Understanding Cybercrimes in Vietnam: From Leading-Point Provisions to Legislative System and Law Enforcement

Hai Thanh Luong[1]
Duy Tan University, Vietnam;
RMIT University, Australia

Huy Duc Phan[2]
Monash University, Australia

Dung Van Chu[3]***, Viet Quoc Nguyen***[4]
Ministry of Public Security, Vietnam

Kien Trung Le[5]***, & Luc Trong Hoang***[6]
People's Police Academy, Vietnam

Abstract

Cybercrimes are growing in Vietnam to pose a number of complicated modus operandi with its sophisticated activities. Dealing with cybercrime's threats is challenging when Vietnam has still lacked manpower policies and professional technologies. As the first specific analyses to focus on Vietnam's context, this paper discusses the efforts taken by the Government of Vietnam to deal with these concerns. Using grey literature with a number of official data and Vietnamese reports, the authors analysis leading-point provisions of Vietnam in combating high-tech crimes and assess legislative frameworks as well as the role of law enforcement authorities. It argued that under distinguished features of communist country, top-and-down organizational model of law enforcement to prevent and combat cyber-related crimes are still effective. To end, some recommendations and call for further researches in the related field in Vietnam will also encourage for scholars, law enforcement, and policymakers.

Keywords: Cybercrime, Law Enforcement, High Tech Crime Investigation, Vietnam.

[1] Institute of Research and Development, Duy Tan University, Da Nang 550000, Vietnam. Email: luongthanhhai1@duytan.edu.vn; Honorary Principal Research Fellow, School of Global, Urban and Social Studies, RMIT University, Melbourne, Vic 3000, Australia. Email: haithanh.luong@rmit.edu.au

[2] PhD Candidate (criminology), School of Social Science, Monash University, Clayton, Vic 3000, Australia. Email: duc.phan@monash.edu

[3] Deputy Director of Department of Criminal Investigation, Ministry of Public Security, Hanoi 100000, Vietnam. Email: chuvandung68@gmail.com

[4] Specialist, Department of Cybersecurity and High-Tech Crime Prevention, Ministry of Public Security, Hanoi 100000, Vietnam. Email: vietmps@gmail.com

[5] Deputy Dean, Faculty of Postgraduate, People's Police Academy, Hanoi 100000, Vietnam. Email: luathinhsu77@gmail.com

[6] Deputy Dean, Faculty of Forensic Science, People's Police Academy, Hanoi 100000, Vietnam. Email: hoangluchvcsnd@gmail.com

Introduction

Information and communication technology (ICT) bring huge advantages to our daily lives. Individuals can use the Internet for shopping, money transferring and many other activities while staying at their own houses. Governments and business also take advantages of technology to govern and develop economy as well as ensure social order for people's lives. However, the development of ICT also poses threats to safety of people in the world when criminals can use technology to commit many types of crimes such as fraud and scams. These activities are often referred as cybercrime, which is an emerging threat to all country. Meanwhile, almost Western countries, Southern Asia and Northern Asian have invested and developed considerably their legal frameworks and strong enforcement to prevent and combat it, most countries in the Mainland Southeast Asian region, including Cambodia, Laos, Myanmar, and Vietnam has been relatively little and limited among institutions which establish their sustainable strategies to fight cybercrime and its related concerns. It is more likely to lead these countries not only become vulnerable targets of offenders to attack, but also face to cause the damage of billions of dollars annually. Paradoxically, the research in relation to these concerns are still lacking to focus at those countries that lead to limitedly understanding their current situation with global readers.

In the 'Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime' both Ngo and Jaishankar (2017) called for further researches and share information about trends and patterns of cybercrime in developing countries. Among of five interested issues form Ngo and Jaishankar' proposals, including Area 2: Assessing the Prevalence, Nature, and Trends of Cybercrime and Area 4: Documenting Best Practices in Combating and Preventing Cybercrime, we would like to introduce and analysis the Vietnam's perspective, a communist country in the Southeast Asian region, to prevent and combat cybercrime. Although this topic is not new phenomena in the world, in the Southeast Asian context in general and Vietnam in particular are lack of academic assessment. Thus, within the scope of paper, we want to focus on Vietnam's policies to deal with this type of crime as the first research's approach. The main aim of paper is not only to identify the trends and its related activities of cybercrime in Vietnam but also to share Vietnam's ideologies and their measures to enhance the effectiveness of combating cybercrime.

1. Cybercrime: A Controversial Debate

To turn back the early 1980s when the personal computer workstations born and its related applications, particularly with the introduction of the 'world wide web' in 1991, the transformative effect of ICT have been becoming as a 'double-edged sword' (Broadhurst & Chang, 2012; Grabosky & Smith, 2017; Hill & Marion, 2016; Owen, Noble, & Speed, 2017). Alongside with apparent contributions in the variety of aspects, there are a number of the inconveniences of computer-related crimes, known as cybercrime. It is a clear point that cybercrime has become a world concern and according to unofficial statistics, the projected loss of cybercrime will reach USD 6 trillion by 2021, up from USD 3 trillion in 2015 (Cybersecurity Ventures, 2017). Consequently, it influences, either directly or indirectly, not only personal but also corporates and nations

as a whole. Although it is considered as one of the specific types of transnational organized crime with its unpredicted impacts on politic, economic, culture, society and even national security as well as international relations, no official definition of United Nations Conventions identifies and concepts exactly about cybercrime and its related contents. Even, many new terminologies and conceptions have approached in this new realm of cyberspace in the last decade after Wall (2004) question 'what are cybercrimes?' To some extent, unfortunately, there is sometimes disagreement over the precise meanings of some of these conceptions and terminologies, and they are used inconsistently and integrated approaches (Clough, 2011; Gercke, 2012; Gordon & Ford, 2006; Grabosky, 2004, 2007; Hill & Marion, 2016).

The term cybercrime stemmed from the concept 'cyberspace' given by Gibson (1995, p. 51), who defined 'consensual hallucination that was computer-generated construct representing abstract data'. Based on this term, a list of terms with 'cyber-' prefix was created such as 'cyberworld', 'cyber-attack', and 'cybercrime' in which the 'cybercrime' term is used synonymously with 'computer crime', 'high-tech crime', 'digital crime', 'electronic crime' and 'technology-enabled crime' (Gibson, 1995; Grabosky, 2004; Wall, 2004). It refers to any acts, intentional or unintentional activities, that involve criminal uses of the Internet or specific software and other networked systems, depending on each national criminal code's regulations, to cause harm to others or some form of a disturbance to commit a different criminal offense. After nearly one and half decades when Wall and others raise the question 'what are cybercrimes?' until present, many scholars and policy-makers assumed that cybercrime are not only new types of crimes committed directly against computers and computer systems such as illegal access or denial of service attacks but also traditional crime abusing the advancement of computing technology such as theft of intellectual properties, online fraud, trafficking in child porn, money laundering and denial-of-service attacks (Grabosky, 2017; Grabosky & Smith, 2017; Hill & Marion, 2016; Owen et al., 2017).

