Crime, Law and Social Change (2022) 77:231–252
https://doi.org/10.1007/s10611-021-09986-7

Legal challenges to combating cybercrime: An approach from Vietnam

Trong Van Nguyen[1,2] · **Tung Vu Truong**[1] · **Cuong Kien Lai**[2]

Accepted: 23 August 2021 / Published online: 10 September 2021

Abstract

This paper explores the legal challenges of combating cybercrime in Vietnam. We used a legal doctrine method to review the updated Vietnamese legal frameworks, consisting of substantive, procedural, and preventive cybercrime law. We then combined the analysis of four cybercrime cases and in-depth interviews of seven senior police officials to analyse the application of cybercrime law. The main findings reveal that by updating its legal system, Vietnam has shown a determination to prevent and disrupt cybercrime. Despite positive results, Vietnam's fight against cybercrime still faces legal challenges, including traditional and novel ones. Moreover, active and flexible approaches within Vietnam's cyberspace management can increase the effectiveness of combating cybercriminal activities; however, they can cause concerns in balancing cybercrime control and human rights protection. These approaches could then constitute a useful case study for other similar situations.

Introduction

Ranked 14th worldwide in number of Internet users [1], Vietnam makes good use of the technology revolution, as its Internet economy is described as 'a dragon being unleashed', with a growth rate of over 40% per year [2]. However, Vietnam is considered one of the new emerging cybercrime centres, along with Brazil, North Korea, India [3]. This negative position is due to the unfavourable statistics of cyberattacks originating from or targeting Vietnam [4]. More particularly, Vietnam is among the top countries concerning hacking capabilities, wherein domestic hacker groups, such as *vefamily* and *mattfeuter*, have implemented cross-border cyberattacks to obtain bank card data to steal money [5–9]. Financial incentives are not the only motivation for cybercrime in Vietnam. The 2016 cyberattacks on Vietnam's airports were assumed to

✉ Trong Van Nguyen
trongnv1607@toki.waseda.jp

[1] Graduate School of Asia-Pacific Studies, Waseda University, Tokyo, Japan

[2] Department of Mathematics, Informatics and Applying Technology Science in Combating Crime, People's Police Academy, Hanoi, Vietnam

be 'politically-coloured' from the outside under sea-related tensions between China and Vietnam [10]. One year later, another series of cyberattacks on the same victims were committed by two domestic teenagers for the purpose of showing off their talents [11]. Child pornography and copyright infringement are other main concerns of this nation [12], which is listed among countries with a high rate of unlicensed software use (74%) [13].

To cope with its negative reputation of cybercrime, Vietnam has implemented significant efforts to regulate cyberspace behaviour. Legal challenges are often considered one of the main factors influencing the effectiveness of the fight against cybercrime worldwide [14]. Similarly, Vietnamese legal framework has loopholes that create obstacles and even failures to bring suspects to justice [4, 12]. Vietnam has recently attempted to fill these legal loopholes, which has had certain positive results. Due to the update of cybercrime law, Vietnamese law enforcement agencies (LEAs) have a legal basis to crack down on many cybercriminal groups. For example, after the Penal Code criminalised the behaviour of sharing stolen bank card data in 2009, a series of Vietnamese hacking forums have been disrupted because of the cooperation between Vietnamese LEAs and their counterparts. In 2013, Vietnam, the US, and the UK established unprecedented cooperation in disrupting the *mattfeuter* gang, regarded as one of the world's major carding networks [6, 15]. While studies of legal issues are important to combat cybercrime, little information has been published about these issues in Vietnam, despite the fact that it is considered a hotspot of cybercrime [3, 4]. Therefore, the approach from the Vietnamese context should be critically examined to better understand the legal landscape concerning cybercrime worldwide.

Against this backdrop, this present study discusses how well the Vietnamese legal system can combat cybercrime. It focuses on Vietnam's attempts to regulate cyberspace by filling legal loopholes, and clarifies practical obstacles and their solutions when Vietnamese LEAs apply cybercrime law. To this end, the study first uses a doctrinal legal method to review the updated substantive, procedural, and preventive law of Vietnam. Furthermore, the research examines criminal profiles of four famous case studies and interviews with high-ranking, high-tech crime police (HTCP) officials to provide a more comprehensive understanding of practical issues.

This paper begins by providing a background of global legal challenges in combating cybercrime. The second section describes the methods for collecting and analysing data. Subsequently, the third section presents research findings, including legal challenges related to substantive criminal law, procedural law, and preventive law. Next, the fourth section focuses on the distinctive characteristics of Vietnam's cybercrime law and legal challenges. Finally, the paper concludes with recommendations for Vietnamese cybercrime-related policy, study limitations, and topics for future research.

Legal barriers to the fight against cybercrime: A global perspective

Cybercrime law is vital for the prevention and disruption of cybercrime. It covers a wide range of contents, including criminalisation, criminal procedure, international cooperation, jurisdiction, the rights and liabilities of individuals and organisations,

and other criminal justice matters in cyberspace [16], p. 52). It can be divided into substantive criminal, procedural, and preventive law [17]. Substantive criminal law regulates criminal behaviours as crime and enacts punishments for culprits. Procedural law guides the processes of applying substantive law and investigating, prosecuting, and adjudicating cybercrime cases. Where substantive criminal and procedural laws focus on bringing suspects responsible for past behaviours to justice, preventive law aims to prevent cybercrime or mitigate risks/consequences of cybercrime.

While cybercrime is considered one of the fastest increasing forms of transnational crime [18], each country has its own criminal legal system. Hence, it may be difficult for countries to trace and arrest cybercriminals located in other countries [14, 19]. In this situation, the harmonisation of law is required,however, this mission is not simple. Only 79% countries have adopted cybercrime legislation, and the share varies by region from 89% in Europe to 72% in Africa [20]. Under the principle of dual criminality, international cooperation can face obstacles when the requested nation does not have any specific legislation covering the cybercriminals' act [21–23]. Moreover, cybercrime investigation is heavily based on digital evidence that still lacks a clear legal status in certain countries [16], p. 165). Consequently, countries with insufficient legislation have a high risk of becoming safe havens for cybercrime.

The international community's different opinions about cyberspace may result in the lack of the harmonisation of cybercrime law. The concept of cyber sovereignty, as a significant factor in establishing cyberspace regulations, is still controversial, with three main disputes over its contradictions with the spirit of the Internet, with human rights, and with the involvement of multi-stakeholders in governance [24]. Furthermore, there has been an increase in the operation of 'state and state-sponsored cybercrime' groups such as PLA Unit 61,398, Unit 8200 [25], which indeed causes many countries to turn a 'blind eye' to such cybercrime. Many countries can use cyberattacks as a new weapon against their rivals [26]. A series of cyberattacks, for example, have been alleged by the US and its allies against China, Russia, and vice versa [26, 27]. As a result, it is difficult to reach a global harmonisation of cyberspace regulations.

