.

REFERENCES

Chen, S., Hao, M., Ding, F. *et al.* (2023). Exploring the global geography of cybercrime and its driving forces. *Humanit Soc Sci Commun 10*(71), 1-10. Retrieved from https://doi.org/10.1057/s41599-023-01560-x

CLOUDFLARE. (2024). What was the WannaCry ransomware attack? Retrieved from https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

Council of Europe. (2001). Convention on Cybercrime, ETS No. 185. Retrieved from https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal 96*(4), 573-592. https://doi.org/10.1177/0032258X221107584

Federal Bureau of Investigation. (2023). *Federal Bureau of Investigation Internet Crime Report 2023*.Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

Gojali, D.S. (2023). Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective. *International Journal of Cyber Criminology 17*(1), 1-11. Retrieved from https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/130/43

Khan, A. A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore. *Laws*, *13*(4), 44. https://doi.org/10.3390/laws13040044

Luong, H. T., & Ngo, H. M. (2024). Understanding the Nature of the Transnational Scam-Related Fraud: Challenges and Solutions from Vietnam's Perspective. *Laws*, *13*(6), 70. https://doi.org/10.3390/laws1306007

National Association of Criminal Defense Lawyers (NACDL). (nd.). Computer Fraud and Abuse Act (CFAA). Retrieved from https://www.nacdl.org/Landing/ComputerFraudandAbuseAct

Sabillon, Regner & Cano M., Jeimy & Serra-Ruiz, Jordi & Cavaller, Víctor. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. *International Journal of Computer Networks and Communications Security, 4*(6). 165-176. Retrieved from

https://www.researchgate.net/publication/304822458_Cybercrime_and_Cybercriminals_A_Comprehensive_Study

Singapore Cybersecurity Act 2018. https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20211231?DocDate=20180312&WholeDoc=1

Singapore Statutes online. (2024). *Computer Misuse Act 1993 (2020 Revised edition), Amended 2021*. Retrieved from https://sso.agc.gov.sg/Act/CMA1993

Trend Research. (2024). *Unmasking pig-butchering scams and protecting your financial future. Trend Micro Incorporated*. Retrieved from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/unmasking-pig-butchering-scams-and-protecting-your-financial-future

Vietnam Law on Cybersecurity 2018- No: 24/2018/QH14

U.S. Department of Justice. (nd.). 9-48.000 - Computer Fraud and Abuse Act. Retrieved from https://www.justice.gov/jm/jm-9-48000-computer-fraud#

Amnesty International. (2018 June 12). Vietnam: New Cybersecurity law a devastating blow for freedom of expression. Retrieved from https://www.amnesty.org/en/latest/news/2018/06/viet-nam-cybersecurity-law-devastating-blow-freedom-of-expression/

Council of Europe. (2022 May 12). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Council of Europe Treaty Series No. 224. Retrieved from https://rm.coe.int/1680a49dab

Council of Europe. (2023 January 1). Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, European Treaty Series - No. 189. Retrieved from https://rm.coe.int/168008160f

U.S. Government Accountability Office (GAO). (2023 June 20b). *Reporting Mechanisms Vary, and Agencies Face Challenges in Developing Metrics.* GAO. Retrieved from https://www.gao.gov/products/gao-23-106080

U.S. Government Accountability Office (GAO). (2023 August 9a). *The U.S. Is Less Prepared to Fight Cybercrime Than It Could Be*. GAO. Retrieved from https://www.gao.gov/blog/u.s.-less-prepared-fight-cybercrime-it-could-be

EUR-Lex. (2023 November 28). *Summaries of EU Legislation: Convention on cybercrime.* Retrieved from https://eur-lex.europa.eu/EN/legal-content/summary/convention-on-cybercrime.html

Murphy, Colin. (2024 March). *Understanding cybercrime*. European Parliamentary Research Service. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf

Trinh, V.D. (2024 March 20). *Vietnam's struggle with cyber security*. EastAsiaForum. https://doi.org/10.59425/eabc.1710972000

Romero, L. (2024 April 8). *Cybersecurity and cybercrime in Singapore- Statistics & facts*. Statista. Retrieved from https://www.statista.com/topics/11333/cybersecurity-and-cybercrime-in-singapore/#topicOverview

Asia Business Law Journal. (2024 April 12). Vietnam issues cybersecurity directive amid attacks. Retrieved from https://law.asia/vietnam-cybersecurity-directive-strengthening-defenses/

Viet Nam News. (2024 June 18). Online scams a growing threat in Viet Nam. Retrieved from https://vietnamnews.vn/society/1657619/online-scams-a-growing-threat-in-viet-nam.html

Morgan, S. (2024 June 24). 2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. Cybercrime Magazine. Retrieved from https://cybersecurityventures.com/cybersecurity-almanac-2024/

Hanna, K.T. (2024, July). *What is the Cybersecurity Information Sharing Act (CISA)?*. TechTarget. Retrieved from https://www.techtarget.com/whatis/definition/Cybersecurity-Information-Sharing-Act-CISA

Petrosyan, A. (2024 July 31). *U.S. Internet users and cybercrime - Statistics & Facts*. Statista. Retrieved from https://www.statista.com/topics/2588/us-internet-users-and-cybercrime/#topicOverview

United Nations. (2024 August 7c). Draft United Nations Convention against cybercrime- A/AC.291/L.15. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes Reconvened concluding session New York, 29 July–9 August 2024. https://documents.un.org/doc/undoc/ltd/v24/055/06/pdf/v2405506.pdf

United Nations. (2024 August 9b). United Nations: Member States finalize a new cybercrime convention. Retrieved from https://www.unodc.org/unodc/en/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html

Singapore Police Force. (2024 August 22). *Mid-Year Scams and Cybercrime Brief 2024.* Retrieved from file:///C:/Users/PC/Downloads/Mid-Year%20Scams%20and%20Cybercrime%20Brief%202024.pdf

United Nations. (2024 November 11a). Third Committee Submits 8 Draft Resolutions to General Assembly, Including Ones on Establishing Cybercrime Treaty, Combating Nazi Glorification. Retrieved from https://press.un.org/en/2024/gashc4428.doc.htm