In the field of policing and criminal justice, almost scholars and policymakers have often recognized that each development's approaches of cybercrime definition are remarkably influenced by experience of law enforcement officers, victims and researchers. Therefore, it has been diversified into a number of explanations. Based on the level of involvement of technology in cybercrime, Gordon and Ford (2006, p. 14) expressed 'cybercrime' as: "any crime that is facilitated or committed using a computer, network, or hardware device". Accordingly, Gordon and Ford (2006) categorized cybercrime into two types: the first type is charactered by a more technical nature, for example hacking and phishing, and second type have greater participation of human in its commission, such as child predation. Notwithstanding, both these authors assumed that there are rare cases where cybercrime is merely type I or Type II. A quite similar approach with these scholars, Choo (2008) separated clearly three typologies of organized crime groups in cyberspace which they exploit advances in ICT to breach legal and regulatory controls, including (1) traditional organised criminal groups which make use of ICT to enhance their terrestrial criminal activities; (2) organised cybercriminal groups which operate exclusively online; and (3) organised groups of ideologically and politically motivated individuals who make use of ICT to facilitate their criminal conduct. On the other hand,

relying on the role of computers in the commission of crimes, Grabosky (2007) classified cybercrime into three categories: (1) crimes where computer is the device to commit crime such as phishing, producing and disseminating child pornography materials; (2) crimes where computers are the object of criminal conducts such as a denial of service attack; and (3) crimes where computers are related to the offence (e.g. Computers store records related to a network of drug trafficking). With a similar perspective, Clough (2011) argued that cybercrime is not a fixed definition but a descriptive term used emphasize the involvement of technology in the process of committing crime.

Again, paradoxically, though there are a number of related conceptions and its relevant understood from different views, till date there is not any common agreed definition of cybercrime. A recent publications of latest literature of scholars and policy-makers also mentions over 30 various types of offenses that fix up with the umbrella of cyber crime's approaches, including 'hacking, malware, identity theft, online fraud, credit card fraud, spamming, web and email spoofing, dating scam, cyberbullying, harassment and stalking, and distributed denial of service attacks' (Ngo & Jaishankar, 2017, p. 2). Both Ngo and Jaishankar (2017, pp. 3-4) state that there are at least three obvious reasons to lead that defining and classifying the different types of cybercrime is a salient and pertinent area of inquiry, including the role of common language to define it, the significance of a clear definition to determine the scope of research, and the effectiveness of different aspects of cybercrime to assist law enforcement and criminal justice agencies to prevent and combat it. To some extent, these reasons are likely to put the concept of cybercrime a close relationship with new norms such as 'cyber criminology' (Jaishankar, 2007), 'digital criminology' (Stratton, Powell, & Cameron, 2017), or 'virtual criminology' (Brown, 2012; Owen & Owen, 2017) which are still calling for further research, both theory and practice, in the next steps.

2. Two in One: Cybercrime's Features in Vietnam

Vietnam is a country with a highly increased number of users of Internet and technology. With nearly 50 million internet users (around 52% of the population), Vietnam is ranked 17th in 20 countries with the highest number of internet users in the world according to the latest ranking published in March, 2017 (Internet World Stats, 2018). Also, online public services and e-government in Vietnam have been expanded. Many public services have been conducted via the Internet such as e-tax, e-customs, import and export procedures and e-business registration. E-commerce and online payment are more and more common in Vietnam. However, the rapid boom of information technology, telecommunications and the Internet also brought about the threat of cybercrime in Vietnam. According to the Internet Security Threat Report 2018 of Symantec Cooperation, Vietnam is one of the top 10 countries affected by targeted attacks, particularly with Internet of Thing in the period of 2015-2017 (Symantec, 2018). Additionally, in the Global Security Index 2017 (GSI), which based on countries' legal, technical and organizational institutions, their educational and research capabilities, and their cooperation in information-sharing networks, the International Telecommunication Union (2017) also refers that Vietnam's cybersecurity has been ranked 101st out of 195 countries compiled by the United Nations International Telecommunication Union,

while regional peers Singapore and Malaysia made it into the top 20 as leading countries in this field.

It is hard to calculate the number of cybercrimes occurring in fact in Vietnam due to the number of underreported cases is remarkable. Besides, Vietnam has not conducted any survey on crime at national level like the other countries such as Australia with Crime Victimization Survey conducted by the Australian Bureau of Statistics or the Crime Survey for England and Wales implemented by Kantar Public on behalf of the Office for National Statistic. All statistics on cybercrime in Vietnam produced to date are prepared by Vietnam law enforcement agencies based on the discovered cases and the arrested perpetrators as well as some particular case studies will be posed by social media alongside with authority's investigative process. Notwithstanding, most Vietnam criminologists, law enforcement agencies and other organizations have the common judgment that the situation of cybercrime in Vietnam is more and more complicated in recent years.

2.1. Attacks against websites and computer system

Attacks against websites and computer system, including direct and indirect actions, have been becoming increasingly to evolve with diverse methods and tricks in almost countries, particularly at weak infrastructure of ICT, and Vietnam is not except for example in the Southeast Asian region. The activities of virus and spy software spreading have grown with its various forms and methods. In which, spy software is sophisticatedly coded in order to avoid being detected by users. The hacker often spread virus and spy software through email, sexual website, society forums and network especially through cell phone application.