There are international and regional treaties concerning cybercrime; however, the international community still lacks a universal convention on cybercrime. Some universal conventions like the United Nations Convention against Transnational Organised Crime and the United Nations Convention on the Rights of the Child cover a wide range of illegal behaviours but do not focus on cybercrime or cyber-related crimes. The Council of Europe's Convention on Cybercrime, also known as the Budapest Convention, was a milestone of harmonising the international community against cybercrime, as it is the first international binding legal instrument [28, 29]. It was supplemented by a 2003 Protocol on xenophobia and racism committed through computer systems. This Convention provides guidance to amend national laws and enhance international cooperation against cybercrime. Despite the requirement of update, it is the most widely ratified international convention on cybercrime. It was opened for signature by all states two decades ago,as of January 2021, roughly 70 nations have signed and ratified the Convention [30]. Some countries like China,

Russia, and India have refused to adopt the Convention, opposing it as an infringement of national sovereignty [31].

Several cybercrime-related instruments have also developed at the regional level, including but not limited to the Agreement on Cooperation in Combating Offences related to Computer Information of Commonwealth of Independent States (2001), the Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (2007), the Agreement among Member States of Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security (2010), the Arab Convention on Combating Information Technology Offences (2010), the Model Law on Computer Crime and Cybercrime of Southern African Development Community (2012), and the African Union Convention on Cyber Security and Personal Data Protection (2014). In 2019, a new Russian-drafted resolution on cybercrime was approved by the United Nations Member Body through a vote of 79–60 with 33 abstentions [32]. Differing from the Budapest Convention, it employs a spirit of Internet sovereignty that has received strong objections from major members of the Budapest Convention like the US, UK, and European Union [33]. Thus far, the international community's attempts to reach a global convention on cybercrime have been insufficient.

The jurisdictional issue in cyberspace is a complicated area for lawmakers; it has become a challenge for LEAs to fight transnational cybercrime [22]. There are often complex circumstances to decide whether jurisdiction should be based on a 'territoriality principle', 'nationality principle', 'effects principle', 'protective principle', or 'universal principle' [34]. The jurisdictional issue can become more serious with the political tension of relevant sides. For example, *CNN* reported controversial extraditions of Taiwanese cybercriminals to Mainland China [35]. Based on an extradition treaty with China, Spain extradited 94 Taiwanese criminal suspects of phone scams to China in 2019. These Taiwanese suspects, together with Chinese suspects, had migrated to Spain to defraud victims in Mainland China through phone scams. A Spanish court agreed to hand all suspects over to the Chinese authorities by stating that all victims were Mainland Chinese. Similar decisions have recently been implemented by many countries in Africa and Southeast Asia concerning Taiwanese suspects in phone scam cases to Mainland China. While Beijing has praised these decisions, Taiwan has often objected to them, calling such acts 'a gross violation of basic human rights'. These decisions have been made amid increasing political tensions between China and Taiwan across the Taiwan Strait. Beijing has adopted the 'one China' policy while Taiwan still runs its own judicial, political, foreign policy, and economic system.

There are no globally agreed rules of a priority system to solve such jurisdictional conflicts, as some international instruments recommend different approaches. For example, the negotiation among concerned states is the first approach adopted by Article 15 of the United Nations Convention against Transnational Organized Crime and Article 22 of the Budapest Convention. Additionally, Article 30 of the Arab Convention provides the instruction to adopt a priority: 'protective principle', 'territoriality principle', and 'nationality principle'. Eurojust (or the European Union Agency for Criminal Justice Cooperation) issued guidelines with main factors that should be considered when

solving judicial conflicts. Accordingly, competent authorities can evaluate various factors like territoriality, suspects, evidence, witnesses, victims, and criminal procedures [36].

The revolution in information and communications technology (ICT) has recently led to more novel challenges in the fight against cybercrime. In the circumstances relating to extraterritorial evidence, legal barriers have emerged in identifying and collecting digital data from cloud storage and service providers [37]. Cloud data can be scattered across numerous servers and multiple countries,hence, it is a complicated task to clarify where data are located and which jurisdiction applies. This challenge is illustrated in *United States v. Microsoft* [38], in which American LEAs required Microsoft to provide digital evidence of a criminal case. In response, Microsoft did not transfer American LEAs the requested content because the data were stored in Dublin and Ireland.

Moreover, the birth of cryptocurrencies, like Bitcoin, has sparked debates about their legal status in many countries [39]. Cryptocurrencies can assist criminals in conducting crime with anonymity, making it difficult for LEAs to trace culprits [3, 40]. The lack of regulations of cryptocurrencies can cause difficulties in solving relevant cases. Furthermore, private sectors play a significant role in coordinating with LEAs to suppress cybercrime [41]. They save crucial information on criminals' identities and activities, however, issues emerge when they must balance cooperating with LEAs and protecting the rights of customers [17].

Thus, scholars have pointed out that legal challenges could hinder the global fight against cybercrime. Legal challenges can originate from the loopholes or nature of substantive, procedural, and preventive law. They can exist in every country, including under-developed, developing, and even developed ones with strong legislation. Vietnam is still a developing country but has a high speed of ICT development. Vietnam is considered a hotspot for cybercrime; the country must update its legal system to cope with the increasing threats of cybercrime. The knowledge of legal issues can enable the effectiveness of the fight against cybercrime. However, little is known about Vietnamese cybercrime law and its application in fighting cybercrime. This study will clarify the Vietnamese legal framework and the extent of legal challenges to combating cybercrime, which can contribute to a better understanding of the global legal landscape on cybercrime.

Method

The research has applied both doctrinal legal research and empirical legal research methods. First, the study presents a brief review of the development of Vietnamese cybercrime law and compares it with international law. Furthermore, the study combines the data collected from four cybercrime cases and in-depth interviews with senior police officials to clarify practical obstacles relating to the Vietnamese cybercrime law.

Doctrinal legal research

As a method to systematically examine problems of the law within an appropriate framework, doctrinal legal research has been widely used by lawyers, judges, and legal researchers since the nineteenth century [42, 43]. In this paper, secondary data from law books, law articles, journals, and newspapers related to the update of the substantive, procedural, preventive law of Vietnam were collected to clarify Vietnam's efforts to develop its criminal system to be more compatible with international standards. Due to its capacity to predict future developments and explain difficulties [42, 44], doctrinal legal research was applied to the provisions of Vietnamese law in comparison to international law (in this case, the Budapest Convention, together with the Additional Protocol). The Budapest Convention has been regarded as the first international convention with a broad impact despite being the subject of certain critiques. Therefore, although Vietnam is not a member of the Budapest Convention and has not shown a likelihood of participation, the comparison is expected to provide the first insights into cybercrime regulation, after which the authors focus on practical challenges via data collected from case studies and interviews.

Case selection

The authors accessed the library of the Vietnamese Police Academy to find the main information about cybercrime cases which were investigated by the HTCP Department (now known as the Department of Cybersecurity and Counter High-tech Crime). The HTCP Department is the central agency for investigating cybercrime, establishing and implementing international cooperation against transnational cybercrime inside the Vietnam Ministry of Public Security (MPS). In addition, the researchers examined annual reports of the HTCP Department, from its inception in 2010 until its end in 2018, when it merged with another organisation to become the Department of Cybersecurity and Counter High-tech Crime. Subsequently, as a compulsory requirement within the internal police force of Vietnam, an official letter from the President of Police Academy was sent to this organisation to allow the researchers to access police files and interview representatives. The researchers were officially permitted to access police files of four cases, which provided unique insights into legal challenges and solutions when applying cybercrime regulation in practice. Police documents included reports of investigative methods, such as observation, house searches, controlled delivery, data collection, and deportation.

