WASEDA UNIVERSITY

GRADUATE SCHOOL OF ASIA-PACIFIC STUDIES

DOCTORAL THESIS

Analyzing cybercrime networks: Transnational computer fraud in Vietnam

サイバー犯罪ネットワークの解明ーベトナムにおけるトランスナショナル・コンピューター詐欺

Full name:	NGUYEN VAN TRONG
Student ID:	4018S304-8

Chief Advisor:	Prof. MIICHI KEN
Deputy Advisor:	Prof. MITOMO HITOSHI

08/2021

TOKYO, JAPAN

ACKNOWLEDGEMENTS

This study would never have finished without the supports of many noble individuals. First and foremost, I would like to express my sincere and deepest gratitude to my chief advisor, Prof. Miichi Ken, for his tremendous support and guidance throughout the academic journey. I feel proud and grateful as I am his first Ph.D. student. I would also like to express my profound gratitude to my deputy advisor, Prof. Mitomo Hitoshi, for the precious comments and suggestions, especially about designing the thesis as a coherent "story." Besides, I would not have completed the thesis without the academic supports from Prof. Bacon Paul Martyn and Prof. Tanaka Ema. The comments of the guidance committee have helped me find and put "puzzles" into a comprehensive thesis.

My special thanks go to Japan International Cooperation Agency (JICA) and Department of Training - Central Committee of Organization and Personnel of Vietnam for sponsoring my Ph.D. study. I am grateful to Graduate School of Asia-Pacific Studies – Waseda University where I have studied the Ph.D. program for three years. I am really proud of being a student of this prestigious university. Besides, I would like to make a special note of appreciation to the Vietnamese Ministry of Public Security for assisting in data collection. I also sincerely appreciate the support of Pol.Maj.Gen. Prof. Tran Minh Huong, the President, and other police officers at the Vietnamese People's Police Academy, where I work for their assistance in my Ph.D. study.

I also greatly appreciate all my friends at Prof. Miichi Ken's "happy zemi," wherein I have learned much to improve my research. Besides, I cannot forget the support of Vietnamese friends and foreign ones who cheered me up when I met difficulties. In addition, I would like to share my sincere thanks to Japanese people. I have received a lot of warm-hearted emotions from them. Japanese people help me overcome homesickness when living in Japan. Indeed, Japanese people's kindness has become my unforgettable memory of Japan. I wish Japan and Japanese people all the best!

This Ph.D. thesis is sincerely dedicated to my family. I am indebted to my grandmother, parents, and parents-in-law for encouraging me to follow this Ph.D. program. Lastly, and most importantly, I am deeply grateful for the love and loyalty of my wife, Lan Phuong, who has sacrificed a lot for my family. This thesis is also dedicated to my lovely daughter, Cat Tuong, who is looking forward to welcoming me back to Vietnam. My family has inspired and motivated me to complete the Ph.D. research. My family is always in my heart.

CONTENTS

LIST OF PUBLICATIONS INCLUDED AS PART OF THE THESIS

The following papers were written as part of this thesis:

1. Trong Van Nguyen (2020). Cybercrime in Vietnam: An analysis based on routine activity theory. International Journal of Cyber Criminology, 14(1), 156–173, DOI: 10.5281/zenodo.3747516

2. Trong Nguyen & Hai Thanh Luong (2020). The structure of cybercrime networks: Transnational computer fraud in Vietnam. Journal of Crime and Justice, DOI: 10.1080/0735648X.2020.1818605

3. Trong Van Nguyen (2021). The modus operandi of transnational computer fraud: A crime script analysis in Vietnam. Trends in Organized Crime, DOI: 10.1007/s12117-021-09422-1

APPREVATIONS

ASEAN	The Association of Southeast Asian Nations
EUCPN	European Crime Prevention Network
FBI	Federal Bureau of Investigation
GCI	Global Cybersecurity Index
HTCP	High-tech Crime Police
ICT	Information Communication Technology
IP	Internet Protocol
ITU	International Telecommunication Union
LEAs	Law Enforcement Agencies
RAT	Routine Activity Theory
SNA	Social Network Analysis
SOCA	Serious Organized Crime Agency
TCF	Transnational Computer Fraud
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
VNCERT	Vietnam Computer Emergency Team
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

ABSTRACT

Under the serious threats of cybercrime to global security, cybercrime's nature has recently become a focal area within criminology and policymaking. For clarifying crime's nature, the criminal network perspective has an important place in the field of both traditional and cyber criminology. Accordingly, existing research often argues about the nature of cybercriminal groups in comparison to traditional criminal organizations. These studies provide valuable insight into the formation and operation of cybercrime networks; however, the field is relatively underdeveloped—particularly insofar as most works have concentrated on the North American and European contexts. Much of the extant research is based on anecdotal or circumstantial evidence or a broad range of cybercrimes. There is a lack of empirical research on specific cybercrimes like computer fraud, especially in the Asian context.

This empirical study examined the elements of specific cybercrime, especially concerning its modus operandi and structure, and expanded the scope of research to the Asian context. It focused on one specific type of cybercrime, namely transnational computer fraud (TCF) in Vietnam – an emerging cybercrime center in Asia. It aimed to clarify the nature of cybercrime networks implementing TCF behaviors. Hence, by figuring out TCF's nature particularly in Vietnam, the research contributed to a more comprehensive understanding of cybercrime networks in general and then proposed counter-crime strategies. In achieving the objectives, crime script analysis and social network analysis were used for analyzing the data collected from investigation files and interviews with police investigators.

The research first clarified the distinguishable modus operandi of two types of TCF: bank card data fraud and phone scams in the Vietnamese context. Vietnam could become an operational base for both domestic and foreign criminals to conduct TCF. In bank card data fraud, Vietnamese fraudsters can obtain illegal money from foreign victims without crossing geographical boundaries. In contrast, migration is a significant factor of phone scams as fraudsters cross borders to establish criminal networks. There are also certain major differences about the modus operandi between two types of TCF in Vietnam: bank card data fraud requires greater use of technology, and both types involve different roles of Vietnamese and foreign suspects.

The examination of Vietnamese TCF case studies led to demonstrate a more comprehensive understanding of cybercrime networks in general. This study proved that central actors who are vulnerable and strategic positions inside cybercrime networks could keep the role

of core members or recruited enablers. Moreover, this study focused on the transformation of cybercrime networks affected much by technological factors. Cybercrime networks tend to be fluid and have dynamic organizational structures. Although certain characteristics of traditional criminal organizations such as trust, hierarchical structures still can exist inside cybercrime networks, technological factors make them distinctive. Since developing criminal organizations' models is an effective method to understand criminal networks and design countermeasures, this study suggested a novel typology of cybercrime networks that can be applied universally. Based on the clear degree of leadership, cybercrime networks include four types: *swarm networks, distributed networks, single-directed networks,* and *group-directed networks*. The typology indicated that networks with a higher degree of online activity are often constructed more loosely than networks with a lower degree of online activity. Inside high-online networks, there is a lack of clear leadership, and their members can be distributed across various places.

From the findings of this research, policy and practical implications for counter-cybercrime strategies were discussed. Accordingly, recommendations concerning international cooperation, prevention, and investigation measures were suggested. First, international cooperation should be targeted and enduring around "hotspot" countries. Second, TCF can be prevented by adopting situational prevention measures at each stage of crime. Third, vulnerabilities inside cybercrime networks can be exploited to investigate and disrupt criminal networks. Furthermore, future research in the field of cybercrime networks with different sources, research methods, and related contexts was also recommended.

CHAPTER I: INTRODUCTION

1.1. Background and statement of the problem

1.1.1. Background of the problem

The information technology revolution is still in progress across the world. By May 2020, the total number of Internet users worldwide had reached 4.65 billion, accounting for 59.6% of the world population, compared to 4.16 billion Internet users in late 2017 and about 3.89 billion Internet users in mid-2017 (Internet World Stats 2020). The Internet has an unprecedented influence on the economy and other aspects of society worldwide (The Internet Society 2017). On average, the Internet makes up 3.4% of the GDP of the large and developed economies that account for 70% of global GDP (Manyika and Roxburgh 2011). In the US, the 2018 Internet sector contributed about US$2.1 trillion, accounting for 10.1% of US GDP, more than twice the value in 2014 (Hooton 2019). It is argued that the innovation driven by the Internet and modern technology will move from developed areas with strong digital economies in North America and Europe to emerging countries in Latin America, Africa, and Asia (The Internet Society 2017).

The spread of information communication technology (ICT) and the Internet, however, has also caused concerns about cybersecurity, especially cybercrime. With a lack of adequate defenses, a connected system or an Internet user can easily become a suitable target of cybercriminals. As a result, computer fraud, unauthorized access, and other types of cybercrimes occur in a “relentless” and “undiminished” way, resulting in the annual global loss of hundreds of billions of US dollars (Bossler and Berenblum 2019; CSIS and McAfee 2018). Cybercrime ranks third, behind government corruption and drug trafficking, as a global economic scourge (CSIS and McAfee 2018). Cybersecurity Ventures (2017) estimates that the global annual cost of cybercrime will increase to US$6 trillion by 2021, double compared to the value in 2015. Over 23 million pieces of stolen bank cards, of which two-thirds were issued in the US, were offered for sale in the first six months of 2019 (Preminger 2019). Half of the citizens have been targeted by phone scammers in the UK, with 17% of individuals targeted five times or more in two years (Couture and Pardoe 2017).

Cybercrime is one of the fastest increasing forms of transnational crime (INTERPOL 2017). Virtual space can be regarded as one typical example concerning the globalization phenomenon as the physical distance is deleted here (Scholte 2005). Cybercriminals no longer migrate to other countries but still possibly implement cyberattacks targeting foreign victims. Besides, cybercriminals are highly networked and cooperate to commit computer crimes (Hutchings 2014; Lusthaus 2012; Nurse and Bada 2018). McGuire (2012) stated that about 80% of cybercrime is implemented by various forms of organizations. With the high requirement of organizational factors, cybercrime may be carried out to obtain a financial profit by small criminal groups, ad hoc networks, or organized groups on a broader scale (EUCPN 2015).

Located in Asia with the most Internet users of all continents, Vietnam has continued to show phenomenal growth in Internet penetration and the application of ICTs. After two decades since the Internet officially appeared in Vietnam, the number of Internet users reached about 68.5 million in December 2018, equivalent to 70.4% of the population, higher than the global average of 59.6% (Internet World Stats 2020). Vietnam ranks 14th worldwide and third in Southeast Asia, with a high statistic of Internet users (Internet World Stats 2020). According to Resolution 52-NQ/TW (2019) of the Political Bureau of the Party Central Committee, Vietnam has determined to be among the top 40 global countries in the Global Innovation Index rankings, with the digital economy making up 30% of GDP by 2030. To achieve this target, the Vietnamese Government has enacted the regulations and implemented specific policies to ensure cybersecurity, such as the 2018 Law on Cybersecurity, the 2015 Penal Code, the 2015 Criminal Procedure Code, and the 2015 Law on Network Information Security. The assurance of cybersecurity is the priority of Vietnam to construct a digital society (Lam 2020).