In the latest Security Intelligence Report (SIR) of the Microsoft (2017) alarmed that Vietnam belonged to the top ten countries in the world with the highest malware encounter and infection rates in the three continuous months from January to March 2017. Yet, the highest numbers of suspected botnet1 IPs, spam sending, and for dictionary attacks is also call for Vietnam's situation in the period of 2016- 2017 (Microsoft, 2018; Symantec, 2018). A Microsoft survey has found that Vietnam is among the countries most vulnerable to a mass cyber-attacks; nearly half of computers were found to contain malware. The SIR v21, or Microsoft's Security Intelligence Report volume 21, was released recently showing that 20 percent of at least 100,000 computers in Vietnam were infected with Prepscam, which is often distributed as a mountable .iso disk file containing a software installer (Microsoft, 2016). Vietnam was listed among the five countries with the highest encounter rates in the world, along with Pakistan, Indonesia, Myanmar, and Mongolia (Microsoft, 2016, 2017). Accordingly, Vietnam also was recorded as the second rank countries, lower than China, was attacked by Sigru virus which can stop some files from working correctly in Windows XP and the rest of earlier operating systems (Microsoft, 2016, pp. 79-80).

According to the Department of High Tech Crime Investigation (2017), in Vietnam, only the first 6 months of 2016, 127,630 network security incidents occurred, triple that figure of 2015. The targets of these attacks are websites and data centers of government agencies, big corporations and banks. In which, there were 8,758 phishing cases, 77,160

deface incidents and 41,712 cases related to malware and at least there were 3225 websites in Vietnam hacked, including 331 websites of education and 177 websites of government agencies. As Hill and Marion (2016, p. 11) argue that each cyber-related criminal is different types and also has a different motivation for his or her illegal activities in the reality to 'commit crimes on the Internet to achieve many goals'. To some extent, in these Vietnam's cases, the purpose of network attacks is to steal, modify and delete valuable data, change the interface of the websites or make the websites overloaded. In additional, in some sensitive cases, 'black-hat hackers' utilized cyberspace to attack national security or civil administrative system with the purpose for implementing their political motivations as a way to get attention for their cause, show their pathways for a particular cause, raise donations, or persuade society to involve their group (Broadhurst & Chang, 2012; Chang, 2017; Choo, 2008; Hill & Marion, 2016; Owen et al., 2017). Especially, the information systems of the two biggest airports of Vietnam, Noi Bai and Tan Son Nhat airports were hacked in 2016. The Civil Aviation Administration of Vietnam reported several attacks, supposedly from 1937cn team, on these two Vietnam airports within the same day (Balduzzi, Flores, Gu, & Maggi, 2018). The IT system for the check-ins of Vietnam Airlines at Tan Son Nhat International Airport was attacked and stopped working. The deface page, which was the same page used on the Vietnam Airlines website, replaced the flight information screens at Noi Bai International Airport by a picture with words insulting Viet Nam and the Philippines regarding the East Sea dispute. The website was recovered at 5.10pm, but a huge amount of private information of the customers was stolen and made public on the Internet and even, the attack caused the delay of 100 flights, affecting thousands of passengers (Balduzzi et al., 2018, p. 48).

2.2. Identity-related Crimes

Alongside with practical target attacked by 'black-hat hacker' on hardware system and its related infrastructures, Vietnam has also been facing to become a potential market of high-tech offenders to use the Internet and its social websites to commit identity-related crimes. In fact, Vietnam has witnessed the boom of identity crime in recent years with the nature and scope of modus operandi more complicated and sophisticated. Identity theft and trading credit card information on underground forums to make counterfeit card and buy goods from online store has increased in recent years. The weakness and looseness to control and manage ICT system, particularly in mobile phone's numbers, are identified as one of the main causes to lead difficulties and barriers to ensure private information. Buyers only need to spend about 1 million VND (around USD 50) to purchase a list of 1500 names, addresses and mobile numbers of clients of Mobifone, Vinaphone and Viettel mobile networks (Duc, 2014; Giam, 2014). In addition, a lot of foreigners entered Vietnam with intent to commit identity fraud and they brought equipment to produce fake credit cards and personal information they had stolen to make payment via wireless EFTPOS machines or withdraw money directly (Duc, 2014; Van, Uyen, & Phuong, 2015). One of the new and complex tricks in the payment process is to make a website, send a phishing link to victims then illegally acquire banking account and transfer money to accounts of the perpetrators (Department of High Tech Crime Investigation, 2017). Cybercriminals also exploit vulnerabilities in the banking system to conduct a lot of

transactions at the same time through Internet banking systems to appropriate money (Anh, 2014; Van et al., 2015). Accordingly, they created fake websites with the interface and the domain name similar to the real bank website, but containing viruses, malware with a view to appropriate account information of customers (Candice, 2017; Van et al., 2015). Criminals also have the ability to listen to voice calls, hack camera systems to steal personal information, especially social network accounts and bank accounts (Department of High Tech Crime Investigation, 2017).

Currently, online fraud is one of the common cybercrime types in Vietnam. According to official documents of anti-cybercrime police force, in recent time, a number of foreigners colluded with Vietnamese offenders with the purpose for making phone calls to victims and cheat them to transfer money to their bank account (Department of High Tech Crime Investigation, 2018). In particular, perpetrators designed e-commerce websites for illegal business, such as advertising discounted goods but sending inferior goods or smuggled or prohibited goods in order to gain profits. Some fraudsters pretend to be foreigners to make friends with victims and additionally, they make victims believe that they will send gifts to them and ask them to pay tax to complete the custom procedures (Duc, 2014; Nghia & Binh, 2014). Of course, however, after receiving money from victims, the fraudsters are out of communication with victims. Other fraudsters set up email accounts like the emails of business partners of targeted companies and send emails requesting the companies transfer money under the business contract to their perpetrators' accounts (Danh & Arun, 2018).

2.3. Others?

The status of illegal gambling, especially football betting, continues to take place publicly in various forms. Particularly, overseas bankers often hook up with Vietnamese gangs to build large gambling networks for both Vietnamese and foreigners, which it is estimated that millions of dollars flowing abroad through gambling activities every day. The illegal trading of online games has increased with turnover reaching trillions VND. Currently, there are over 500 online games released in the Vietnam market, of which more than 200 online games are operating illegally (Department of High Tech Crime Investigation, 2018). In particular, in the few recent years, online gambling activities are more and more complicated under many forms via colluding among local and foreigners to make an online network. According to LEAs of Vietnam, there are many Vietnamese individuals cooperate with their foreign conspiracies to set up gambling websites to attract gamblers to involve a number of illegal games (Department of High Tech Crime Investigation, 2018; VNS, 2018). In fact, during the recent one decade, when Vietnam became a potential investment's target to develop economically, many foreign criminals have entered Vietnam under cover of various backgrounds such as investors, businessman, tourists, and students, operating mostly in economic hugs, metropolitan cities, and border provinces. Among those offenders are come not only from the Southeast Asian region but also involving African criminals, namely Nigeria, Congo, Ghana, Cameroon, and South Africa (VLLF, 2018).