Interview

Semi-structured interviews were conducted with elite participants, who are leaders or senior investigators of the Department of Cybersecurity and Counter High-tech Crime. The snow-ball technique was applied to find interviewees. The researchers exploited the Police Academy's personnel database to establish relationships with senior police officials. Nine police officials were contacted for interviews; however,

only seven agreed to attend interviews, which lasted 45–60 min. One was in charge of directing the investigation of two cases; three were senior investigators, each directly involved in one case, and the remaining three were senior officials who had significant experience in investigating transnational cybercrime (Appendix Table 1). To ensure personal confidentiality and the rights of officials of Vietnamese LEAs, all seven interviews were not recorded. Handwritten notes were predominantly used, first in the Vietnamese language, which were then translated into English before entry, for analysis. NVivo 12 software was used for descriptive transcription on Windows.

Thematic analysis

As a flexible approach, thematic analysis was used to analyse the collected data. As one of the most common approaches in qualitative research analyses, it focuses on identifying and analysing themes (or patterns) within data [45, 46]. This research applied six steps, as suggested by Braun and Clarke [45], consisting of familiarizing with the data, generating initial codes, searching for themes, reviewing themes, defining themes, and producing the report. The study used an inductive approach, rather than a deductive approach, to identify the main themes and sub-themes. Accordingly, driven mainly by data, three main themes were selected, including 'substantive criminal law', 'procedural law', and 'protective law'; within each main theme, there are three sub-themes of 'main contents', 'legal issues' and 'practical consequences'. These themes and sub-themes were used to analyse the entire body of data to clarify the research question. All relevant data extracts were collated into groups identified by these themes and sub-themes.

Results

Substantive criminal law

According to the criminal policy of Vietnam, only behaviours that are regulated by the Penal Code are crimes. Before 2010, many dangerous cyberspace-related behaviours were not regulated under the Penal Code. Since 2010, when the 1999 Penal Code (amended in 2009) became valid, many dangerous cyberspace-related behaviours were regulated by the legal systems of Vietnam. The 1999 Penal Code (amended in 2009) was valid from 2010 to 2017. Afterward, the Penal Code of 2015 (amended in 2017) has been valid since 2018. The new code has one specific section titled 'Offences against Regulations on Information Technology and Telecommunications Network', consisting of nine articles regarding what is often recognised as cybercrime. Besides these, many other criminal behaviours related to cyberspace, such as infringement upon copyright and child pornography, are regulated in other sections of the two penal codes.

Judged by the standards of the Budapest Convention, the newest Penal Code of Vietnam appears adequate (see Appendix Tables 2, 3). The Budapest Convention

recommends samples of criminal offences that should be adopted by each party under domestic law. Vietnam is not a member of the convention; however, the current Vietnamese Penal Code of 2015 covers the core cybercrimes of the Budapest Convention. Certain cyber offences of the Budapest Convention can be compatible with two or three Articles that are regulated by the Vietnamese Penal Code. In certain cases, based on the description of specific behaviours, cyber offences of the Budapest Convention can be prosecuted based on Articles of traditional crime under Vietnamese legislation.

For example, 'illegal interception' referred to in the Budapest Convention is covered by two Articles of the 2015 Vietnamese Penal Code. 'Illegal interception', regulated by Article 3 of the Budapest Convention, concerns the violation of the confidentiality of computer data and systems. Similarly, in Vietnam, the behaviours of 'illegal interception' include listening to, monitoring, surveilling, or recording conversations illegally, through technical means. This could be prosecuted by Article 159 or Article 289 of the 2015 Penal Code. Therefore, if these behaviours are not implemented with complicated techniques, 'illegal interception' can be addressed by Article 159 of the 2015 Penal Code, which states: 'Infringement upon other persons' confidentiality and safety of mail, telephone, telegraph, or other means of private information exchange'. This does not focus on the technical aspects of interception, but on the traditional confidentiality of citizens' rights. However, if 'illegal interception' is a subsequent step of illegal access at a high degree of technology, this behaviour can fall under Article 289 of the 2015 Penal Code, which states: 'Illegal infiltration into the computer network, telecommunications network, or electronic device of another person'.

The loopholes of the previous penal codes significantly impacted the practice of LEAs in combating cybercrime. For example, before 2010, the behaviour of sharing sensitive data, such as stolen bank card information, had not been a crime because the 1999 Penal Code did not cover such behaviour. Accordingly, before 2010, there was no legal basis to prosecute transnational cybercrime groups who shared or purchased stolen bank card data. Many underground websites constructed by Vietnamese hackers were used popularly as a meeting point where Vietnamese and foreign members exchanged bank card data [5]. However, since 2010, the behaviour of exchanging and uploading bank card data illegally has been regulated by the penal code. The update establishes the ground for cooperation between Vietnamese LEAs and their counterparts to shut down many carding forums.

On the basis of the updated legal framework, in 2013, one of the world's largest carding forums, run by Vietnamese hackers, was cracked down on by the joint operation known as 226 T between the Vietnamese MPS, Serious Organised Crime Agency (SOCA), and Federal Bureau of Investigation (FBI). Operating at least from 2009 to 2013, Van Tien Tu and other accomplices designed the *mattfeuter* underground sites, with approximately 16,000 members. The *mattfeuter g*ang was estimated to have traded in 1.1 million pieces of stolen bank card data, causing at least US$200 damage to global victims. When discussing the legal challenges of this case, the senior investigator, I03, who was also responsible for investigating the case, shared the role of the legal basis as follows:

> The cooperation [between SOCA, FBI, and HTCP Department of Vietnam] was unprecedented, especially because it lasted for a long time [from August 2009 to May 2013]. One difficulty was that in the first period, the behaviour of uploading and sharing bank card data on the Internet was not regulated strictly under the 1999 Penal Code. When the new version of Penal Code [amended in 2009] was valid, the principle of dual criminality was guaranteed. Owing to the cooperation between Vietnam and counterparts, beside the *mattfeuter* forums, many Vietnamese carding forums such as *vefamily.com* and *vietexpert.info* were cracked down in this period. (Interview #3)

The 2009 amendment of the 1999 Penal Code updated almost all behaviours of cybercrime, but there were also related issues [47, 48]. For instance, before 2018, when the 2015 Penal Code became valid, the behaviour of collecting and storing illegal bank card data created a potentially difficult prosecution. Despite the danger, these behaviours were not strictly ruled out in the old version of the penal code. If law enforcement forces wanted to bring these dangerous acts to justice, they used another article about computer fraud. As a result, before 2018, it was not easy to prosecute suspects with only the behaviour of stealing bank card information or their further illegal activities could not be clarified beyond a doubt.

Under the expansive growth of cryptocurrency, many countries have issued policies and laws on this subject [39]. The anonymity makes it open to cybercrime and other illegal activities such as money laundering and tax evasion. In Vietnam, cryptocurrency is not a legal means of payment, which is determined by Official Dispatch 02/CT-NHNN enacted by the State Bank of Vietnam on April 13, 2018. Accordingly, the issuance, supply, and use of cryptocurrency for payment instruments are not allowed in Vietnam. However, investment activity and business relating to cryptocurrency are not clearly defined as prohibited actions. This means that cryptocurrency is banned as a means of payment but is allowed to be traded in Vietnam. The Vietnamese government is on the road to establishing a legal framework for cryptocurrency.