However, Vietnam is still regarded as a new center of cybercrime, together with other countries like Brazil, India, and North Korea (CSIS and McAfee 2018). Vietnam is among the nations with the most negative reputations relating to online behaviors such as sources of spam, botnets, malware, and cyberattacks. In Vietnam, many cybercriminal groups have recently been investigated and arrested by high-tech crime police (HTCP). Among them are computer fraud groups in which fraudsters use various techniques to defraud victims. For example, in phishing cases, Vietnamese cybercriminals could attempt to obtain confidential information such as bank accounts' passwords or social networks' login by using fake emails or links supposedly from banks or trustworthy institutions (HTCP Department 2016). Besides, in the *muaban24* case, the online "Ponzi scheme" was utilized to defraud investors of VND631 billion (over US$31.5 million) (HTCP Department 2012). Domestic factors are prominent in these phishing and "Ponzi scheme" cases as fraudsters and victims often are Vietnamese.

Whereas bank card data fraud and phone scams are among the most infamous transnational cases investigated by Vietnamese cyber police. In these cases, fraudsters and/or victims are foreign. Fraudsters conduct cross-border deviant behaviors to obtain victims' money, causing severe consequences. For Vietnamese fraudsters attacking overseas, bank card data fraud has become a common endeavor; Vietnam is one of the top countries in terms of hacking capacities with the local community of "black hat" hackers (Lusthaus 2020). Domestic cybercriminal groups such as *mattfeuter, vefamily, vietexpert,* and *hkvfamily* operated transnationally to obtain bank card data of foreign victims, then used these data for online purchases or making fake cards (HTCP Department 2010, 2011, 2013, 2014, 2015). In May 2013, a US$200 million worldwide credit card fraud ring run by Vietnamese criminals was infiltrated through cooperation between the HTCP Department of Vietnam, the Serious Organized Crime Agency (SOCA) of the UK, and the Federal Bureau of Investigation (FBI) of the US (FBI 2013; HTCP Department 2013). The arrest information immediately appeared in many Vietnamese and international newspapers. Reuters, for example, cited a SOCA official's description of the case as "one of the world's major facilitation networks for online card fraud" (Flitter 2013).

Additionally, phone scams have recently become a serious transnational threat originating from or targeting Vietnam as 65% of computer fraud reports received by Vietnamese police in the first half of 2020 were related to phone scams (Ministry of Public Security 2020). Groups of foreign offenders, mainly from Mainland China, Taiwan, and Korea, entered Vietnam, then set up the calling systems of Voice over Internet Protocol (VoIP) to make fraudulent calls to their countries' citizens (HTCP Department 2014, 2015). In May 2015, for example, the HTCP Department carried out Operation TQ2015 to arrest 24 Chinese and Taiwanese offenders who appropriated about CNY20 million from Chinese victims via phone scams (HTCP Department 2015). Furthermore, Vietnamese offenders have recently cooperated with foreign criminals to increasingly implement phone scams to deceive Vietnamese citizens (HTCP Department 2015, 2016, 2017).

1.1.2. Statement of the problem

To cope with transnational cybercrime, law enforcement agencies (LEAs) need to enhance international cooperation with counterparts and design suitable counter-crime strategies; however, this work is not straightforward (Goodman 2010; Peters and Jordan 2020; United Nations 2019; UNODC 2013). The lack of mutual understanding among countries reduces the efficiency of the global fight against transnational cybercrime (United Nations

2019; UNODC 2013). Besides, conventional counter-crime policies are likely to be ineffective in preventing and investigating cybercrime (Goodman 2010). One of the productive approaches to control cybercrime is to develop a deeper and broader understanding of the nature of cybercrime (Bossler and Berenblum 2019; Leukfeldt, Lavorgna, and Kleemans 2017; Ngo and Jaishankar 2017). The knowledge about cybercrime's characteristics is the foundation for LEAs to develop and carry out counter-cybercrime strategies. Moreover, understanding cybercrime's nature can benefit every individual and organization. They can figure out how cybercrime occurs and protect themselves against cybercrime.

The criminal network perspective, together with its analysis techniques, has been beneficial for studying crime's nature. Rather than clarifying isolated individuals' criminal behaviors, the criminal network perspective views crime as the result of interactions between members within a social context (Morselli 2009). As one actor inside the society, a criminal can cooperate with, learn from, or be influenced by others to commit crimes (Black 2013; Holt 2020; Sellers and Winfree 2010). Therefore, understanding interactions between members can support the study on crime's nature. The criminal network perspective is advantageous as a plurality of crimes involves more than one individual (Morselli 2009). Simultaneously, network analysis techniques have been developed to support criminal network research. Among them, social network analysis (SNA) has become a useful tool for LEAs to study criminal phenomena and develop disruption strategies (Campana 2016). This approach interprets social networks as a set of actors and relations (Campana 2016; Lindquist and Zenou 2019; von Lampe 2003). It provides a way of viewing and approaching specific problems through social relations; moreover, it also is a set of analytic tools for investigating these social relations and their consequences (Campana 2016; McGloin and Kirk 2010; Morselli 2009, p.161).

The criminal network perspective has recently been applied to cyber criminology. Some scholars have stated that cybercrime, as “old wine in new bottles,” possesses the same elements of terrestrial crime (e.g., Brenner 2004, Grabosky 2001). Whereas others have argued that cybercrime groups bring the flexible network model differing from the hierarchical structures of traditional criminal organizations (e.g., Brenner 2002; Hutchings and Holt 2014; Leukfeldt, Lavorgna, and Kleemans 2017; McGuire 2012). The majority of extant studies on cybercrime networks have focused on cybercrime as including a broad range of crimes. More specifically, they have tended to adopt the concept of traditional “organized crime” to analyze cybercrime networks, the relationship between members, off- and online aspects, as well as the online trust among members (e.g., Brenner 2002; Décary-Hétu and Dupont 2013; Grabosky 2001; Hutchings and Holt 2014; Leukfeldt, Kleemans, and Stol 2017; Lusthaus 2012; Lusthaus and Varese 2017; Nurse and Bada 2018; Soudijn and Zegers 2012; Wall 2015). Some researchers have recommended specific typologies of cybercrime networks (Choo and Smith 2008; Leukfeldt, Kleemans, and Stol 2017; McGuire 2012).

While existing studies provide valuable insight into the formation and operation of cybercrime networks, the field is relatively underdeveloped—particularly insofar as most scholars have concentrated on the North American and European contexts (Bossler and Berenblum 2019). There is still an argument among scholars about cybercrime networks, most of which concern similarities and differences between cybercrime networks and traditional criminal organizations. Certain disagreements possibly result from the lack of empirical research on this topic. Many existing studies have been based on anecdotal or circumstantial evidence or adopting cybercrime as including various crimes. In this respect, there is a marked lack of empirical research on specific types of cybercrime networks in Asia, which has some countries like Vietnam, India, and North Korea listed as emerging cybercrime centers (CSIS and McAfee 2018).

Furthermore, under the criminal network perspective, many existing studies have interpreted "networks" as a loose model to describe cybercrime groups, distinguishing it from formal hierarchical models. In cyber criminology, there is not much research adopting SNA that views "networks" as a set of actors and relations. Pitfalls related to strict data requirements are likely to hinder the development of SNA in cyber criminology (see Campana 2016). Moreover, under the criminal network perspective, greater attention should also be directed towards central actors, as they provide essential clues during the investigation and combating of cybercrimes by LEAs (Morselli 2010). According to Morselli (2009, p.12), centrality "could be measured simply as the number or proportion of contacts with whom a participant is directedly connected within a network." Central actors hold vulnerable and strategic positions within criminal networks (Morselli 2010; van der Hulst 2009). By clarifying the organizational structure and central actors of cybercrime networks, LEAs can develop investigation hypotheses and implement effective methods of disrupting criminal networks (Morselli 2009; van der Hulst 2009).

As such, there is a need to clarify the structure of specific cybercrime networks and expand the scope of research to the Asian context. To ensure analytical precision and limit potential research bias, this study focuses on transnational computer fraud (TCF) in Vietnam—a developing country in Asia with a known cybercrime center (CSIS and McAfee 2018).

Computer fraud is considered the most significant threat among cybercrimes (with 24%, in terms of severe consequences) (UNODC 2013, p.27). TCF is often considered the cyber-enabled aspect of cybercrime[1], wherein computer fraudsters use ICT to defraud victims by remote control and across national boundaries. TCF can also be viewed as a whole process, including many stages in which digital devices and networks can become both targets and tools of crime. For example, hackers may attack the databases of websites to steal customers' credit card data before obtaining illegal money. In the first stage, digital data is mainly the target of hacking conducted only through the use of ICT. Subsequently, the Internet and digital devices become tools for defrauding victims. Therefore, clarifying the nature of TCF networks facilitates a more comprehensive study on cybercrime networks.

Before using Vietnamese case studies to clarify cybercrime networks' structure, it is vital to investigate the cybercrime context and TCF's modus operandi in Vietnam as little information is available. Routine activity theory (RAT) is applied to analyze the first sight of cybercrime's causations in Vietnam. RAT holds a vital role in constructing environmental criminology, which established criminal network perspective development. Based on RAT, crime occurs as three factors, namely likely offenders, suitable targets, and the absence of capable guardians converge in one time and space (Cohen and Felson 1979). Besides, crime script analysis has been adopted to analyze crime as a whole process of behaviors (Dehghanniri and Borrion 2019). Both these analytical approaches emphasize situational crime prevention regarded as a useful tool for countermeasures. Accordingly, crime can be prevented by reducing crime opportunities via modifying the environment (Freilich and Newman 2017). Moreover, with the use of crime script analysis, actors, their roles, and their relationships are identified for SNA during various crime stages (Duijn and Klerks 2014; Sparrow 1991). Therefore, RAT and crime script analysis are useful for combining SNA to explore cybercrime networks' nature.