Regarding illegal gambling online activities, Vietnam Police have blocked almost hundreds of gambling websites, detected and investigated many cases, operations as well as arrested a lot of gamblers (Asian Times Staff, 2018a; VNS, 2018). However, lacking international legal framework, especially bilateral treaties in mutual legal assistance and extradition between Vietnam and their partners and consequently, in many cases, cooperating to track down fugitives and to arrest perpetrators is not successful or even cannot be applied (Department of High Tech Crime Investigation, 2018; VLLF, 2018). The various criminal's backgrounds include foreigners and law enforcement officers to lead the complications, difficulties and barriers in the process of investigation of authorities. The most typical case to prove this concern was investigated successfully by Phu Tho Provincial Police Department and Ministry of Public Security in last year when they dismantled the most prominent online gambling syndicate, worth the US $426.3 million, and prosecuted at least 92 people to court, whose faced a total of seven criminal offences under the 2017 Criminal Code of Vietnam, namely organizing gambling activities and purchasing fake invoices to money laundering, bribing and abuse of power (Ba, 2018; VNS, 2018). According to investigators, this ring on web portals Rikvip/Tip.club had established an extensive network of 25 'tier 1 agencies' and nearly 5,900 'tier 2 agencies' with approximately 43 million account users since being operated in mid-2015 (Ba, 2018; Department of High Tech Crime Investigation, 2018). Sadly, among those offenders, there are two senior police officers in the field of anti-cybercrime criminal investigation to involve and corrupt in this online gambling ring, whose sentenced to 9 and 10 years in prison (AFP, 2018; Asian Times Staff, 2018b; Department of High Tech Crime Investigation, 2018; Khanh, 2018).

In addition, the dissemination of pornography, prostitution advertisement, sensitive photos to humiliate victims tend to increase. The pornography websites have attracted hundreds of thousands of visitors daily. Particularly, there has been the spread of child pornography through social networks by Vietnamese people. Furthermore, copyright infringement is becoming a major concern and even, Vietnam is one of the countries with high infringement rates in the world (U.S. Department of State, 2017).

It is clear that cybercrime in Vietnam has been growing rapidly in various forms with a large number of serious cases occurred in recent years. It has been causing devastating damages to the Vietnam government, enterprises and people. Especially, Vietnam has gradually become a choice of transnational cyber criminals when they intend to commit cybercrime.

3. Vietnam's Responses to tackle Cybercrimes

To confront this complicated situation of cybercrime in Vietnam, Vietnam Communist Party and Vietnam government have issued directives to mobilize the power of all political system in the fight against cybercrime. To implement the policy on cybercrime, the Ministry of Public Security (MPS), the main body in charge of crime prevention and suppression in Vietnam, has conducts many appropriate measures to prevent, detect and suppress cybercrime in Vietnam. However, there have not been any research projects or academic papers analysing comprehensively the trends of cybercrime in Vietnam, laws on cybercrime and how laws on cybercrime have been implemented by the MPS. Thus,

there is a room for such this paper to provide a better overview on the work of combating cybercrime in Vietnam. Since then, some recommendations can be given to improve this work in the future.

a. Leading-Point Provisions

As one part of institutional society of communist countries, according to current constitution of Vietnam, the Vietnamese Communist Party (VCP) is the highest-ranking leading sector and impact on all field and subject. Accordingly, VCP also orient and regulate most activities, structure, and responsibilities of public security's forces to protect national security and maintain social order, including ensuring safety on cyberspace. Indeed, the problem of cybercrime has received attention from the Politburo and the Central Committee of the VCP since early years of 21st century. On 22nd October 2010, the Politburo of the VCP issued the instruction number 48-CT/TW on "Enhancing the Party's leading position in the work of combating crime in new era". Under the direction of the VCP, the Government also issued the document to direct the work of combating cybercrime at national level. On 10th June 2011, Vietnam Prime Minister Nguyen Tan Dung signed Directive Number 897/CT-TTg dated 10th June 2011 on "implementing measures to ensure cybersecurity". The Directive required all Ministries and bodies of the Government, provinces and cities to take all appropriate measures to prevent virus and malicious programs and protect the information system. Besides that, to enhance the work of protecting online safety, on 16th September 2013, Secretariat of the VCP's Central Committee issued the Direction number 28-CT/TW with the purpose for developing and publishing law on information safety and guiding documents in the direction of responsibility for ensuring the safety of information for organizations or individuals as well as dealing to information security violations. Among of authorities, the importance of the duties of combating cybercrime were emphasized to public security's agencies. In order to have a more powerful policy on cybercrime, on 7th April 2014, Prime Minister issued Decree number 25/2014/NĐ-CP to prescribe the Prevention and Combat of Cybercrimes and Other Law Violations Involving High Technology. In which, Article 5 of the Decree set out the policy of government on cybercrime and other violations using technology. Accordingly, Vietnam's authorities will focus on:

1. To invest special-use modem technical equipment and facilities and mobilize scientific and technological potential for specialized agencies to fulfil the tasks of preventing and combating crimes and other law violations involving high technology.

2. To prioritize the selection of officers and attract specialists excellent at information and telecommunications technologies to serve the prevention and combat of crimes and other law violations involving high technology; to provide training and retraining for specialized officers to improve their professional qualifications, legal knowledge, foreign language, knowledge about and skills of using hi-tech means and equipment; to appoint officers who satisfy criteria of political and moral qualities and professional qualifications for domestic and overseas training in the prevention and combat of crimes and other law violations involving high technology.