While the regulations of cryptocurrency are still being constructed, illegal activities concerning cryptocurrency have occurred with serious financial consequences. Some companies fabricate virtual investment projects to collect investment capital, which is a type of cyber fraud in nature. In 2018, a Vietnam-based startup Modern Tech was accused of appropriating about US$660 million. Modern Tech advertised its cryptocurrencies iFan and Pincoin with a huge monthly interest of at least 48%. Members could also receive large commissions for introducing new members. However, after more than 32,000 customers invested in iFan and Pincoin, they could not withdraw their investment in cash. Although the trade of cryptocurrency is not prohibited in Vietnam, there is no unified view about whether cryptocurrency is a type of asset [49]. Consequently, LEAs face difficulties when solving cases in which cryptocurrency is stolen or obtained illegally, as Vietnamese criminal law regulates only assets as the target of fraud and theft behaviours.

Procedural law

Concerning regulations about procedure, since 2010, investigations and proceedings against cybercrime in Vietnam have been based on two criminal procedure codes and one law. From 2010 to 2017, the powers and procedures of processing criminal cases were laid out in the 2003 Criminal Procedure Code. Since 2018, the 2015 Criminal Procedure Code has been in force. Both codes play an important role in regulating matters of international cooperation in criminal proceedings. This includes articles specifying principles for international cooperation, judicial assistance, extradition, and the transfer and receipt of files, documents, objects, exhibits, and money related to criminal cases. Additionally, the Law on Mutual Legal Assistance that was enacted in 2008 has created a legal foundation for mutual legal assistance and the extradition and transfer of convicts.

One primary challenge related to procedure law is that the term 'digital evidence' is not included in the 2003 Criminal Procedure Code. Therefore, before the 2015 Criminal Procedure Code was enacted, there was a dispute about whether digital evidence was accepted. The lack of procedural laws on digital or electronic evidence plagues the global fight against cybercrime [16, 50], p. 165). The Budapest Convention, opened for signature in 2001, suggests that each state adopt legislative and other measures to preserve, search for, and collect digital evidence. After nearly two decades, digital evidence was officially regulated in the 2015 Criminal Procedure Code of Vietnam. Accordingly, preservation, search, access, and collection of digital data are under Articles 88, 99, 107, and 196 of the 2015 Criminal Procedure Code.

The HTCP Department [5, 6, 48] emphasised the lack of regulation for digital evidence as a major challenge hindering the effectiveness of investigating and prosecuting cybercrime. Before the 2015 Procedure Code, to prosecute cybercriminals, digital evidence often had to be printed into traditional documents, although such requirements could take a long time. Even computer printouts caused disputes about the admissibility of digital evidence when evaluating the originality of evidence. The update of adding digital evidence into the 2015 Criminal Procedure Code is a crucial step to create a legal basis for digital forensics. However, LEAs still cope with practical obstacles since there is currently no clear guideline for the authentication and integrity of digital evidence. The methods of collecting, analysing, and presenting digital evidence are not unified, as the application of digital forensics depends heavily on practitioners' qualifications and views. One decade after its founding, the Vietnamese HTCP still faced challenges relating to technical snags and human resources [11]. The ability of law enforcement officials, especially at local police stations, is limited when processing digital evidence. They are not equipped and well trained to use specialized tools for digital forensics. This issue indeed has a negative impact on the admissibility of digital evidence when it is used to solve cybercrime cases.

As an enthusiastic member of the international community against transnational crime, Vietnam has participated in multilateral instruments on criminal matters (e.g. the United Nations (UN) Convention against Transnational Organised Crime, the Association of Southeast Asian Nations (ASEAN) Treaty on Mutual Legal Assistance in Criminal Matters, the 2003 Cybersecurity Strategy of Asia–Pacific

Economic Cooperation (APEC), and the ASEAN Declaration to Prevent and Combat Cybercrime at the 31st ASEAN Summit). Such movements seek to advance Vietnam's cooperation with the international community against transnational crime. Additionally, Vietnam had signed 21 bilateral treaties regarding mutual legal assistance and 11 bilateral treaties about extradition as of July 2017 [51]. However, these bilateral instruments seem outdated in combating cybercrime. The content of these treaties focuses on traditional crimes rather than cybercrime, while the fight against cybercrime requires more special mechanisms of cooperation concerning digital data, 24/7 network.

Applying jurisdictional principles can be a challenge for international cooperation against transnational cybercrime, as more than one country asserts jurisdiction over one specific cybercrime case [22, 34]. In 2015, 24 Chinese and Taiwanese criminals entered Vietnam and hired two apartments in Ho Chi Minh City to implement phone scams in Mainland China. Vietnamese sovereignty was used as the operational base for foreign offenders to implement transnational crime scripts. Vietnamese LEAs carried out Operation TQ2015 and cooperated with LEAs of Mainland China and Taiwan to solve this case. There was an argument over an appropriate approach to jurisdiction among relevant parties. Under the 'territoriality principle', the case could be solved within the jurisdiction of Vietnam, where the criminal behaviours occurred. The 'effects principle' and 'protective principle' could also be invoked when all victims were Chinese. However, lastly, after close dialogues among the counterparts, Vietnam handed Chinese suspects over to Chinese authorities while Taiwanese suspects were transferred to Taiwanese authorities.

Interviewee I04 explained the reason for applying the national principle in case C03 and other similar cases in Vietnam:

> This case is a typical one in which a big group of Chinese and Taiwanese offenders brought tools to enter Vietnam to set up the system of fraudulent VoIP calls. They used the Vietnamese Internet infrastructure to implement phone scams on Chinese victims. All offenders and victims were Chinese. Vietnam did not receive any harm. The transfer of the case was based on legal frameworks and bilateral agreements [between Vietnam and Mainland China and Taiwan]. LEAs of Vietnam transferred the case, but foreign counterparts had to inform the result of the criminal process and response to the requests of Vietnam. (Interview #4)

International cooperation between law enforcement must cope with differences in procedural legal systems [50, 52]. This challenge was clearly shown by analysing the data of Operation 129 T. In the period of 2008 to 2010, Vuong Huy Long and other accomplices joined the website *vefamily.com* (consisting of around 2,000 members) to buy and sell stolen credit card data. Vietnamese hackers attacked foreign websites to obtain credit card information. Afterwards, they used stolen credit card data to buy products online from American websites. To prosecute criminals, Vietnamese LEAs implemented Operation 129 T and attempted to set up international cooperation with the US Department of Homeland Security. However, there is a sizeable difference in the results of cooperation between the LEAs of Vietnam and America in Operations 129 T and 226 T. In the *mattfeuter* case (Operation 226 T),

information from criminals' Gmail and Yahoo accounts and carding websites hosted in America could be easily obtained by Vietnamese HTCP with the support of the FBI. However, in the *vefamily* case (Operation 129 T), Vietnam's LEAs could not establish international cooperation effectively with their American counterparts.