This study fits within the increasing capacity of applying the network perspective to criminology. The criminal network perspective, together with SNA has been used to develop a deeper and broader understanding of cyber networks via examining Vietnamese TCF cases. This study is among the first works applying SNA into cyber criminology. Besides, crime

[1] Cybercrime can consist of two aspects: cyber-dependent or cyber-enabled ones (The Crown Prosecution Service 2019). Cyber-dependent crimes include "core" computer criminal behaviors like illegal access, illegal interception, and data interference. Cyber-enabled ones consist traditional crimes that can be committed with the use of the Internet and digital devices, such as fraud, stalking, and gambling.

script analysis is used to investigate TCF's modus operandi in the Vietnamese context. The knowledge about TCF networks constitutes a foundation for suggesting counter-crime strategies, including international cooperation, prevention, and investigation strategies.

1.2. Research objectives and questions

1.2.1. Research objectives

The thesis aims to better understand the characteristics of cybercrime networks by analyzing the modus operandi and structure of Vietnamese TCF networks. Although the data analysis focuses on TCF case studies collected in Vietnam, to some extent, its vital findings contribute to knowledge about the nature of cybercrime networks in Asia as well as in the global scope. First, the thesis clarifies the characteristics of TCF's modus operandi in the Vietnamese context. Then, the thesis uses Vietnamese TCF case studies to explore the structure of cybercrime networks committing TCF as one specific type of cybercrime. In this respect, by figuring out TCF's nature particularly in Vietnam, the study contributes to a more comprehensive understanding of cybercrime networks in general while giving recommendations for counter-cybercrime strategies.

1.2.2. Research questions

In achieving the objectives, the primary research questions raised in this study are:

Question 1: How is TCF implemented in the Vietnamese context?

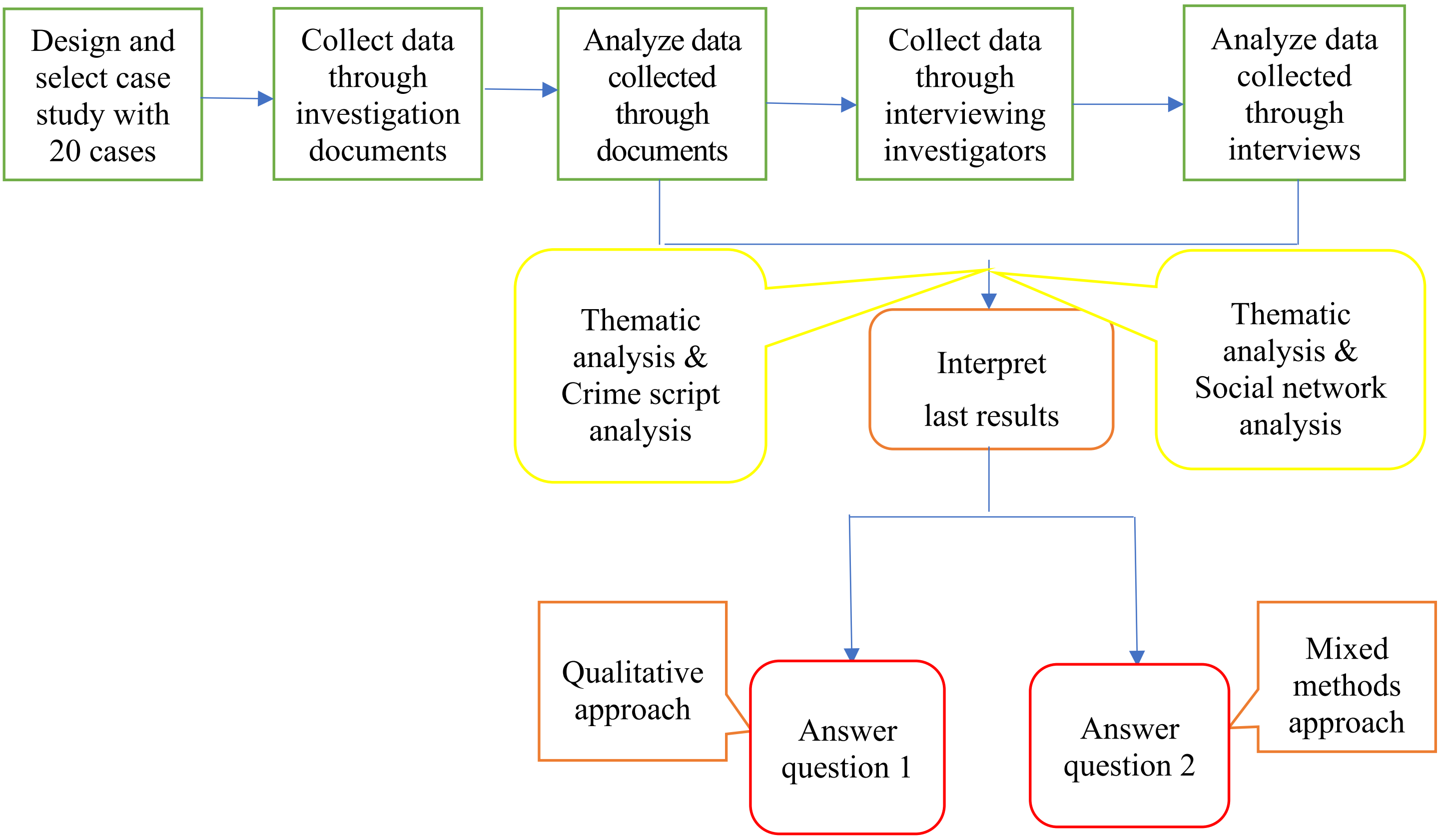
Question 2: How are cybercrime networks structured to conduct TCF?

The modus operandi and structure of cyber networks are two significant aspects to understand the nature of cybercrime. Question 1 focuses on clarifying the modus operandi of TCF in the Vietnam context. Question 2 aims to explore the structure of TCF networks as one specific type of cybercrime networks by using Vietnamese TCF case studies. Question 2 has been addressed with two sub-questions: What are the distinguishable characteristics of the organizational structure of TCF networks? Who occupies the central points in TCF networks? Besides presenting the distinctive characteristics of TCF's modus operandi in the Vietnamese context, the study demonstrates a more comprehensive understanding of cybercrime networks in general. Subsequently, the study proposes a new typology of cybercrime networks based on the clear degree of leadership. Consequently, counter-crime strategies should be designed to cope with this untraditional crime.

1.3. Research design

The research design refers to the appropriate framework of research methods and techniques chosen by researchers (Creswell 2007, 2009). It ensures that researchers address the subject matter effectively and coherently. In other words, it provides the blueprint for collecting and analyzing the data, which leads to strong and convincing conclusions (Gorard 2020). There are three types of designs: qualitative, quantitative, and mixed methods[2] (Creswell 2009). This study used a qualitative approach to answer Question 1, and a mixed-methods approach to answer Question 2. Data were drawn from the analysis of 20 TCF case studies and in-depth interviews with the police officers directly involved with these cases. The research methodology was formulated with several specific research stages (see Figure 1.1).

Figure 1.1. The process of research


Design and select case study with 20 cases
Collect data through investigation documents
Analyze data collected through documents
Collect data through interviewing investigators
Analyze data collected through interviews
Thematic analysis & Crime script analysis
Interpret last results
Thematic analysis & Social network analysis
Qualitative approach
Answer question 1
Answer question 2
Mixed methods approach

[2] Qualitative research is used to determine human experiences about their social reality (Creswell 2007; Gorard 2020; Silverman 2013). In other words, it is the process of collecting, analyzing, and reporting non-numerical data. Denzin and Lincoln (1994, p.2) emphasized that qualitative research aims to understand "phenomena in terms of meanings people bring to them.'' Whereas, quantitative research focuses on objective "fact" rather than subjective "meaning" that is the pursuit of qualitative one (Silverman 2020, p.3). It is the process of collecting, analyzing, and reporting numerical data (Creswell 2007; Gray 2014). Mix-methods research means that qualitative and quantitative research techniques are mixed or combined into a single study (Creswell 2009; Gray 2014; Johnson et al. 2007).

More specifically, a multi-qualitative approach was used to answer Question 1. One of the main reasons for using the qualitative approach is that the present research is exploratory as the topic is new (Creswell 2009). The qualitative approach is beneficial for explaining “how” and “why” a specific phenomenon or behavior occurs in a particular context (Agee 2009). As presented in the above section, one of the main objectives of this research is to analyze TCF networks' modus operandi in the Vietnamese context. Little research has been done on networks of specific cybercrimes like TCF, especially in the Asian context. Therefore, the qualitative approach is suitable for exploring how TCF is implemented in Vietnam.

The combination of several sources of data and qualitative methods was applied to answer Question 1. The results extracted from one source of data or one method may be verified by others; therefore, one single approach's deficiencies can be overcome (Babbie and Mouton 2001; Robson and McCartan 2016). The multi-qualitative approach was designed into two steps concerning case studies from investigation documents and in-depth interviews. In the first step, the study focused on 20 case studies that were derived from investigation documents. Subsequently, the second step was conducted with interviews with 14 investigators who were in charge of these cases. The initial findings from case studies with investigation documents were utilized to formulate interviews with investigators. Afterward, thematic analysis and crime script analysis were used to clarify TCF's modus operandi.

The study has applied a mixed-methods approach to answer Question 2. The combination of qualitative and quantitative techniques is expected to be complementary rather than incompatible with each other (Ulmer and Wilson 2003). Therefore, it is more than simply collecting, analyzing nun-numerical and numerical data; it associates both research forms so that the overall conclusion is stronger and more persuasive than either qualitative or quantitative approach (Creswell et al. 2003).

In particular, this study has used the mixed-methods approach in SNA, which clarifies TCF networks' structure. Data collection was first conducted with qualitative methods, which has been explained in the above paragraphs. Next, the data were analyzed with the mixed-methods approach using both qualitative and quantitative SNA. Case studies from investigation documents and interviews could create a record of relationships between actors. These relationships were then transformed into numerical data. Besides findings from qualitative methods, TCF networks' structure was presented and identified with matrices and statistical analysis. The mixed-methods approach supported the researcher to have a more robust analysis of TCF networks with empirical data.

1.4. Research methods

1.4.1. Designing and selecting case study

A case study is an empirical research strategy explaining in-depth a contemporary phenomenon involving real-world context, especially when the distinction between phenomenon and context may be unclear (Yin 2018, p.1). It is considered one of five social science research strategies, including experiments, archival analysis, surveys, histories[3], and case studies (Yin 2018, p.5). The case study, as compared to the four remaining methods, is preferred to answer "how" or "why" questions about a contemporary set of events, and when behavioral events cannot be manipulated (Martinson and O'Brien 2015). Moreover, there is a lack of available empirical data on a broad and complex phenomenon concerning TCF networks in Vietnam. Therefore, the case study approach was expected to collect data effectively for answering two main questions.