3. To ensure funds for the prevention and combat of crimes and other law violations involving high technology

The Decree stipulates responsibilities of agencies, organizations, enterprises and individuals in the prevention and combat of cybercrime such as the MPS, the Ministry of National Defense, the Ministry of Justice, the Ministry of Information and Communications and other relevant agencies. In which, the MPS assumes the prime responsibility for, and coordinates with related ministries and sectors in, assisting the Government in organizing, monitoring, directing and guiding the prevention and combat of crimes and other law violations involving high technology (Article 18). The Decree marked an important step in the development of policy on cybercrime.

b. Legislative reflections

As compared to other traditional types of crime such as burglaries, murders, and drug-related crime, 'cybercrime' is relatively a newer concept in Vietnam. It has been mentioned by scholars and lawyers especially since 1997 when Vietnam established its first Internet service provider. During 1990s, as the crimes related to online activities started emerging resulting in the need to create a criminal code to address these activities, Vietnam added "Cybercrime" as one of the crimes in its Criminal codes. The Criminal Code No. 15/1999/QH10 or Criminal Code of Vietnam 1999 (CCV) that was passed by Vietnam National Assembly on 21st December 1999 criminalized some types of cybercrime for the first time.[7] Although there was a number of practical gaps in meaning and its related application in term of cyber offences at that time, it is noted that these articles were mechanically inherited from Russian laws by Vietnamese lawmakers (Anh, 2014). As a result, these articles were so vague and ambiguous that there was no case prosecuted under these articles between 1999 and 2008 (Duc, 2014; Giam, 2014). Therefore, on 19th June 2009, law 37/2009/QH12 passed to amend and supplement the 1999 CCV. The new law slightly amended the contents of these three articles and added two new articles related to cybercrime.[8]

[7] In which, three articles of Chapter XIX on 'Crimes of Infringement upon Public Safety' mentioned criminal activities related to computers:

- Article 224. Creating and spreading, scattering electronic virus programs,
- Article 225. Breaching regulations on operating, exploiting and using computer networks.
- Article 226. Illegally using information in computer networks

[8] Thus, Criminal Code 1999 (amended and supplemented in 2009) had 5 articles on cybercrime including:

- Article 224. Spreading computer viruses and programs with a feature of harming the operation of computer networks, telecommunications networks, Internet and digital devices
- Article 225. Obstructing or disordering the operation of computer networks, telecommunications networks, Internet and digital devices
- Article 226. Illegally uploading information onto or using information on computer
- Article 226a. Illegally accessing computer networks, telecommunications networks, Internet or digital devices of other persons.
- Article 226b. Using computer networks, telecommunications networks, Internet or digital devices to appropriate property.

Law 37/2009/QH12 made the three articles 224, 225 and 226 much stronger over its original version by supplementing the 'objectivity' of crime including computer networks, telecommunication networks, internet and digital devices; the addition of specific criminal conducts as well as the element of damages. The Articles 226a and 226b were also added to deal with the appearance of new modus operandi of cybercrime at that time. These five provisions set the base for investigation, prosecution and trial against hundreds of cybercrime cases from 2009 to 2017 (Department of High-Tech Crime Investigation, 2018). However, the disparities were confirmed as many Vietnamese criminologists and law enforcement officers stated that the implementation of this law had such serious loopholes that if their enforcement solely rely on it, a good percentage of cybercrime cases cannot be investigated and prosecuted properly (Anh, 2014). Indeed, the majority of cybercrime cases (80%) were prosecuted only under 226b; some cases were prosecuted under 226a (Department of High Tech Crime Investigation, 2017; Internet World Stats, 2018). There were no cases prosecuted under the Articles 224 through 226 although harmful activities such as spreading virus and denial of service attacks occurred more and more seriously. The main reason for this situation is that these articles considered the seriousness of damages caused by cybercrime as a compulsory factor to accuse criminals, but the investigation agencies struggled to detect the exact costs of the crimes. As a result, a large number of cybercriminals fell outside the scope of prosecution.

In order to solve this problem, during 2012, Joint Circular number 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC was combined by Ministry of Public Security (MPS), Ministry of Defence, Ministry of Justice, Ministry of Information and Communications, Supreme Procuracy and Supreme Court refer and guide the application of provisions on crime involving information technology and telecommunications. Accordingly, this Joint Circular provided explanation for some contents of the articles such as 'harmful computer program', 'digital data', 'computer network', 'causing serious consequences' and 'earning huge illegal profit'. In fact, to some extent, it partly addressed some problems of the 1999 CCV (amended and supplemented in 2009) but it is precedence in the 2015 CCV.

On 27th November 2015, Criminal Code No. 100/2015/QH13 or CCV 2015 was passed by the Vietnam National Assembly to substitute for the Criminal Code 1999 (amended and supplemented in 2009). This law with the highest number of provisions related cybercrime addressed various acts of illegal online and computer-related criminal activities and endeavoured to criminalise most of the cybercriminal activities, which affected Vietnam in recent years. It was supposed to come into force from 1st July 2016 to replace the 1999 CCV (amended and supplemented in 2009).[9] However, prior to that

[9] Ten articles on cybercrime was set by the 2015 CCV including:

- Article 285. Manufacturing, trading, exchanging, giving instruments, equipment, software serving illegal purposes
- Article 286. Spreading software programs harmful for computer networks, telecommunications networks, or electronic devices
- Article 287. Obstruction or disturbance of computer networks, telecommunications networks, or electronic devices

many mistakes were detected and the implementation of CCV 2015 was not determined until the National Assembly finished the revision of this criminal code again. On 20th June 2017, Law No. 12/2017/QH14 on Amending and Supplementing Some Provisions of the 2015 CCV passed and it set to go into effect in 1st January 2018 as the starting date of this Code. The new law abolished Article 292 as it was strongly criticised for discouraging start-up companies that conduct online business. However, this law did not change the content of any other nine articles.

In the 2015 CCV contains two distinguished parts, namely General Provisions and Criminal Offences. 'General Provisions' include general definitions, criteria for exemptions from criminal responsibility and sentencing guidelines; meanwhile, 'Criminal Offences' section is divided into chapters pertaining to the criminal objects of offenses. In other words, each chapter stipulates offense-causing damages to a type of criminal object that is protected by the Constitution and Vietnam Laws. For instances, Chapter XIII focuses on offenses against national security; Chapter XIV describes offenses against a person and one's reputation. Offenses related to cyberspace are specified in the Section 2 "Offences against regulations on information technology and telecommunications network" of Chapter XXI "Offences against regulations on information technology and telecommunications network". Although the 2015 CCV represents as a big leap towards the fight against cybercrime in Vietnam, but whether or not it is strong enough to deal with the fast-growing threat of cybercrime and what should be done to make it more robust in preventing cybercrime is still questionable. However, the response to this quest cannot be achieved only by exploring cybercrime and its legality within Vietnam region till cybercrime terminologies and aspects pertaining to cybercrime are not scrutinised with international standards. Such comparison is necessary to get some insight about any possible gaps in Vietnamese literature relating to cybercrime and connected facets, based on which some future recommendations can be made to improve the detection and control of cybercrime in Vietnam.