The analysis of investigation documents and interviews indicate that the failure of the *vefamily* case was a result of the difference between the two countries regarding the requirement to collect data. Vietnam's procedural legal system does not always require a court warrant to access data (see the 2015 Criminal Procedure Code and the Law on Cyber Security). However, a court warrant is often a compulsory requirement for American LEAs when approaching data [53, 54]. To explain this, senior investigator, I02, who was also in charge of the *mattfeuter* case, shared the following:

> The first point of setting up international cooperation was implemented by the US LEAs. After receiving a request [from their US counterpart], Vietnamese police carried out Operation 226T to clarify the suspects. Under the operation, Vietnamese police requested [the FBI] to support in collecting information about victims, banks, websites, and mails hosting in the US. At this time, the US Department of Justice filed charges against Vietnamese suspects of transnational fraud networks, therefore with a court order, the American LEAs were quick to clarify the information, and then responded to Vietnam's requirement. (Interview #2)

However, investigator I03 of the *vefamily* case explained the negative result of international cooperation as Vietnamese LEAs could not provide necessary documents requested by American LEAs in this case:

> Operation 129T was established and implemented first by the HTCP Department [of Vietnam]. When we sent the request of supporting data collection to the US Immigration and Customs Enforcement (ICE), ICE required us to submit more evidence and documents which satisfied their domestic legal system. According to the American law, a court warrant should be generally issued before LEAs get data. We failed to provide the requested documents because the investigation was only at the first stage. We could not obtain the court warrant. [In Vietnam], when we set up an investigative operation, we are allowed to implement some specialized methods to collect information without the court warrant. (Interview #3)

In comparison with informal mechanisms of international cooperation, formal ones, such as extradition and mutual legal assistance, have not been used as much. In all three case studies, informal forms of international cooperation were used for sharing information, collecting evidence, and arresting culprits. In Operation TQ2015, foreign suspects were also illegal immigrants who violated Vietnamese regulations about residence management. Vietnam transferred the investigative documents and deported foreign suspects to Mainland China and Taiwan based on the 2014 Minute of 4th Conference about Countering Crime, signed by the Vietnamese MPS and the Chinese MPS; the 2012 Agreement between the

Vietnam Economic and Cultural Office in Taipei and the Taiwanese counterpart. In this case, 'deportation under the control of LEAs' removed foreign suspects from Vietnam with fast-track procedures. After receiving suspects, the counterparts took over the case, and officially arrested them inside their territory or international zones.

The informal form of international cooperation via the INTERPOL channel is used popularly (instead of mutual legal assistance) by Vietnamese LEAs. In Vietnam, to some extent, the evidentiary requirements of investigations and prosecutions may be accepted using the INTERPOL channel. Evaluating the role of formal and informal mechanisms of international cooperation in combating cybercrime, interviewee I04 shared the following:

> Vietnam has entered many treaties, at both bilateral and multilateral levels. This movement creates a legal basis for establishing and carrying out formal international cooperation in combating cybercrime. However, the traditional mechanism [of formal international cooperation] often takes a long time and complicated procedures. Whereas, sharing information related to cybercrime requires quick speed. To investigate cybercrime, 24/7 networks are vital. Time is gold! (Interview #4)

According to the function of INTERPOL, its I-24/7 network is an informal communication channel that assists law enforcement officers of all member countries in sharing information and in coordinated operations with counterparts [55]. Via INTERPOL, Vietnamese police forces have received many requests from their counterparts to investigate suspicious information about cybercrime [5–7]. In the *vefamily* case, on 18 December 2009, via the Vietnam INTERPOL Office, the HTCP Department received the FBI's request to clarify information about suspicious IP addresses. In the *mattfeuter* case, the HTCP Department cooperated with SOCA and the FBI through the Vietnam INTERPOL Office to exchange information and conduct a 'controlled delivery' method to trace suspects. However, the efficiency of international cooperation via INTERPOL is called into doubt when, in some situations, there are no responses from counterparts when the Vietnamese police forces send requests. Evaluating the efficiency of the INTERPOL network, interviewee I01 explained the following:

> INTERPOL with its I-24/7 network has provided substantial support to Vietnamese cyber police in sharing information related to cybercrime. However, the result of cooperation is not all positive, maybe because INTERPOL covers a wide range of crimes and it does not create a binding mechanism for cooperation. In some cases, when Vietnamese police forces sent a request for cooperation to counterparts [via INTERPOL], there were no responses. I think that a 24/7 network that specialises in cybercrime is more important for assisting Vietnamese police forces in sharing information and carrying out transnational operations with their counterparts (Interview #1).

With the acknowledgement of a call for a 24/7 network that specialised in cybercrime, the Vietnam HTCP Department joined the G8 24/7 High Tech Crime

Network in 2015. The G8 24/7 contact points create a quick procedure for receiving and sending requests. In 2016, the HTCP Department received and processed fire requests from their counterparts via the G8 24/7 network [56]. In 2017 and 2018, the number of requests processed were seven and four, respectively [11, 57]. The participation of the Vietnamese cyber police in the G8 24/7 network shows the strong commitment of Vietnam in international cooperation against cybercrime.

Preventive law

The principle of cyberspace sovereignty is a core element of Vietnamese preventive regulation against cybercrime. Article 2 of the 2018 Law on Cybersecurity defines the term 'national cyberspace' as cyberspace established, managed, and supervised by the government. The journal *Communist Review: The Organ of Political Theory of Communist Party's Central Committee* states that the assurance of national sovereignty is to protect the sovereignty of the territory, land area, sea area, sky area, and cyberspace [58]. Cyberspace territory includes information areas that the state manages and controls directly or indirectly with policies, regulations, and technology capacities,it is a part integrated into the national territory [59]. All these statements prove that cyberspace activities must be under the Vietnamese government's management under the principle of national sovereignty.

The central task of ensuring cybersecurity is assigned to the MPS. Based on Article 8 and Article 36 of the 2018 Law on Cybersecurity, police forces are in charge of presiding over coordination with other Ministries to protect cybersecurity and combat cybercrime. Before 2018, the MPS had two main entities dedicated to cybercrime and cybersecurity, including the HTCP Department and the Cybersecurity Department. They are called Cybersecurity Task Forces inside MPS. In 2018, both agencies merged into the Department of Cybersecurity and Counter High-tech Crime.

Joint liability is at the core of the mechanism of protecting cybersecurity. Cybersecurity Task Forces are organised under the MPS and the Ministry of National Defence. Differing from the role of the MPS, the Ministry of National Defence is responsible for military information systems. In addition, based on Article 30 of the 2018 Law on Cybersecurity, other cybersecurity-related forces are to be arranged at central and local agencies that directly manage important information systems. Organisations and individuals can be mobilised to participate in protecting cybersecurity and combating cybercrime. Service providers are responsible for coordinating with and facilitating Cybersecurity Task Forces to conduct the activities of protecting cybersecurity. Thus, cybersecurity protection requires all organisations and individuals to cooperate with Cybersecurity Task Forces.

One of the most controversial aspects of cybersecurity policy is related to service providers' obligations. The Vietnamese government requires service providers to keep data and establish offices within the country (Article 26, the 2018 Law on Cybersecurity). Accordingly, even the cloud data of Vietnamese end-users are required to be stored in Vietnam for a period of time. On the one hand, these

regulations are evaluated actively and positively as creating a legal foundation for protecting individual and national data, ensuring rights and legitimate interests in cyberspace [60–62]. Moreover, such legislation supports cybercrime prevention and investigation as Vietnamese LEAs can request service providers for cooperation conveniently [60]. On the other hand, it has also been criticised for increasing censorship on personal freedoms,besides, technology companies must spend more fees to operate their businesses in Vietnam [63, 64].