For analytic generalizations, researchers should sufficiently access the data of potential cases, such as reviewing documents, interviewing individuals, or implementing field observations. Research can be designed with single- or multiple- case studies (Martinson and O'Brien 2015). Compared with single-case designs, multiple-case ones are generally preferred because they can provide more robust and compelling evidence (Yin 2003). In this study, to generalize the nature of cybercrime networks, the researcher used 20 TCF cases investigated by Vietnamese police. In such cases, offenders committed computer fraud regulated by the Vietnamese Penal Code. These behaviors are regulated by Article 226b: Using computer networks, telecommunications networks, Internet or digital devices to appropriate property – the 1999 Penal Code, amended in 2009[4] or Article 290: Using computer networks, telecommunications networks, digital devices to appropriate property – the 2015 Penal Code, amended in 2017[5] (see Appendix 1).

More specifically, Vietnamese police forces are still attempting to apply ICT to crime statistics; however, the Vietnamese current registration system of criminal cases is unable to provide a quick overview of all cases involving TCF. Therefore, case studies were selected via

[3] The experiment method provides insight into cause and effective relationships by the manipulation of variables (McLeod 2012). The archival analysis is to seek out and extract evidence from existing records, such as newspapers, personal letters, digital records, objects, or other sources (Allen 2017a). The survey method is the technique of collecting the primary data from a sample of participants through their responses to questions (Mathers, Fox, and Hunn 2007). The historical method is to study the meanings, stages, and characteristics of past events, based on interpretations (Given 2008).

[4] The 1999 Penal Code, amended in 2009, was valid from 2010 to 2017.

[5] The 2015 Penal Code, amended in 2017, has taken effect since 2018.

the snowball method. Snowball sampling is a technique of identifying and recruiting potential subjects from existing research participants (Atkinson and Flint 2001; Handcock and Gile 2011). It can be put in the broader context of link-tracing methodologies based on initial samples' social bond to expand potential contacts (O'Malley and Marsden 2008; Spreen 1992). Under this circumstance, it is often used to collect a sample from a hard-to-reach population in which conventional sampling approaches are impossible or ineffective (Atkinson and Flint 2001; Handcock and Gile 2011). With practical advantages, it has been applied most frequently to implement qualitative research (Atkinson and Flint 2001).

Starting points were cyber police officials at both national and provincial levels[6]. Using the People's Police Academy's personnel database, the researcher asked Vietnamese cyber police officials whether they knew any past TCF cases investigated by their organization or others since the HTCP Department's establishment in 2010 and its transformation into the Department of Cybersecurity and Counter High-tech Crime in 2018. Via their recommendations, the researcher continued to establish a relationship with investigators directly involved with TCF cases. Afterward, with the official letters signed by the Director of Police Academy, the researcher could access investigation files and interview investigators.

In case study research, purposive sampling is prevalent because this case selection technique can ensure that selected cases represent a sufficient range of conditions (Gray 2014; Palinkas et al. 2015). There are different strategies of purposive sampling; however, criterion sampling seems to be applied most commonly in research (Palinkas et al. 2015). Various criteria can be applied to choose suitable cases based on research objectives and questions (Martinson and O'Brien 2015). At the initial stage, a total of 31 potential cases were obtained by the snowball method. Subsequently, only cases that met the following specific criteria were selected:

- First, only completed criminal cases[7] were chosen. Completed cases ensure that the data collected were reliable. Besides, the usage and publication of these data do not create negative impacts on the process of solving cases of LEAs.

[6] Vietnamese police forces (with the full name People's Public Security of Vietnam) are organized into four levels under the management of the Ministry of Public Security. Cyber police officials work at two highest levels: the HCTP Department (now being the Department of Cybersecurity and Counter High-tech Crime) at the central level and Divisions at the provincial one.

[7] Completed criminal cases are cases in which Vietnamese LEAs had enough evidence to prosecute suspects for computer fraud-related activities.

- Second, these cases were transnational[8] according to the United Nations (UN) Convention on Transnational Organized Crime (2000).
- Third, the number of members inside each case was at least three, as one indispensable factor of an "organized criminal group"[9] defined by the UN Convention against Transnational Organized Crime (2000).

In total, this study successfully obtained 20 cases investigated by HTCP between 2010 and 2018, including nine cases conducted by the department headquarters and 11 by provincial police forces. The most common reason for excluding unsuitable cases was insufficient evidence for prosecution, whereas all potential cases satisfied the third criteria. The modus operandi of these 20 cases can be divided into bank card data fraud and phone scams (see Table 1.1). The 12 cases of bank card data fraud can be divided into two categories: using bank card data for online purchases and making fake cards. In the eight phone scam cases, Vietnamese cyber police were unable to clarify all network members, but only one in the "caller group" or "money mule group." To respect human rights and protect confidentiality, this study codes all names of suspects, cases, and investigators with letters and numbers (see Appendix 2).

Table 1.1. Sample cases

Cases	Modus Operandi	
C01, C03, C04, C05, C07, C08	Using bank card data for online purchases	Bank card data fraud
C06, C09, C10, C13, C19, C20	Using bank card data to make fake cards	
C02, C15, C18	Caller group	Phone scams
C11, C12, C14, C16, C17	Money mule group	

[8] Transnational crime means that crime is committed in more than one country; or in one country but a substantial part of its preparation, planning, direction or control occurred in another country; or in one country but involved an organized criminal group that implement criminal activities in more than one country; or in one country but significantly affecting other countries (Article 3, The UN Convention on Transnational Organized Crime 2000).

[9] Organized criminal group means "a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit." (Article 2, the UN Convention against Transnational Organized Crime 2000).

1.4.2. Data collection through investigation documents

There are six most common sources of evidence in implementing case studies: archival records, direct observations, documentation, interviews, participant-observation, and physical artefacts (Yin 2003, p.85). It is highly recommended to combine multiple sources because each source has strengths and weaknesses (Creswell 2007, p.75; Yin 2003, p.85). Within the data triangulation approach, findings and conclusions of case study research are probably much more accurate and convincing. Accordingly, potential issues concerning validity can be solved. This research combined data extracted from investigation documents and in-depth interviews to collect primary data on TCF cases.

Documents play an important role in any data collection in a case study research (Yin 2003, p.87). Data collection took place at the Department of Cybersecurity and Counter High-tech Crime (at the central level) and four police stations of Hanoi, Haiduong, Haiphong, Vinhphuc, Nghean (at the provincial level). The fieldwork was undertaken in Vietnam two times, first in October 2019 and second in March-April 2020. For the first time, the researcher focused on collecting essential data about the modus operandi and structure of all 20 TCF cases. At this time, the researcher had to allocate time suitably to work at different agencies in only one month before flying back to Japan according to the permitted research plan. After that, the second field trip was implemented to recheck the data to ensure the reliability of the research findings.

With the permission of leaders of targeted agencies, the researcher was allowed to work at a private room or a private table for collecting data from investigation documents. The researcher could access police files, including confidential documents. Investigation files consisted of a collection of reports reflecting various investigative techniques such as interviews, item seizure, observation, location searches, and wiretaps (i.e., the secret phone tapping and digital data collection). To satisfy security and confidentiality requirements, the researcher was only permitted to read police files and make notes on a private laptop.

After the collection of data from investigation documents finished, initial data analysis was conducted. At this stage, initial data analysis does not aim to address the research questions directly but ensures that the later comprehensive analysis can be implemented efficiently (Huebner, Vach, and Cessie 2016). Moreover, this step allowed the researcher to gain the first main ideas within TCF cases in the current study, which made the researcher more active in implementing subsequent interviews. The researcher could notice TCF's information, which was unshown or shown unclearly inside investigation documents. The researcher could then discuss interviewees to clarify such information in more detail.

1.4.3. Interview

The interview is one popular and powerful method of collecting data in qualitative research. Using verbal technique is implemented to explore respondents' understanding, experiences, and opinions of the social world in great depth (Gill et al. 2008; Kvale 1996; Rubin and Rubin 2012). Interviewees can "express their own thoughts and feelings" by "their own voice" (Berg 2007, p.96). Moreover, the interview is a valuable method for discovering the construction and negotiation of meanings naturally, in which the misconceptions of participants are possibly solved (Cohen et al. 2007, p.29). The flexible approach of this technique could allow the researcher' discretion in raising additional or sensitive questions (Hagan 2010).

There are three main types of interviews, including structured, unstructured, and semi-structured interviews[10]. This study used semi-structured interviews, which are considered to be the most appropriate method within this context. The flexibility of this format, compared to structured interviews, permits researchers to explore the in-depth knowledge of a particular subject (Gill et al. 2008). This characteristic is significant for the current study, aiming to explore the modus operandi and structure of TCF networks intensively. Moreover, in comparison with the unstructured approach, semi-structured interviews often consume less time and are managed more easily (Gill et al. 2008). Therefore, instead of choosing structured and unstructured interviews, the researcher selected a semi-structured approach with a set of questions focusing on specific topics.

More specifically, the analysis of the criminal investigation was integrated by interviews with police officials directly involved in these cases. While police files often only focus on presenting evidence of criminal activity, the in-depth interviews with police officials could provide primary data, supplementing the shortage of data from official documents. Some participants shared valuable information that was not shown in investigation documents but assisted in detail about TCF's nature, such as preparing tools for VoIP fraud, the recruitment of money mules, or criminals' living habits. Furthermore, interviews could be expanded to cover information about other TCF cases. Therefore, the information collected through interviews could provide more insights into TCF's modus operandi and structure.

[10] Structured interviews are highly standardized with a complete set of pre-determined questions (Kvale 1996; Myers 2009). Accordingly, the researcher must carry out the written instructions, strictly regulated with the order of questions (Gill et al. 2008). By contrast, unstructured interviews do not follow the pre-planned set of questions. Towards a normal conversation, interviewers play the role of a catalyst by encouraging respondents to express their experiences (Cohen et al. 2007). Semi-structured interviews consist of both components of two other types. Here, interviewers maintain basic interview structure with appreciable flexibility. Thus, the order of scheduled questions may change; additional questions might be raised to expand further and clarify specific issues (Gray 2014).

After the initial document analysis, the researcher implemented semi-structured interviews with open-ended questions in October 2019. With the official permission of each organization's leaders, the researcher contacted 18 investigators involved in the 20 selected cases to request an interview. Of these, 14 who had been in charge of 19 of the selected cases agreed to attend interviews. One investigator had been involved in two of the cases, two investigators had been involved in three of the cases, while the rest had been involved in only one of the cases (see Appendix 3).