- Article 288. Illegal provision or use of information on computer networks or telecommunications networks
- Article 289. Illegal infiltration into the computer network, telecommunications network, or electronic device of another person
- Article 290. Appropriation of property using a computer network, telecommunications network, or electronic device
- Article 291. Illegal collection, storage, exchanging, trading, publishing of information about bank accounts
- Article 292. Illegal provision of services on computer network or telecommunications network
- Article 293. Illegal use of radio frequencies dedicated to emergency services, safety services, search and rescue, or national defence and security
- Article 294. Deliberate harmful interference of radio frequencies

c. Law enforcement's responses

Under the direction and management of VCP and Government, all appropriate measures have been conducted to deal with the growing threat of cybercrime by the Ministry of Public Security (MPS). To some extent, based on current regulations and official information, this section will analyse the work of law enforcement against cybercrime with three pillar fields: deployment of task force, prevention and investigation, and international relations. By doing this, our presentation will provide the detail of structure, function, and cooperation of Vietnam's counter high-tech crimes police forces at the time.

(i). Establishment of the specialized units

According to Article 4 of Law on the People's Public Security forces number 73/2014/QH13, dated 27th November 2014, the MPS is the body in charge of "protecting the national security, ensuring social order and safety, fighting against crimes". It has specialized standpoints and thoughts of VCP in the Direction number 28-CT/TW (2013), referring the dominated role of public security's agencies to ensure information security and detect any cyber-related crimes. In other words, thus, the MPS is the main actor taking responsibility of preventing and suppressing cybercrime in Vietnam.

Before 2010, there had not been specialized units in charge of combating cybercrime in MPS. This duty had been performed by police units on criminal investigation on economic-related crime police forces. The leaders of MPS recognized that such organizational structure was not strong enough to face with the rapid growth of cybercrime in Vietnam. Therefore, on 4th February 2010, Minister of MPS decided to establish the Department of High-Tech Crime Investigation (DHTCI) under the General Department of Police. This decision marks an important milestone in the fight against cybercrime in Vietnam. The DHTCI is assigned the task of preventing and investigating cybercrime at the national level and also representatives of MPS and Vietnam's government to involve into the Southeast Asian region's forum to prevent and combat cybercrime. To establish police units on cybercrime at the local level, the MPS decided that police teams on cybercrime would be established as part of police divisions which belong to criminal investigation on economic-related crime police force in 31 out of 63 provinces/cities in Vietnam (Department of High Tech Crime Investigation, 2018). Alongside with police forces in DHTCI's field, facing to serious cybersecurity's attacks, particularly in fake news relating standpoints and policies of VCP and Government, in 2014, one independent department in security forces has also established to manage and control information system security and cybersecurity related to sovereignty. However, the same other countries in the Southeast Asia, between cybercrime and cybersecurity are interactions with a number of threats to impact on cyberspace and social order, therefore, in 2018, two above departments merged into department of cybersecurity and high-tech crime prevention police (Department of High Tech Crime Investigation, 2018).

Generally speaking, the specialized force combating cybercrime has been formed from central level to local level since 2010. This improvement in organizational structure has

brought the remarkable results of combating cybercrime investigation that will be presented in next section.

(ii). Cybercrime prevention and investigation

In term of prevention, the DHTCI has advised a lot of agencies, organizations and enterprises of measures to protect the security and safety of important database systems. The DHTCI has actively cooperated with news agencies, social media to propagandize the new tricks of cybercriminals. Also, they have promoted "The Movement of the Entire Population to Participate in the Protection of National Security" in order to raise awareness of people and encourage them to actively provide intelligence about cybercrime (Nghia & Binh, 2014). In 2015, the DHTCI received information about hundreds of incidents via its hotline. It also instructed citizens how to prevent, handle and report cybercrime to the competent authorities when approaching to social networks, online games and the trend of shifting social aspects of social life into cyberspaces.

In term of investigation, DHTCI has put unlimited effort to carry out all professional measures to discover and investigate cybercrime cases. Since 2010, the DHTCI has discovered and verified 1,295 cases related to using technology to commit crime, arrested 1,640 subjects, seized hundreds of billions VND and many exhibits in cybercrime cases (Department of High Tech Crime Investigation, 2017). Hundreds of operations and plans have been conducted to dismantle cybercriminal networks, particularly with professional activities to combat networks of illegal gambling on the internet, in which the DHTCI prevented gamblers from 1,450 websites and diverted over two million attempts to access these websites (Department of High Tech Crime Investigation, 2017). In observation Cybercrime and Cybersecurity in ASEAN of Chang (2017), the author considered that Vietnam had witnessed the boom of identity crime in recent years with the nature and scope of modus operandi more complicated and sophisticated. Particularly, fraudulent activities on the Internet to appropriating properties such as identity theft and trading credit card information on underground forums to make a counterfeit card and buy goods from an online store has increased in recent years (Asian Times Staff, 2018a; VNS, 2018).

Some recent evidences of the Department of High Tech Crime Investigation (2018) pointed out some transnational crime's groups were created by many foreigners collude with Vietnamese offenders to utilize phone calls to victims and cheat them to transfer money to their bank account. In particular, perpetrators designed e-commerce websites for illegal business, such as advertising discounted goods but sending inferior products or smuggled or prohibited goods to gain profits (Duc, 2014; Nghia & Binh, 2014). To do this, the offenders often change their modus operandi to avoid being detected by LEAs via setting up a counterfeiting Website of enterprises to swindle and appropriate money from customers when they charge money by prepaid cards; purchasing online but no goods delivery or delivering bad quality goods (Duc, 2014; Nghia & Binh, 2014; VNS, 2018). By doing this, they can steal and acquire information on credit card holders to draw out money, online purchase air-tickets, goods or online services payment. One of the complicated cases of this cybercrime's type was dismantled by cooperating and collaborating among 52 out of 63 provincial police department to address at least 12 fraudsters, who scammed over 560 victims to appropriate a total of US$1.8 million (Asian

Times Staff, 2018a; VNS, 2018). To contrast, the professional capacity of LEA officers, who are directly involved in combating cybercrimes is limited because this is new area and Vietnam police have not much experience and strong skills (Department of High Tech Crime Investigation, 2018). Besides, the technical equipment is not enough so that the effectiveness of combating cybercrimes is insufficient to support.