Discussion

Vietnam, as one of the emerging cybercrime centres [3], must implement many solutions to deal with legal challenges in the fight against cybercrime. The update of cybercrime regulations seems to be the most effective method, although the process can be cumbersome. This review of the Vietnamese legal framework proves that some loopholes of the older versions of the penal code were corrected under the 2015 Penal Code (amended in 2017). More particularly, before 2010, only a few dangerous behaviours related to information communications technology were regulated as cybercrime. Since 2010, the number of cybercrime articles has increased. Especially with the application of the 2015 Penal Code, the substantive criminal law of Vietnam can be regarded as sufficient, compared to the Budapest Convention.

The Budapest Convention, which is itself nearly 20 years old, is evaluated as inadequate and should be updated. Therefore, it is necessary to evaluate the ability of Vietnamese cybercrime law to combat current cybercrime context. Accordingly, the research can identify serious legal loopholes. More specifically, the lack of clear regulations about cryptocurrency is problematic. Differing from certain countries like Japan and the UK, which legalise cryptocurrency in their legal frameworks [39], Vietnam bans its use as a legal form of payment. While the official legal framework about cryptocurrency is being constructed, cryptocurrency is increasingly exploited by cybercriminals, with serious consequences. This issue does impose negative impacts on the prevention and disruption of cybercrime. Moreover, it can lead to other issues concerning civil and business laws when the trade of cryptocurrency is not prohibited. For example, tax agencies do not have a legal basis for collecting the tax of business activities relating to cryptocurrency because it is not officially considered a type of asset. Hence, the Vietnamese government should respond quickly to update regulations on cryptocurrency.

In comparison with substantive criminal law, procedural law seems to bear more challenges in apprehending and prosecuting cybercriminals. The dissimilar legal regulation of authorities and procedures is a unavoidable issue because each country has its own legal system [21–23]. Moreover, despite being updated in the newest Procedural Criminal Code, digital evidence still causes certain difficulties for LEAs. Vietnamese LEAs lack unified guidelines for collecting, analysing, and using digital evidence. Consequently, the admissibility of digital evidence can be impacted by the ability and view of LEAs.

Additionally, jurisdiction in cyberspace could become another obstacle for LEAs to fight transnational cybercrime [22, 34]. Operation TQ2015 illustrates a dispute about

which jurisdiction should apply between the three states of Vietnam, Mainland China, and Taiwan. In comparison with the Spanish case and other cases relating to Chinese and Taiwanese suspects [35], Vietnam selected a different option based on the 'unofficial' 'national principle'. While Vietnam officially recognises the 'one China' policy with only the People's Republic of China, Vietnam-Taiwan relations are implemented at an unofficial level. Moreover, in this case, Vietnam was not harmed when all suspects and victims were foreign. With a close dialogue between Vietnamese LEAs and partners, the last option was based on the 'unofficial' 'national principle'. Chinese and Taiwanese suspects were handled over to the respective authorities. This Vietnamese approach may be useful for the adoption in other similar cases.

Vietnam is a member of certain multilateral and bilateral treaties. However, these treaties often focus on traditional crimes rather than cybercrime, which requires special forms of international cooperation relating to digital data and rapid information exchange. These treaties regulate formal forms such as mutual legal assistance and extradition that require complicated and time-consuming legal procedures. In practice, Vietnamese LEAs tend to use informal forms that can increase the speed of exchanging information and investigate transnational cybercrime. While in the Spanish case it took two years to extradite Chinese and Taiwanese suspects [35], 'deportation under the control of LEAs' could be an effective fast process in the Vietnamese case. Here Vietnamese LEAs are based on residence management regulations to hand over illegal immigrants to counterparts. In addition, the evidentiary standard via the INTERPOL channel can still be somewhat accepted in prosecuting criminals. Furthermore, the 24/7 networks of INTERPOL or G8 High Tech Crime Network also support Vietnamese LEAs to help clarify suspicious information rapidly. Such flexible approaches are expected to increase the effectiveness of counter-cybercrime methods while there is still a lack of official treaties on cybercrime between Vietnam and others.

The preventive law of Vietnam emphasises the principle of sovereignty in cyberspace. Accordingly, online behaviours must be regulated under the principle of national sovereignty. Moreover, the 2018 Cybersecurity Law calls for compulsory local storage of data by service providers, opening offices in Vietnam, and cooperating with LEAs when being requested. These regulations illustrate an active approach of the Vietnamese government to combating cybercrime and other illegal activities. They permit Vietnamese LEAs to solidify their management over cyberspace within Vietnamese borders. Simultaneously, they restrict access from outsiders to data relating to Vietnamese end-users. However, they fuel debates about the balance between cybercrime control and human rights [63, 64]. This approach of Vietnam is different from the Budapest Convention, especially concerning Article 32, which permits transborder access from outsiders to local data. It is similar to the new UN Russian-drafted resolution, which also focuses on Internet sovereignty [33].

Conclusion

Vietnam can be evaluated as a cybercrime centre, and the Vietnamese government definitely needs to implement various methods of combating cybercrime. The amendment of cybercrime law shows a strong determination of Vietnam in the fight

against cybercrime. In particular, the new version of the Vietnamese cybercrime law covers a list of cybercrimes, as recommended by the Budapest Convention, wherein some cybercrime behaviours can be processed under provisions of legislation on traditional crime. However, it still includes problematic issues, especially relating to cryptocurrency, digital evidence, jurisdiction, dissimilar legislation, and individuals' and organisations' liability. Besides, active and flexible approaches are expected to increase the effectiveness of preventing and disrupting cybercrime; however, they can cause concerns over balancing cybercrime control and the protection of human rights.

The update or correction of the legal system will have a major impact on each country's ability to combat cybercrime. The research findings have implications for improving the legal system in Vietnam. First, a clear regulation about cryptocurrency is needed to prevent and interrupt illegal activities relating to cryptocurrency. The legal position of cryptocurrency should be clarified, such as whether it is a form of currency or only a form of assets. This identification can create a legal basis for protecting the rights of victims in cryptocurrency-related cyberfraud cases and other related activities like business and tax collection. Second, Vietnam should quickly enact unified guidelines of digital evidence that focus on how to authenticate digital evidence, prove its integrity, and ensure its admissibility. Third, the flexible, informal approach can be used effectively in certain situations; however, the formal approach should be considered carefully to improve enduring countermeasures. While the international community is still attempting to reach a universal convention on cybercrime, Vietnam should enhance formal cooperation with key partners that are often relevant to cybercrime originating from or targeting Vietnam. Last, it is important to balance cyberspace regulation and human rights protection. Cyberspace regulation should be precise and avoid providing practitioners with opportunities for power abuse or unbounded discretion.

Although this study attempts to provide valuable insight into Vietnam's approach to the legal challenges against cybercrime, it has certain limitations. Interviews were held with only seven high-ranking cyber police officials who were involved directly in investigations of cybercrime. However, the fight against cybercrime can be relevant to other forces as well, such as INTERPOL within MPS, the Supreme People's Procuracy, the Supreme People's Court, and the Ministry of Justice. In addition, the application of the cybercrime law in practice should be analysed more critically with the examination of the background and training of LEAs, the attitudes of individuals and organisations towards the current cybercrime law, and the trend of cybercrime. Future research should consider larger samples of participants and other sources and methods, to reach a more comprehensive finding.

Appendix 1

Table 1

Acknowledgements We would like to thank Prof. Ken Miichi (Waseda University) for his advice and his comments on earlier versions of the article.