The procedure of conducting in-depth interviews was adapted from Boyce and Neale's (2006) guide with five steps: planning, developing instruments, collecting data, analyzing data, and disseminating findings. The interview protocol was designed with specific sections (see Appendix 4). All interviewees are Vietnamese; thus, interviews were implemented in this language. Before questioning the participants, the researcher explained the project's primary information and participants' rights. The next section of the interview protocol included four parts. The first part clarified private information about participants. The second part with one general question aimed to let interviewees recall and tell the content of the case freely. The third section with specific questions was then divided into two sub-sections, including modus operandi and structure of TCF. The last section closed key components with additional comments and asked for possible future contact.

Open-ended questions were used during 14 semi-structured interviews. Instead of providing interviewees with predetermined answer choices, open-ended questions allow participants to express answers in their own words (Allen 2017b). They support researchers to gain a comprehensive look into topics being studied; hence, they are often used in qualitative studies and exploratory research (Allen 2017b). In this study, open-ended questions allowed respondents to provide more options and opinions concerning TCF cases. Moreover, this approach could establish a closed and trusting relationship between the researcher and interviewees to discuss TCF cases.

All interviews were implemented at the participants' agencies. Each interview lasted 45–60 minutes. Given the restricted nature of the issue discussed in interviews and to protect Vietnamese LEA officials' rights, permission was granted for the recording of only five interviews. The nine remaining interviews were not recorded, but notes were taken. The difficulty in taking notes was that it was difficult to reach a comprehensive capture of information. This issue could affect the quality of collecting data, although the researcher attempted to make notes of all information.

1.4.4. Data analysis

Thematic analysis

As a foundational method, thematic analysis is a process for encoding qualitative data. It is described as a "translator" for facilitating communications between the language of qualitative approach and quantitative approach (Boyatzis 1998, p.7). The thematic analysis not only supports researchers in identifying, analyzing, describing, and reporting themes (or patterns) of each case study but also allows them to apply these themes to analyze interview data (Joffe and Yardley 2004, p.57). Furthermore, with "a novice qualitative researcher," this approach is also a relatively uncomplicated technique that assists the researcher in constructing a model that best suits the data and the scope of research questions (Braun and Clarke 2006, p.98; Trahan and Stewart 2013, p.64).

There are two ways to identify themes (or patterns) within data in thematic analysis: inductive approach and deductive approach[11]. In this study, an inductive approach, rather than a deductive one, was implemented with a recursive process, involving six phases identified by Braun and Clarke (2006). The study identified specific themes driven by data; however, researchers should not be free themselves of theoretical commitments (Braun and Clarke 2006). The inductive thematic analysis was used to cooperate with crime script analysis to examine the modus operandi of TCF, and with SNA to clarify TCF networks' structure. The sequential six phases of thematic analysis will be presented as follows:

Phase 1: Familiarize with the data

It is significant for researchers to immerse themselves with collected data and familiarize themselves with the deep and broad data content (Braun and Clarke 2006). At this phase, the repeated reading of the entire data was implemented in an active way looking for meanings and possible patterns. The researcher took notes and marked interesting ideas for coding that could be turned back in subsequent steps. This activity supported the researcher in obtaining general knowledge about TCF cases. Besides, ideas about possible patterns about TCF networks' various characteristics were also shaped.

[11] The inductive approach is driven by data themselves without trying to fit into pre-existing patterns (Braun and Clarke 2006). The deductive approach identifies themes (or patterns) by the researcher's theoretical interest in the area (Braun and Clarke 2006).

Phase 2: Generate initial codes

Following the first step, various initial codes produced from the data were organized into meaningful groups. In this phase, manual coding was carried out with writing notes and using highlighters to mark relevant phrases and sentences. The entire data from investigation documents were worked on systematically to identify interesting aspects that could form the foundation of repeated themes (or patterns). After going through the entire data, the researcher collated all data extracts into groups identified by code. Many potential themes about TCF networks' nature could be generated based upon the data-driven method (see Figures 1.2, 1.3, 1.4).

Figure 1.2. Initial thematic map, showing six potential themes to analyze the modus operandi of bank card fraud

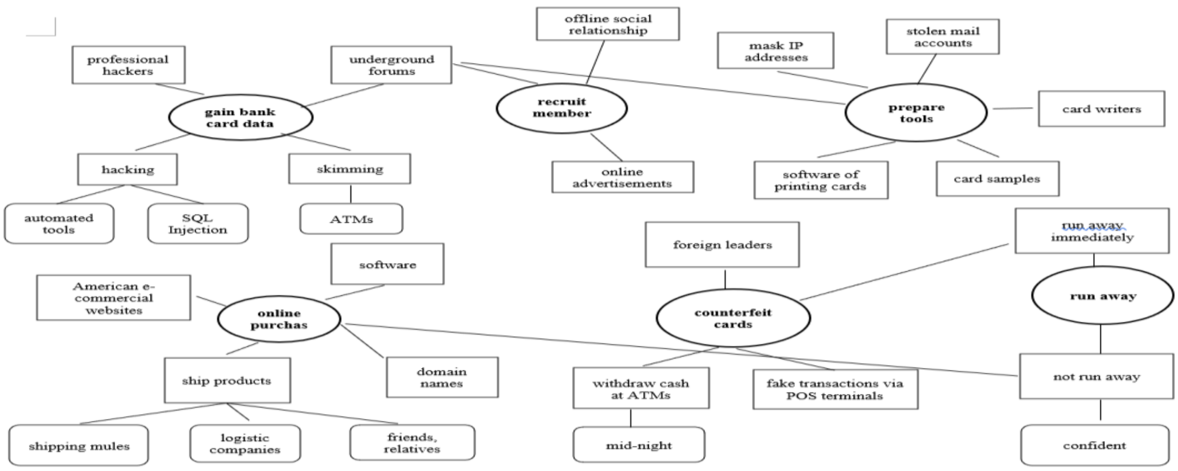


Figure 1.3. Initial thematic map, showing seven potential themes to analyze the modus operandi of phone scams

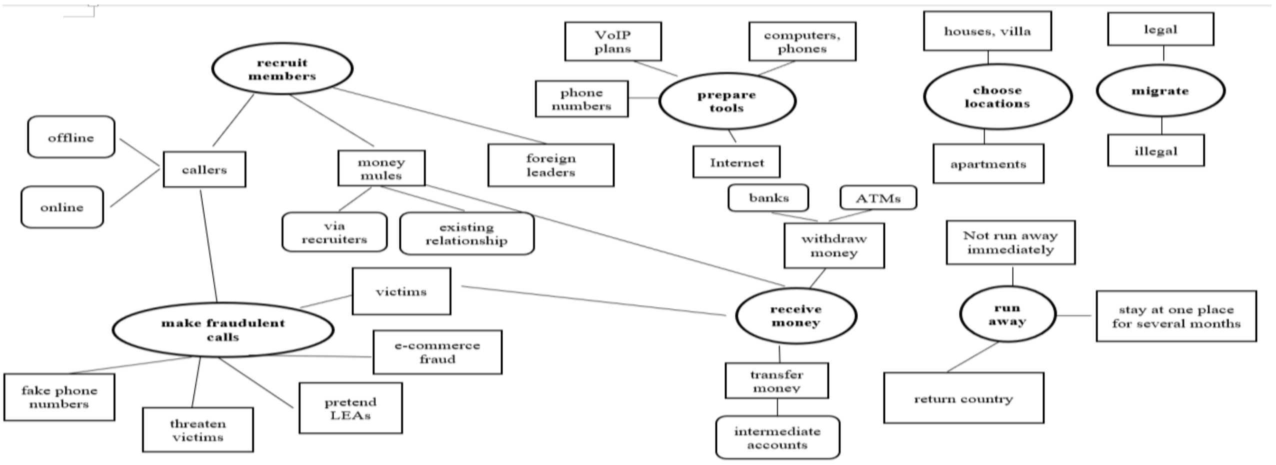
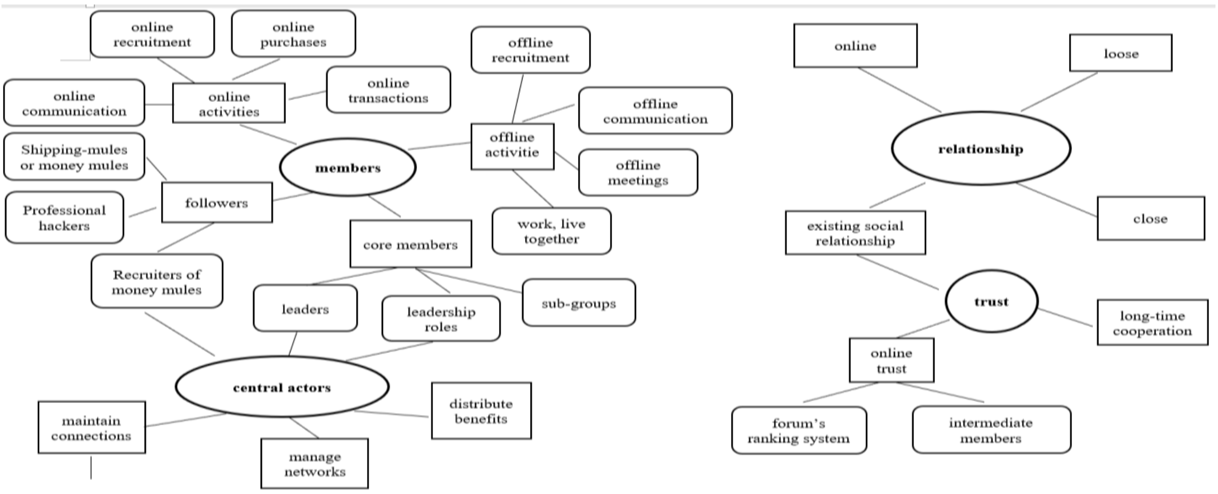


Figure 1.4. Initial thematic map, showing four potential themes to analyze the structure of TCF networks



Phase 3: Search for themes

After collecting different codes, the researcher focused on categorizing these codes into potential themes and sorting relevant data extracts within these themes. As illustrated by Figures 1.2, 1.3, and 1.4, mind-maps were used to search for potential themes concerning the modus operandi and structure of TCF networks. A list of candidate themes (including both main themes and sub-themes) was formed with relevant data extracts. Besides, the researcher started to consider the link between codes, between potential themes, and between the level of potential themes (main themes and sub-themes).

Phase 4: Review themes

At this phase, themes were processed with two levels, including review and refinement. At the first level, candidate themes and coded data extracts were examined for their coherence. The second level ensured that themes could satisfy the meaning of the entire data set. As a recursive process, the thematic analysis includes a series of activities moving back and forward throughout the phases (Braun and Clarke 2006). Re-reading the entire data set, checking coded data extracts, and re-coding from the data set were implemented until a satisfactory collection of different themes were clarified. To make the final themes more useful and accurate, the researcher decided to combine, discard some initial themes. For example, "trust" became one part of "relationship" to analyze TCF networks' structure. "Gain bank card data" merged with "recruit members" and "prepare tools" to create a new theme titled "preparation."