In short, the work of combating cybercrime of Vietnam Police force has achieved the remarkable results through building a variety of effective measures to deal with cybercrime. In fact, increasing number of operations carried out and a lot of subject arrested that reflected the effort of DHTCI in combating cybercrime in Vietnam. On the other hand, however, it means that they are also still need more capable abilities and professional skills to enhance their effectiveness to investigate cybercrime's cases due to these crimes will never stand on one modus operandi.

(iii). International cooperation

Due to the borderless nature of cybercrime that is conducted on cyberspace, a large number of cybercrimes involves many different countries. Hence, international cooperation in information exchange and coordinating investigations of such crimes is crucial for every country. Additionally, as the cybercrime police force of Vietnam has been shaped for a short time in comparison with other countries like the United States or Australia, the force can receive support from other countries in term of equipment and experience through international cooperation. From 2010 to 2014, The DHTCI has actively cooperated with foreign law enforcement agencies in verifying and investigating 84 cybercrime cases (Department of High Tech Crime Investigation, 2017). In which, some noticeable cases are as follows:

- In 2012, DHTCI collaborated with the Australian Federal Police in "Trove" Operation against the group of hackers specializing in building servers called CrimeIRC to form a service of identity theft and trading banking information for cybercriminals around the world. The information provided by the Vietnamese side has helped the Australian Police to stop these criminals from being able to obtain about 80 million Australian dollars from the card information.
- In May 2013, DHTCI teamed up with the National Crime Agency (NCA) of the United Kingdom and the Federal Bureau of Investigation (FBI) of the United States to investigate the criminal organization named Mattfeuter using stolen credit card information, arrest Van Tien Tu and his accomplices. This crime group operated from 2005 and caused the financial damage of about $300 million.
- In December 2013, DHTCI discovered the group of Chinese people who entered Vietnam and set up a network for Chinese citizens to gamble online on the website www.cm688.com to avoid the detection of the Chinese authorities. The information provided by DHTCI helped the Ministry of Public Security of China arrest 11 people and seize several servers and exhibits in Foshan City, China.

DHTCI also has cooperated with law enforcement agencies of Russia, Japan, South Korea, Turkey, Czech Republic and Switzerland in information exchange in dozens of cases via Interpol channel. Australian Federal Police assisted DHTCI in the establishment

of the data centre and providing a lot of specialized hardware and software to collect and recover electronic data from computers and mobile devices. India has sponsored PDCI for Indira Gandhi Electronic Data Recovery Centre. Moreover, the United States, Australia, Singapore, Korea, the United Kingdom, France, China and India have also coordinated with PDCI in organizing training courses for the anti-cybercrime police officers.

Conclusion: Challenges Ahead Still

It is clear that ICT and its applications provide enhancement to the variety of positive factors such as economic, society, culture, and development and however it now also offers criminal the means of causing loss and harm to users. This paper has just outlined the cybercrime concerns and the ways that Vietnam has been facing to difficulties and barriers in the process of preventing and combating high-tech related crimes. The past couple of years can be seen as the booming years for ICT and the Internet's applications in the Vietnam, as the one of the highest rates in the Southeast Asian region. We can see the number of Internet users, social pages and its software online to play illegal gambling that have appeared with the unpredicted forms in recent times. Notwithstanding, the digital amazement is also question as a real challenge to Vietnam with its unforeseeable consequences and might hamper the process of industrialization and modernization of Vietnam in the future.

To reiterate that involvement of Vietnamese criminals and foreigner as well in any forms of high-tech related crimes are causing a great image problem to the country and have also led economic loss and security threat to the nation. To put cybercrime under control and prevention, the Vietnam's authorities has created a professional task force in the field of counter-cybercrime in public security and a number of its relevant units, both national and local level, to enforce cyber legislations; proclaimed nine specific articles in the 2017 CCV by the National Assembly for separate chapter in order to investigate and combat cybercrime; and also enhanced to open wider the international law enforcement cooperation in the Asia and Pacific regional and around the world to improve the capacity and effectiveness of applying techniques and skills to deal with the unpredictable operations of cybercrime's activities. It is hoped that these efforts will go a continuous strategy in anticipating and reducing cybercrime to the limitedly negative in Vietnam.

However, as we argue that ICT and in particular the Internet are always invisible and intangible with its diverse and complex applications in the virtual world, especially in the era of 4.0 Revolution. As the above assessed and discussed, the new article in the 2017 CCV in terms of cybercrime's offenses needs to be tested and updated where necessary. At this time, not too much case studies are investigated and prosecuted by law enforcement agencies and criminal justice bodies and thus, the DHTCI and its specific forces must be able to apply these legislations effectively while proving professional knowledge and comprehensive understood on cyberspace scope and its technical skills to collect evidence based on criminal procedure law. In addition, as none of the ASEAN member state is a signatory to the Budapest Convention, Vietnam should be researched carefully and compared relevantly to the current legislative system to forward for joining and signing it in the soon steps. By doing this, Vietnam can boost their contributed role to build and maintain international cooperation, which is a pillar principle highlighted in the

Convention, in the region and beyond. It will be also permitted national legal authorities to involve the international computer crime assistant network via the '24/7 network' (Chang, 2017). Regarding to the effectiveness of law enforcement agencies, as we argued by ourselves that the DHTCI might not always be able to implement an excellent role in preventing and combating cybercrime in one country. It still needs to rely highly and build up the network of closed relationship with other institutions to improve their professional tactics to collect evidence in relation to hacking or other cybercrime activities. To sum, invaluable implementation in combating cybercrime depends very much on the harmonization and integration among legislative system itself, the level of law enforcement authorities to apply it, and contributions in international cooperation's sharing with others.

References

AFP. (2018). Vietnam Arrests Another Police Official over Online Gambling Ring. DailyMail. Retrieved from https://www.dailymail.co.uk/wires/afp/article-5586355/Vietnam-arrests-police-official-online-gambling-ring.html.

Anh, N. N. (2014). Vietnam Law on Cybercrime. Paper presented at the Conference on Theoretical and Technical Problems on Counter-Cybercrime in Vietnam, Hanoi, Vietnam [Vietnamese language].

Asian Times Staff. (2018a). Old Cybercrime Tricks on the Rise in Vietnam. Asian Time. Retrieved from http://www.atimes.com/article/old-cybercrime-tricks-on-the-rise-in-vietnam.

Asian Times Staff. (2018b). Two Top Cops Implicated in $420 Million Online Gambling Ring. Asia Times. Retrieved from http://www.atimes.com/article/two-top-cops-implicated-in-420-million-online-gambling-ring.