Table 1 Interviewee information

Interviewee	Age	Rank	Gender	Note
I01	46	Senior Colonel	Male	Directing investigation of Operation 129 T, 226 T
I02	39	Lieutenant Colonel	Male	Investigating Operation 129 T
I03	37	Major	Male	Investigating Operation 226 T
I04	35	Major	Male	Investigating Operation TQ2015
I05	33	Captain	Female	
I06	37	Major	Male	
I07	40	Lieutenant Colonel	Male	

Author contribution All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Trong Van Nguyen. The first draft of the manuscript was written by Trong Van Nguyen. Tung Vu Truong and Cuong Kien Lai commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding No funding was received for conducting this study.

Declarations

Ethics approval All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

Conflicts of interest The authors declare no potential conflicts of interest.

References

1. Internetworldstats. (2020). *World Internet usage and population statistics*. https://internetworldstats.com/stats.htm#links
2. Google & Temasek. (2018). *e-Conomy SEA 2018: Southeast Asia's Internet economy hits an inflection point*. https://www.thinkwithgoogle.com/_qs/documents/6730/Report_e-Conomy_SEA_2018_by_Google_Temasek_v.pdf
3. McAfee & CSIS. (2018). *Economic impact of cybercrime – No slowing down*. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf
4. Nguyen, T. V. (2020). Cybercrime in Vietnam: An analysis based on routine activity theory. *International Journal of Cyber Criminology, 14*(1), 156–173. https://doi.org/10.5281/zenodo.3747516
5. HTCP Department. (2010). *Bao cao tong ket nam 2010* [Annual report 2010]
6. HTCP Department. (2013). *Bao cao tong ket nam 2013* [Annual report 2013]
7. HTCP Department. (2014). *Bao cao tong ket nam 2014* [Annual report 2014]
8. Nguyen, T., & Luong, H. T. (2020). The structure of cybercrime networks: Transnational computer fraud in Vietnam. *Journal of Crime and Justice,* 1–22.https://doi.org/10.1080/0735648X.2020.1818605
9. Nguyen, T. V. (2021). The modus operandi of transnational computer fraud: A crime script analysis in Vietnam. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-021-09422-1
10. Goel, A. (2016). *The great cyber game in South China Sea*. https://cyware.com/news/the-great-cyber-game-in-south-china-sea-883f7f39?PageSpeed=noscript
11. HTCP Department. (2017). *Bao cao tong ket nam 2017* [Annual report 2017]

Table 2 Comparison of cybercriminal behaviours between Vietnamese criminal law and the Budapest Convention

The Budapest Convention	2015 Penal Code, amended in 2017
Article 2: Illegal access	Article 289: Illegal infiltration into the computer network, telecommunications network, or electronic device of another person
Article 3: Illegal interception	Article 159: Infringement upon another person's confidentiality and safety of mail, telephone, telegraph, or other means of private information exchange; or Article 289: Illegal infiltration into the computer network, telecommunications network, or electronic device of another person
Article 4: Data interference	Article 286: Spreading software programs that are harmful for computer networks, telecommunications networks, or electronic devices; or Article 287: Obstructing or disordering the operation of computer networks, telecommunications networks, or digital devices; or Article 294: Deliberate harmful interference of radio frequencies
Article 5: System interference	Article 287: Obstructing or disordering the operation of computer networks, telecommunications networks, or digital devices; or Article 294: Deliberate harmful interference of radio frequencies
Article 6: Misuse of devices	Article 285: Manufacturing, trading, exchanging, or giving over instruments, equipment, or software serving illegal purposes; or Article 286: Spreading software programs that are harmful for computer networks, telecommunications networks, or electronic devices; or Article 288: Illegally uploading or using information on computer networks or telecommunications networks
Article 7: Computer-related forgery	Article 212: Forging documents in an offering or listing profile or Article 290: Using computer networks, telecommunications networks, or digital devices to appropriate property; or Article 341: Fabricating an organisation's seal or document and use thereof
Article 8: Computer-related fraud	Article 290: Using computer networks, telecommunications networks, or digital devices to appropriate property; or Article 291: Illegally collecting, storing, exchanging, trading, and publishing information about bank accounts
Article 9: Offences related to child pornography	Article 326: Distributing pornographic materials
Article 10: Offences related to infringements of copyright and related rights	Article 225: Infringement of copyrights and relevant rights

Table 3 Comparison of cybercriminal behaviours between Vietnamese criminal law and the Additional Protocol to the Budapest Convention

The Additional Protocol	2015 Penal Code, amended in 2017
Article 3 – Dissemination of racist and xenophobic material through computer systems	Article 288: Illegally uploading or using information on computer networks or telecommunications networks
Article 4 – Racist and xenophobic motivated threat	Article 133: Threat of murder
Article 5 – Racist and xenophobic motivated insult	Article 155. Insults to another person
Article 6 –Denial, gross minimisation, approval or justification of genocide or crimes against humanity	Article 288: Illegally uploading or using information on computer networks or telecommunications networks
Article 7 – Aiding and abetting	Article 17. Complicity

12. Luong, H. T., Duc Phan, H., Chu, D. V., 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), 290–308. https://doi.org/10.5281/zenodo.3700724
13. BSA. (2018). *Software management: Security imperative, business opportunity.* https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf
14. Europol & Eurojust. (2019). *Common challenges in combating cybercrime*. https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime
15. FBI. (2013). *Leader in $200 million international stolen data ring charged in New Jersey as part of worldwide takedown.* https://archives.fbi.gov/archives/newark/press-releases/2013/leader-in-200-million-international-stolen-data-ring-charged-in-new-jersey-as-part-of-worldwide-takedown
16. UNODC. (2013). Comprehensive study on cybercrime - Draft. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
17. UNODC. (2019b). The role of cybercrime law. https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html
18. INTERPOL. (2017). *Global cybercrime strategy (summary)*. https://www.interpol.int/en/content/download/5586/file/Summary_CYBER_Strategy_2017_01_ENLR.pdf
19. Gercke, M. (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/CybercrimelegislationEV6.pdf
20. UNCTAD. (2020). *Data and privacy unprotected in one third of countries, despite progress*. coursereg.waseda.jp/portal/simpleportal.php?HID_P14=EN. Accessed 28 Apr 2021
21. Clough, J. (2014). A world of difference: The Budapest Convention on cybercrime and the challenges of harmonisation cybercrime: A global challenge. *Monash University Law Review*, *40*(3), 698–736. https://link.gale.com/apps/doc/A422445386/AONE?u=waseda&sid=AONE&xid=f83b8d9d
22. Maillart, J. (2019). The limits of subjective territorial jurisdiction in the context of cybercrime. *ERA Forum, 49*, 375–390. https://doi.org/10.1007/s12027-018-0527-2
23. Singh, M., & Singh, S. (2007). Cyber crime convention and trans border criminality. *Masaryk University Journal of Law and Technology, 1*(1), 53–66.
24. Yeli, H. (2017). A three-perspective theory of cyber sovereignty. *PRism, 7*(2), 109–115.
25. Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, *8*(1), 1–20. https://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf
26. Shasha, C. (2021). *Cyber security becomes new US weapon against China, Russia*. Global Times. https://www.globaltimes.cn/page/202103/1217885.shtml
27. Volz, D., & McMillan, R. (2021). *Massive hacks linked to Russia, China exploited U.S. Internet security gap*. The Wall Street Journal. https://www.wsj.com/articles/massive-hacks-linked-to-russia-china-exploited-u-s-internet-security-gap-11615380912. Accessed 28 Apr 2021