Phase 5: Define and name themes

After having a relatively good list of themes, the researcher defined and refined these themes further. All themes and sub-themes were identified with relevant data to ensure coherence and consistency. For analysis to answer Question 1, the three final themes were defined, including “preparation,” “activity,” and “post-activity” for exploring the modus operandi of TCF (see Figure 1.5). They also represent certain primary stages (or “script scenes”) of crime script analysis (Cornish 1994). At each stage, computer fraudsters perform “scripted actions” to complete the crime. Therefore, based on specific data about “scripted actions,” two or three sub-themes were added to support the two main themes of “preparation,” and “activity.” When analyzing bank card data fraud, “preparation” involves “sourcing bank card data,” “recruiting members,” and “preparing tools”; whereas for phone scams, “preparation” is supported with two sub-themes “recruiting members” and “preparing tools and locations.” For bank card data fraud, “activity” consists of “online purchases” and “counterfeit cards”; while “activity” of phone scams concludes “making fraudulent calls” and “receiving money.”

For analyzing the structure of TCF networks of Question 2, the final three main themes were applied, including “actors,” “relationships between actors,” and “central actors,” which are regarded as the core components of network analysis (Chiesi 2001; Freeman 1978; McGloin and Kirk 2010; Scott 2000) (see Figure 1.6). Within each theme, two or three sub-themes were

Figure 1.5. Final thematic map, showing three main themes to analyze the modus operandi of TCF networks

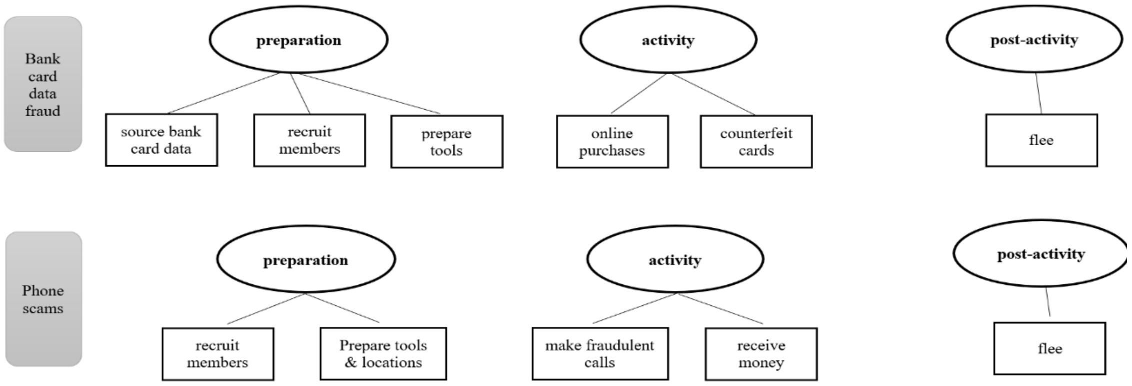
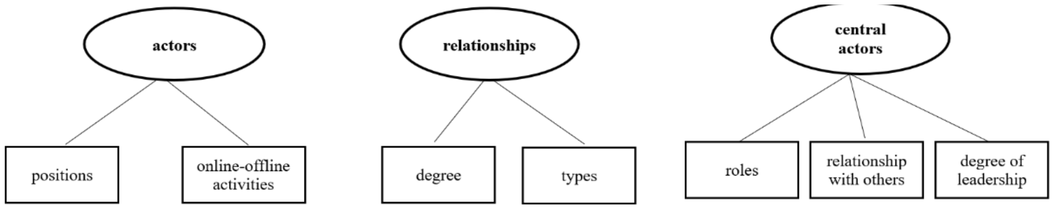


Figure 1.6. Final thematic map, showing three main themes to analyze the structure of TCF networks



identified. For “actors,” the sub-themes were “positions” and “online-offline activities.” For “relationships,” the sub-themes were “degree” and “types”; and for “central actors,” the sub-themes included “roles,” “relationship with others,” and “degree of leadership.”

Phase 6: Produce the report

The last phase included the final analysis and its write-up on the modus operandi and structure of TCF networks. The entire research's write-up was implemented after the analysis of entire data from both police documents and interviews had finished. Such write-up has been expected to provide a coherent and comprehensive story within and across specific themes. The write-up has been presented in the interpretive chapters of the dissertation.

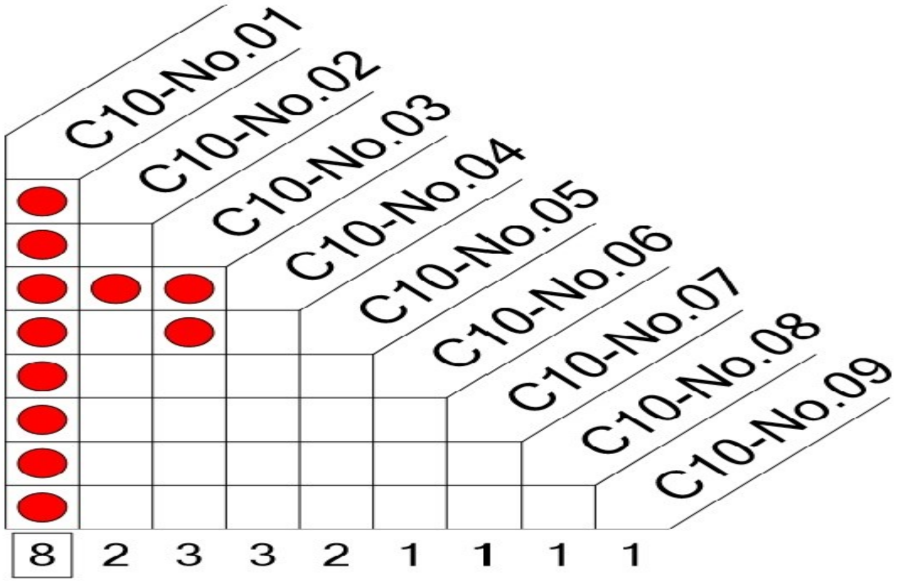
Social network analysis

The application of SNA in the study of crime has been growing up. In criminology, SNA has been used to study traditional criminals and identify the structure and central actors of criminal networks (e.g., Campana and Varese 2013; Mancuso 2014; Morselli 2009, 2010). In this study, for analysis to answer Question 2, the final three main themes, including “actors,” “relationships between actors,” and “central actors,” are three of the core components of SNA (Chiesi 2001; Freeman 1978; McGloin and Kirk 2010; Scott 2000). The characteristics of these themes are examined during the whole process of TCF which has been clarified clearly with Question 1.

To be specific, this research used RFFLow and NodeXL software to visualize TCF social networks. Such visualizations constitute a powerful technique for LEAs, enabling the measurement and illustration of the relations involved in criminal networks, as well as the development of counter-crime strategies (McGloin and Kirk 2010; Sparrow 1991). RFFLow Software has been utilized to construct association matrixes and graphs of social networks between the criminal members. Meanwhile, NodeXL enables the calculation of graph metrics in relation to network centrality. Figure 1.7 illustrates an example of association matrixes.

Figure 1.7 shows the number of relationships between each member within the C10 network. Each red dot symbolizes a link between a member and others in conducting cybercrime. As Figure 1.7 illustrates, as a central actor, suspect C10-No.01 had the greatest number of relationships (8), while four suspects, namely, C10-No.06, C10-No.07, C10-No.08, and C10-No.09 had only one link. Afterward, the graphs mapped through the constructing association matrixes provide valuable insights into crime patterns and criminal networks.

Figure 1.7. Association matrix of C10 network



Subsequently, NodeXL was used to calculate graph metrics (see Appendix 5). Freeman (1978) recommended three notions, namely, degree centrality, closeness centrality, and betweenness centrality, which have been reaffirmed by various scholars, including McGloin and Kirk (2010) and Sparrow (1991) in the area of criminology and policing. Degree centrality (DC) illustrates the number of unique edges that link one actor with the others in a network. Closeness centrality (CC) indicates how close an actor is to all others inside a network. It refers to the index of network cohesion. In this regard, higher closeness centrality reflects a more desirable centrality score. Lastly, betweenness centrality (BC) measures the extent to which a node influences the communication paths between other nodes, thereby facilitating the identification of individuals who play a "bridge spanning" role in a network.

1.5. Obstacles and solutions

Research ethics establish guidelines for researchers in conducting academic research activities faithfully without misconduct (The Japan Sociological Society 2005). Researchers must be cautious about any adverse effects caused by conflicts of interest and any misconduct concerning research activities (Waseda University 2015). This research is one part of the Ph.D. program at Graduate School of Asia-Pacific Studies (GSAPS), Waseda University, Japan. The collection of data was implemented in Vietnam. Therefore, the research must obey the ethical regulation of both Japan and Vietnam. The interviews were implemented faithfully with the protection of the rights of participants. All participants are Vietnamese police officers. Therefore, they do not belong to vulnerable groups defined by the SAGE Encyclopedia (Allen 2017c). Official permission had been granted by leaders of organizations before interviews were implemented, which is a requirement inside Vietnamese police forces. Participants were explained the details of the research and their rights before the researcher received their consent. Furthermore, researchers must ensure participants' confidentiality (Creswell 2009). Accordingly, the anonymity of individuals has been protected during the current research. Their names were coded in data analysis and interpretation. The data from both interviews and investigation documents have been stored securely to prevent from disclosure. Only authorized individuals could access them, which has been pledged to police organizations and participants by the researcher.

Fairness and reliability should be ensured in research (Waseda University 2015). Being a Vietnamese police officer, the researcher is considered an insider when conducting the study. Being an insider could assist the researcher to have many advantages. For example, the researcher received many supports from police agencies. Besides, the researcher could have a particular understanding of the research topic. These points, however, may result in bias and a loss of objectivity. To restrict these negative effects, the researcher was always aware of these issues and conducted steps carefully through all different research stages. Additionally, the researcher always emphasized the role of a Ph.D. student of Waseda University when working at police agencies to collect data.

Data were collected and analyzed with a combination of several sources of data and methods. The researcher was only allowed to read and make notes of investigation documents at police agencies; therefore, the researcher could miss essential data. To ensure the quality of data, the researcher conducted semi-structured interviews with police investigators who had been in charge of these cases. During interviews, the researcher used open-ended questions to encourage participants to share their ideas freely. After interviews ended, online communication was asked to establish if the researcher would like to clarify further information. After analyzing the first-trip data, another research trip was conducted. At this time, the researcher aimed to check the accuracy of data collected from investigation documents and interviews. The researcher was allowed to re-access police files to revise data. Furthermore, "member checking" could be useful as the final reports or specific parts of findings are examined by participants (Creswell 2009). The researcher again discussed police officials who had been interviewed before. The researcher provided opportunities for participants to comment on the results.