Ba, D. (2018). Vietnam to Prosecute Former Senior Cops in Multimillion Dollar Gambling Case. News. 19 July 2018. Retrieved from https://e.vnexpress.net/news/news/vietnam-to-prosecute-former-senior-cops-in-multimillion-dollar-gambling-case-3779966.html.

Balduzzi, M., Flores, R., Gu, L., & Maggi, F. (2018). A Deep Dive into Defacement: How Geopolitical Events Trigger Web Attacks.

Broadhurst, R., & Chang, L. (2012). Cybercrime in Asia: Trends and Challenges. In J. Liu, B. Hebenton, & S. Jou (Eds.), *Handbook of Asian Criminology* (pp. 49-63). New York: Springer.

Brown, S. (2012). Virtual Criminology In: E. McLaughlin & J. Muncie (Eds.), *The Sage Dictionary of Criminology*. London: Sage.

Candice, D. T. (2017). Cybersecurity Governance Framework in Vietnam: State of Play, Progress and Future Prospects. *Asian Research Policy, 8*(1), 86-97.

Chang, L. (2017). Cybercrime and Cyber Security in ASEAN. In J. Liu, M. Travers, & L. Chang (Eds.), *Comparative Criminology in Asia* (pp. 135-148): Springer, Cham.

Choo, K.-K. (2008). Organized Crime Groups in Cyberspace: A Typology. *Trends in Organized Crime, 11*(3), 270-295.

Clough, J. (2011). Cybercrime. *Commonwealth Law Bulletin, 37*(4), 671-680.

Cybersecurity Ventures. (2017). 2017 Cybercrime Report.

Danh, N., & Arun, G. (2018). The Interface between Electronic Banking and Accounting Modules: A Case Analysis of Companies in Vietnam. *Journal of Advances in Management Research*, *15*(3), 241-264.

Department of High Tech Crime Investigation. (2017). Annual Report on Cyber Crime in Vietnam 2016. Retrieved from Hanoi, Vietnam [Vietnamese language, internal document]:

Department of High Tech Crime Investigation. (2018). Annual Report on Cyber Crime in Vietnam 2017. Retrieved from Hanoi, Vietnam [Vietnamese language, internal document]:

Duc, M. N. (2014). Characteristics of cybercrime and Solutions to Enhance Effectiveness of Cybercrime Prevention and Suppression. Paper presented at the Conference on Theoretical and Technical Problems on Counter-Cybercrime in Vietnam, Hanoi, Vietnam [Vietnamese language].

Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. Geneva, Switzerland.

Giam, M. B. (2014). Discussion on Necessary Traits, Ability and Skills of Anti-Cybercrime Police Officers. Paper presented at the Conference on Theoretical and Technical Problems on Counter-Cybercrime in Vietnam, Hanoi, Vietnam [Vietnamese language].

Gibson, W. (1995). *Neuromancer*. London: Harper Collins Publishers.

Gordon, S., & Ford, R. (2006). On the Definition and Classification of Cybercrime. *Journal in Computer Virology*, *2*(1), 13-20.

Grabosky, P. (2004). The Global Dimension of Cybercrime. *Global Crime*, *6*(1), 146-157.

Grabosky, P. (2007). *Electronic Crime*. New Jersey: Pearson.

Grabosky, P. (2017). The Evolution of Cybercrime, 2006-2016. In T. Holt (Ed.), *Cybercrime through an Interdisciplinary Lens* (pp. 15-36). New York: Routledge.

Grabosky, P., & Smith, R. (2017). Cybercrime. In D. Palmer, W. de Lint, & D. Dalton (Eds.), *Crime and Justice: A Guide to Criminology* (5th ed., pp. 243-277). Sydney, Australia: Thomson Reuters (Professional) Australian Limited.

Hill, J., & Marion, N. (2016). *Introduction to Cybercrime: Computer Crime, Laws, and Policing in the 21st*. California: ABC-CLIO, LLC.

International Telecommunication Union. (2017). Global Cybersecurity Index 2017. Retrieved from Geneve, Switzerland:

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

Jaishankar, K. (2007). Cyber Criminology: Evolving a Novel Discipline with a New Journal. *International Journal of Cyber Criminology*, *1*(1), 1-6.

Khanh, V. (2018). Vietnam Arrests Second Senior Police Official in Illegal Gambling Case. Reuters. Retrieved from https://www.reuters.com/article/us-vietnam-police-

arrest/vietnam-arrests-second-senior-police-official-in-illegal-gambling-case-idUSKCN1HD1FI.

Microsoft. (2016). Microsoft Security Intelligence Report. Retrieved from Washington D.C:

Microsoft. (2017). Microsoft Security Intelligence Report. Retrieved from Washington D.C:

Microsoft. (2018). Microsoft Security Intelligence Report. Retrieved from Washington D.C:

Nghia, Q. P., & Binh, H. P. (Eds.). (2014). Principles and Provisions to Prevent and Combat High-Tech Crimes. Hanoi, Vietnam [Vietnamese language]: The People's Police Academy of Vietnam.

Ngo, F., & Jaishankar, K. (2017). Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime. *International Journal of Cyber Criminology*, *11*(1), 1-9.

Owen, T., Noble, W., & Speed, F. (2017). *New Perspectives on Cybercrime*. Cham, Switzerland: Palgrave MacMillan.

Owen, T., & Owen, J. (2017). Virtual Criminology: Insights from Genetic-Social Science and Heidegger. *Journal of Theoretical & Philosophical Criminology*, 7(1), 17-30.

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a 'Digital Criminology'? *International Journal for Crime, Justice and Social Democracy*, *6*(2), 17-33.

Symantec. (2018). Internet Security Threat Report.

U.S. Department of State. (2017). Investment Climate Statements 2017. Washington D.C.

Van, D., Uyen, L., & Phuong, L. (2015). Measuring the Impacts of Internet Banking to Bank Performance: Evidence from Vietnam. *Journal of Internet Banking and Commerce*, *20*(2), 1-14.

VLLF. (2018). Foreigners: On a Crime Spree. Vietnam Law & Legal Forum.

VNS. (2018). Sophisticated Cyber Crime on the Rise in Vietnam. Society. 14 August 2018. Retrieved from https://vietnamnews.vn/society/463726/sophisticated-cyber-crime-on-the-rise-in-viet-nam.html#lKgRWkic0JHQpk03.97.

Wall, D. (2004). What are Cybercrimes? *Criminal Justice Matters*, *58*(1), 20-21.