28. Boni, B. (2001). Creating a global consensus against cybercrime. *Network Security, 2001*(9), 18–19. https://doi.org/10.1016/S1353-4858(01)00918-7
29. Peters, A., & Jordan, A. (2020). Countering the cyber enforcement gap: Strengthening global capacity on cybercrime. *Journal of National Security Law & Policy*, *10*(3), 487–524. Retrieved from http://thirdway.imgix.net/JNSLP.pdf
30. The Council of Europe. (2021). Chart of signatures and ratifications of Treaty 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=fDCxuST0. Accessed 16 Jan 2021
31. Mehrotra, K. (2019). On global cybercrime, India votes in favour of Russia-led resolution. *The Indian Express*. https://indianexpress.com/article/india/on-global-cybercrime-india-votes-in-favour-of-russia-led-resolution-6130980/
32. Stolton, S. (2020). *UN backing of controversial cybercrime treaty raises suspicions*. EURACTIV. https://www.euractiv.com/section/digital/news/un-backing-of-controversial-cybercrime-treaty-raises-suspicions/
33. Sherman, J., & Morgus, R. (2018). *Breaking down the vote on Russia's new cybercrime Resolution at the UN*. New America. https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/breaking-down-vote-russias-new-cybercrime-resolution-un/
34. Brenner, S., & Koops, B. (2004). Approaches to cybercrime jurisdiction. *Journal of High Technology Law*, *4*(1), 1–46. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507%5Cn, http://ssrn.com/abstract=786507.
35. Jiang, S. (2019). *94 Taiwanese criminal suspects extradited from Spain to Beijing*. CNN. https://edition.cnn.com/2019/06/07/asia/taiwan-extradition-beijing-intl/index.html
36. Eurojust. (2016). *Guidelines for deciding 'which jurisdiction should prosecute?'* https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2016_Jurisdiction-Guidelines_EN.pdf
37. UNODC. (2019a). Challenges relating to extraterritorial evidence. https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/challenges-relating-to-extraterritorial-evidence.html
38. United States v. Microsoft (584 U.S. __ (2018)
39. Global Legal Research Center. (2018). *Regulation of cryptocurrency around the world*. The Law Library of Congress. https://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf
40. United Nations. (2019). *Countering the use of information and communications technologies for criminal purposes*. https://www.unodc.org/documents/Cybercrime/SG_report/V1908182_E.pdf
41. UNODC. (2019c). Who conducts cybercrime investigations? https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/who-conducts-cybercrime-investigations.html
42. Gawas, V. M. (2017). Doctrinal legal research method a guiding principle in reforming the law and legal system towards the research development. *International Journal of Law, 3*(5), 128–130.
43. Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. *Deakin Law Review, 17*(1), 83–119. https://doi.org/10.21153/dlr2012vol17no1art70
44. Tiller, E. H., & Cross, F. B. (2006). What is legal doctrine? *Northwestern University Law Review, 100*(1), 517–534.
45. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.
46. Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*(1), 1–13. https://doi.org/10.1177/1609406917733847.
47. HTCP Department. (2011). *Bao cao tong ket nam 2011* [Annual report 2011]
48. HTCP Department. (2012). *Bao cao tong ket nam 2012* [Annual report 2012]
49. Bien, T. Van, & Oanh, N. M. (2020). Tien ao va mot so van de phap ly dat ra o Viet Nam hien nay [Cryptocurrency and legal issues in Vietnam]. *State and Law Review, 4*(384), 30–40. https://vass.gov.vn/nghien-cuu-khoa-hoc-xa-hoi-va-nhan-van/Tien-ao-va-mot-so-van-de-phap-ly-114#_ftn10
50. Desnoyers, S. (2013). *The challenges of cybercrime for international law enforcement*. Utica College.
51. Vietnam Ministry of Foreign Affairs. (2017). *Danh muc cac hiep dinh ve tuong tro tu phap va phap ly giua Viet Nam va cac nuoc* [List of treaties of mutual legal assistance and legal issues between Vietnam and other countries]. https://lanhsuvietnam.gov.vn/Lists/BaiViet/Bàiviết/DispForm.aspx?List=dc7c7d75–6a32–4215-afeb-47d4bee70eee&ID=414. Accessed 8 Mar 2020
52. Heusala, A.-L., & Koistinen, J. (2018). 'Rules of the game' in cross-border cooperation: Legal-administrative differences in Finnish-Russian crime prevention. *International Review of Administrative Sciences, 84*(2), 354–370. https://doi.org/10.1177/0020852315625786

53. Brier, J. (2017). Defining the limits of governmental access to personal data stored in the cloud: An analysis and critique of Microsoft Ireland. *Journal of Information Policy, 7*, 327. https://doi.org/10.5325/jinfopoli.7.2017.0327
54. Schwartz, P. M. (2017). Legal access to the global cloud. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3008392
55. INTERPOL. (n.d.). *What is INTERPOL?* https://www.interpol.int/Who-we-are/What-is-INTERPOL
56. HTCP Department. (2016). *Bao cao tong ket nam 2016* [Annual report 2016]
57. Department of Cybersecurity and Combating High-tech Crime. (2018). *Bao cao tong ket nam 2018* [Annual report 2018]. Hanoi.
58. Lam, T. (2020). *Bao dam an ninh mang trong tinh hinh moi* [Ensure cybersecurity in the new situation]. Vietnam Communist Party's Central Committee. Retrieved from https://www.tapchicongsan.org.vn/web/guest/tin-tieu-diem/-/asset_publisher/s5L7xhQiJeKe/content/bao-dam-an-ninh-mang-trong-tinh-hinh-moi
59. Dai, Q. T. (2015). *Khong gian mang: Tuong lai va hanh dong* [Cyberspace: Future and action]. Public Security Publishing House.
60. Chinh, N. M. (2019). *Hoan thien phap luat ve an ninh mang trong tinh hinh hien nay* [The improvement of law on cybersecurity in the present]. Vietnam Communist Party's Central Committee. https://tapchicongsan.org.vn/the-gioi-van-de-su-kien/-/2018/812604/hoan-thien-phap-luat-ve-an-ninh-mang-trong-tinh-hinh-hien-nay.aspx#!
61. Dong, A. (2020). *Truyen thong, an ninh mang va luat phap* [Media, cybersecurity and law]. The Communist Party of Vietnam. https://nhandan.com.vn/binh-luan-phe-phan/truyen-thong-an-ninh-mang-va-luat-phap-579963/
62. Hoa, N. T. N., & Long, B. T. (2020). Nhin lai mot nam thuc hien phap luat ve an ninh mang [One year of implementing the law on cybersecurity]. *Political Theory Journal*, *4*, 93–99. Retrieved from http://lyluanchinhtri.vn/home/index.php/thuc-tien/item/3172-nhin-lai-mot-nam-thuc-hien-phap-luat-ve-an-ninh-mang.html
63. Cooper, G., & Le, H. (2018). *Vietnam's new Cybersecurity Law: A headache in the making?* Duane Morris, pp. 14–16. https://www.duanemorris.com/articles/static/cooper_le_cybersecurity_practitioner_0718.pdf
64. SaveNET. (2018). *Luat an ninh mang: Nhung dieu can biet* [Law on cybersecurity: Basic knowledge].