1.6. Structure of the dissertation

This thesis is organized into eight chapters beginning with this introduction.

Chapter II. Literature review

Following this introduction, Chapter II reviews the literature on cybercrime networks and theoretical backgrounds. After reviewing the definition of cybercrime, this chapter clarifies the criminal network perspective. This perspective has become a prevalent approach to study the nature of crimes. As one powerful technique of network perspective, SNA is highlighted with its essential contributions in criminology. The criminal network perspective, together with SNA, constructs the key theoretical framework of this present study. Next, the transformation and typologies of cybercriminal networks are presented. Under the influence of the criminal network perspective, some scholars have tried to explore the nature of cybercrime networks; however, there is still a lack of empirical studies on specific cybercrimes, like TCF in Asia. This gap will be examined clearly by this section. Afterward, the chapter reviews the commission of computer fraud and the crime script analysis approach. Lastly, RAT and its application in cyber criminology are presented. This chapter will explain the suitability of combining crime script analysis and RAT with SNA to study cybercrime networks' nature.

Chapter III. Cybercrime and cyberspace regulation in Vietnam

Chapters III and IV examine the cybercrime context in Vietnam, which provides the background for clarifying TCF networks in the following chapters. Both these chapters are mostly based on secondary data from published and unpublished reports of domestic and international organizations. Chapter III provides a general situation of cybercrime and cybercrime regulation in Vietnam. The situation of computer fraud in Vietnam is also presented here. Furthermore, to cope with cybercrime risks, the Vietnamese Government needs to implement particular policies also analyzed in this chapter. The provision of Vietnamese cybercrime-related policies helps the researcher consider policy and practical recommendations appropriate for the Vietnamese context.

Chapter IV. The reasons for cybercrime in Vietnam: An analysis based on the routine activity theory

Following Chapter III, this chapter focuses on clarifying the reasons for the cybercrime situation in Vietnam. Based on RAT, the chapter analyzes three factors, including likely offenders, suitable targets, and the absence of capable guardians. Accordingly, it suggests that proximity to high concentrations of potential cybercriminals with capacity and motivation increases the capability of cyber victimization[12] in Vietnam. Then, this chapter analyzes suitable targets with four dimensions – value, inertia, visibility, and accessibility. The absence of capable guardians is examined with three levels: governmental, organizational, and individual ones. Understanding the causations of general cybercrime helps the researcher present recommendations more comprehensively after Chapters V, VI explore the nature of TCF networks.

Chapter V. The modus operandi of transnational computer fraud: A crime script analysis in Vietnam

Before highlighting recommendations for counter-cybercrime strategies, the thesis identifies cybercrime's nature. Chapters V and VI clarify the modus operandi and structure of TCF networks. This chapter presents the findings of Question 1, which elucidates TCF's process in the Vietnamese context. It examines two types of crime: bank card data fraud and phone scams. Firstly, this chapter provides the descriptive statistics of 20 case studies. It presents preliminary information about the background of these case studies, the characteristics of suspects and victims, and the consequences of these cases. Subsequently, as the first central theme of TCF characteristics, its modus operandi is clarified with a crime script analysis framework: preparation, activity, and post-activity. As a new emerging center of cybercrime, Vietnam is likely to become an operational base for domestic and foreign criminals to conduct computer fraud. The study proves that TCF, as an intersection between fraud, technology, and transnationality, does not request direct interaction between offenders and individual victims. This chapter also discusses the modus operandi of bank card data fraud and phone scams in the Vietnamese context. There are specific significant differences among them: bank card data fraud requires more technology use, and the role of Vietnamese and foreign criminals in the two types of TCF is different.

Chapter VI. The structure of cybercrime networks: Transnational computer fraud in Vietnam

Understanding the modus operandi of TCF in the Vietnamese context is the intermediate step for examining TCF networks' structure in Chapter VI. The chapter focuses on answering

[12] Victimization is the process of becoming a victim or being victimized by illegal behaviors (Muratore 2014)

Question 2, contributing to a more comprehensive understanding of cybercrime networks in general. Data drawn from the analysis of 20 TCF case studies and in-depth interviews with investigators prove that TCF can operate both online and offline depending on modus operandi. Moreover, central actors can keep the role of core members or recruited enablers inside cybercrime networks. Furthermore, almost all networks' structures are likely to change as the networks develop. This chapter suggests a new typology based on the clear degree of leadership, which indicates that networks with a high degree of online activity are often constructed more loosely than networks with a lower degree of online activity.

Chapter VII. Recommendations for counter-crime strategies

From understanding the modus operandi and structure of TCF entities, Chapter VII discusses relevant policy and practical recommendations. The recommendations are divided into three categories: international cooperation, prevention, and investigation strategies. First, international cooperation plays an important role in counter-crime policies. This content should be targeted and enduring with the identification of "hotspot" countries. Second, situational prevention measures can be conducted to prevent TCF and mitigate the effects of crime on victims. Cyber police can implement specific strategies to act upon three factors: offenders, targets/victims, and places. Third, LEAs can exploit vulnerabilities within cybercrime networks to investigate these networks. Significant vulnerabilities such as central actors, trust, and hacking forums can be used to disrupt cybercrime networks. These recommendations are expected to increase the effectiveness of the fight against TCF as well as other cybercrimes.

Chapter VIII. Conclusion

Chapter VIII concludes with restating key findings and contributions from the whole study. Vietnam is likely to become an operational base for both domestic and foreign offenders to implement TCF. TCF in Vietnam exhibits certain distinguishable characteristics concerning its modus operandi. There are big differences between each type of TCF, such as the degree of technology, the interaction between suspects and victims, the roles of Vietnamese and foreign criminals. Moreover, the study clarifies the nature of cybercrime networks in general by examining the organizational structure and central actors of Vietnamese TCF case studies. Technological factors lead to the transformation of cybercrime networks, suggesting adjustments to counter-crime strategies. Finally, this chapter acknowledges the limitations of the research and proposes the future of study on cybercrime networks.

CHAPTER II. LITERATURE REVIEW

2.1. Introduction

This chapter reviews the literature on cybercrime networks and identifies the present study's theoretical framework. It includes seven sections. After the introduction, the second section summarizes the definitions of cybercrime with two main aspects: cyber-dependent and cyber-enabled ones. Subsequently, the third section reviews the criminal network perspective to provide necessary information about the study on criminal organizational systems. Especially, social network analysis and its application in criminology are highlighted in this section. Afterward, the fourth section presents the main contents of existing research on cybercrime networks. Here the transformation of cybercrime networks and their typologies are emphasized. Next, the fifth section focuses on the commission of computer fraud and crime script analysis. The sixth section examines routine activity theory before the final section concludes this chapter.

2.2. Cybercrime conception with two main aspects

Cybercrime has evolved from criminal misuse of computers emerging in the 1960s (Brenner 2007). The compound word "cybercrime" came after the concept "cyberspace" coined by William Gibson (1984). "Cyberspace" is defined as the virtual world of computers or "a graphical representation of data abstracted from the banks of every computer in the human system" (Gibson 1984, p.51). The prefix "cyber-" also forms many other words related to cybercrime, such as "cybersecurity," "cyberattack," "cyber-war." The term "cybercrime" is now used popularly; however, the definition of cybercrime often depends on the purpose of usage.

More specifically, international organizations often focus on listing or categorizing cyberspace-related behaviors rather than defining the term "cybercrime." Confirming a lack of international definition of cybercrime, the UN uses a typology to explain cybercrime with three types: "cyber-dependent offenses," "cyber-enabled offenses," and "online child sexual exploitation" (United Nations, n.d.). "Cyber-dependent offenses" infringe the confidentiality, integrity, and availability[13] of computer systems and data (e.g., hacking, malware attacks, DDoS

[13] Confidentiality, integrity, and availability (CIA Triad) are three main portions of information security (ISO 2018). Confidentiality is to ensure data available only to authorized individuals, entities. Integrity is to ensure data accurate and complete. Availability is to ensure data accessible and usable when required by authorized entities.

extortion[14]). Whereas "cyber-enabled offenses" use technology to facilitate traditional crimes such as online frauds, money laundering. "Online child sexual exploitation" makes use of the Internet to abuse children – known as "sextortion." Somewhat similarly to the UN, INTERPOL (2017) distinguishes two fundamental categories of Internet-related crime: "advanced cybercrime" and "cyber-enabled crime." Online child sexual exploitation belongs to "cyber-enabled crime" in INTERPOL's (2017) typology.

The Budapest Convention CETS No.185 (or The Council of Europe Convention on Cybercrime) (2001), which has been regarded as the first international convention on combating cybercrime, also does not define the term "cybercrime." The convention only provides a list of cybercrimes divided into four categories. Firstly, "offenses against the confidentiality, integrity, and availability of computer data"[15] are similar to the first type inside the typology of the UN and INTERPOL (2017). The three remaining categories cover traditional offenses using computer systems. They belong to cyber-enabled offenses listed by the UN and INTERPOL (2017). These groups consist of "computer-related offenses,"[16] "content-related offenses,"[17] and "offenses related to infringements of copyrights and related rights."

Within the scientific community, many scholars have attempted to define cybercrime. The term "cybercrime" can be replaced by other terms such as "computer crime" (Hollinger and Lanza-Kaduce 1988; Richardson 2008), "high-tech crime" (Branigan 2004; Newton 2003), "digital crime" (Gogolin 2010; Taylor et al. 2014), "e-crime" (Marcelline and Charlie 2009; Yar 2012), "Internet crime" (Jewkes and Yar 2009), "virtual crime" (Grabosky 2001). Moreover, the definitions of "cybercrime" tend to be different based on the study's context and content (see Gercke 2012). In other words, behaviors that are categorized as cybercrime are "in the eyes of the beholder" (Payne 2020, p.4). To prove the challenges of selecting a universally-accepted definition, Payne (2020) listed at least nine common concepts of cybercrime; however, none of them is perfect.

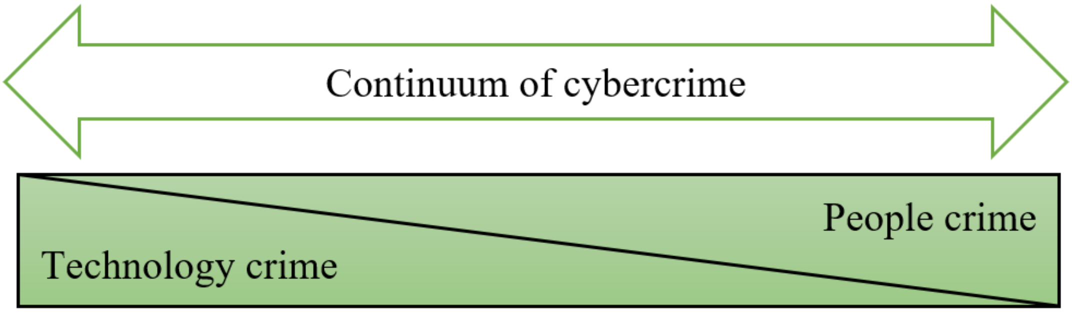
[14] DDoS extortion refers to Distributed Denial of Service attacks in which attackers overwhelm target websites with too much fake traffic (Kaspersky n.d.).

[15] "Offences against the confidentiality, integrity and availability of computer data and systems" include " illegal access," "illegal interception," "data interference," "system interference," and "misuse of devices" (The Budapest Convention on Cybercrime 2001).

[16] "Computer-related offences" consist of "computer-related forgery" and "computer-related fraud" (The Budapest Convention on Cybercrime 2001).

[17] "Content-related offences" include "offences related to child pornography" (The Budapest Convention on Cybercrime 2001).

Figure 2.1. Continuum of cybercrime suggested by Gordon and Ford (2006)



Gordon and Ford (2006) admitted that modeling a comprehensive definition of cybercrime is complicated because existing research tends to be descriptive rather than developing from a theoretical framework. The authors used the popular concept of cybercrime as “any crime that is facilitated or committed using a computer, network, or hardware device” (Gordon and Ford 2006, p.2). To illustrate more clearly cybercrime definition, they divided cybercrime into two types: Type I of cybercrime is mostly technological, and Type II has a more pronounced human element (see Figure 2.1). This recommendation provides insights into future research that might examine “technical” and “human” aspects of cybercrime. Accordingly, “technical” and “human” factors of specific acts should be clarified more to understand the nature of cybercrime, which supports for the design of countermeasures.

The current study does not seek to define the term “cybercrime” per se. Choosing the correct definition of cybercrime is similar to selecting “the right belt for the right outfit” (Payne 2020, p.22). Depending upon the purpose of using the term “cybercrime,” it is often defined variously in different contexts. However, cybercrime can be viewed with at least two significant aspects (The Crown Prosecution Service 2019). In the first dimension, cybercrime can be recognized as “core” computer criminal behaviors that infringe the confidentiality, availability, and integrity of computer data. In this group, cybercrime behaviors are new, technological, and only exist with ICT development. Illegal access, illegal interception, and data interference, for example, cannot be implemented without computers and networks. Unlike the first aspect, the second concerns traditional crimes that become non-traditional as criminals exploit ICT to commit crimes. Without the Internet and digital devices, these crimes still exist; however, the usage of ICT makes them increase in scale or consequences.

Viewing cybercrime with these two aspects fits the opinions of the UN, INTERPOL (2017). The first aspect of cybercrime includes cyber-dependent offenses or advanced cybercrime, whereas the second consists of cyber-enabled offenses in the typology of UN, INTERPOL (2017). Moreover, this consideration helps the researcher better explain the study's focus when only TCF – one specific cybercrime has been clarified. In nature, TCF is cyber-enabled, focusing upon the second aspect of cybercrime, wherein ICT is used mainly as a tool to help fraudsters obtain illegal money from victims. Furthermore, it is appropriate for the popular continuum of cybercrime suggested by Gordon and Ford (2006). Accordingly, although cybercrime can be dependent on or enabled by technology, technical factors differentiate cybercrime from traditional crimes. Following the suggestion of Gordon and Ford (2006), the role of technology inside TCF will be clarified and discussed in detail to understand more the nature of cybercrime.

To sum up, cybercrime can be viewed with at least two aspects: cyber-dependent and cyber-enabled ones. This study clarifies the nature of TCF being one specific act of cybercrime. It focuses upon the second dimension of cybercrime as technology enables criminals to defraud victims. The role of technology within TCF will be evaluated and discussed to contribute to more understanding of cybercrime.

2.3. Criminal network perspective and social network analysis

The criminal network perspective is necessary as most crimes are relevant to more than one person (Morselli 2009, p.1). Living inside a social context, a suspect can be impacted by, learn from, or coordinate with others to conduct criminal behaviors (Black 2013; Holt 2020; Sellers and Winfree 2010). Hence, this perspective is beneficial for understanding crime's nature since it views crime as the consequence of interactions between members inside criminal organizational systems (Morselli 2009). Criminal organizational systems are across a continuum from simple co-offending decisions to complicated designs (Morselli 2009; Williams 2001). The former may only aim to seize a criminal opportunity by the one-time partnership. In contrast, the latter is organized in a bureaucratic-like infrastructure to monopolize illegal markets.

The study on criminal organizational systems has developed during the long history of criminology. As far back as the 1930s, according to differential association theory, first recommended by Sutherland (1939, 1947), offenders learn crime from "intimate personal groups." Besides, Sutherland (1947) suggested the new theory titled "differential social organization." With this novel concept, the scholar argued that:

> …crime is rooted in social organization and is an expression of that organization. A group may be organized for criminal behavior or organized against criminal behavior. Most communities

> are organized both for criminal and anti-criminal behavior and in that sense the crime rate is an expression of the differential group organization. (Sutherland 1947, pp.8,9)

Sutherland's ideas extended from the early Chicago School research, famous for urban sociology and symbolic interactionism (Browning, Cagney, and Morris 2014). Based on symbolic interactionism, individuals as actors in the social world develop and build upon through the repetitive acts of social interactions (Pascale 2010). In other words, individuals living in social worlds can interact with others to create symbolic worlds, and in return, the worlds' aspects impact these individuals in certain times and contexts (Blumer 1969; Franzese and Seigler 2020).

Following on from Sutherland's ideas and the Chicago School works, scholars in the 1970s and 1980s were increasingly paying attention to the spatial convergence of criminals (Morselli 2009). RAT, first proposed by Cohen and Felson (1979), arose as a key theoretical approach in criminology in this period (Wikström 2009). It explains three essential elements of making up a crime, including likely offenders, suitable targets, and the absence of capable guardians. The rise of RAT led to the development of environmental criminology, which views criminal patterns within particular environments (Wortley and Mazerolle 2008). Subcultural theories of crime have been developed; accordingly, crime and delinquency are viewed as "learned" behaviors from certain groups or subcultures where social factors form values and attitudes of supporting criminal activities (Black 2013; Holt 2020). As one of the most popular subcultural theories, social learning theory suggests that criminal behaviors occur when a person interacts with pro-crime individuals rather than anti-crime ones (Akers 1973; Sellers and Winfree 2010).

Whereas social control theory, first formed by Hirschi (1969), argues that the inclination for delinquent behaviors exists as a part of innate human nature, but this propensity can be inhibited by bonds or commitments with parents, family, friends, schools, and other aspects of society. Therefore, crime occurs if such bonds are weak or not well set up (Carrington 2016). Unlike differential association theory established by Sutherland (1939) and other theories that seek to explain why individuals engage in crime originating from the outside context, social control theory uses the opposite approach from the inside of humans. It focuses on answering why individuals restrain offending (Akers and Sellers 2004). Although the main contents of theories can be different, they cite social environment to explain deviant behaviors (Carrington 2016). These theories have put forward the criminal network perspective to understand crime's nature. Accordingly, criminal behaviors' characteristics and reasons can be interpreted from criminal relations inside criminal organizational systems.

The traditional paradigm for examining criminal organizational systems focused on the hierarchical structure of criminal organizations (Williams 2001). This interpretation possibly originated from the rise of bureaucratic-like criminal organizations or confederations in the 1960s in America (Cressey 1969). As claimed by Cressey (1969), Italian-American criminal confederations like La Cosa Nostra were governed by rules and regulations with a "top-down chain" of authority. Like the structure of government, bureaucratic criminal organizations possess a clear division of labor under the direction of a supreme leader, with different levels of followers, each having a defined duty (Abadinsky 2007, p.6; Albanese 2010, p.97).[18]

Researchers have been increasingly using the network perspective to explore criminal phenomena (Morselli 2009; Williams 2001). Under the "coming of a networked criminology" (Papachristos 2011, p.101), there are two ways of interpreting "networks." The substantive approach views networks as a distinct form of social organizations.[19] In this approach, "networks" can be defined in the middle of "market"[20] and "hierarchy" frameworks in the following way:

> Networks are "lighter on their feet" than hierarchies. In network modes of resource allocation, transactions occur neither through discrete exchanges nor by administrative fiat, but through networks of individuals engaged in reciprocal, preferential, mutually supportive actions.

[18] Besides hierarchical structure, criminal organizations use systematic violence and corruption to assist their illegal business (Clark 1982, p.228; Finckenauer and Voronin 2001, p.2; Maltz 1976). They target to gain monopoly control over criminal markets or territorial basis (Abadinsky 2007, pp.3,6; Albanese 2000; Finckenauer 2005). Moreover, within their business operation, there was a close connection between illegal activities and the legal economy (Paoli 2002, p.51). Accordingly, Finckenauer (2005, p.65) proposed a framework for studying organized crime as follows: "structure/organized hierarchy," "ideology," "continuity," "violence/use force or threat of force," "restricted membership/bonding," "illegal enterprises," "penetration of legitimate business," and "corruption." This conventional model may be regarded as one of the highest levels of criminal organizational systems.

[19] Many scholars have embraced the network perspective to describe the emerging organizational form of organized crime. Williams (2001, p.62) described that "organized crime is increasingly operating through fluid network structures rather than more formal hierarchies." Potter (1993), Finckenauer and Waring (1998) stated that organized crime in the US currently operates mainly through network structures. Furthermore, Hobbs (2002) evaluated the network model as the global framework of organized crime. There, reciprocal relationships between actors are essential to maintain criminal networks' operation (McIllwain 1999). Accordingly, members can be provided illicit items and services or other material opportunities in return for engaging in criminal networks (McIllwain 1999). Members' interaction is based on horizontal relationships rather than hierarchical organizations' vertical relationships (Le 2013, p.31).

[20] Market is a spontaneous coordination mechanism that is open to all members and based on self-interested actions of members. No trust is required, and agreements are strengthened by legal sanction. (Powell 1990, pp.301-302).

> Networks can be complex: they involve neither the explicit criteria of the market, nor the familiar paternalism of the hierarchy. (Powell 1990, p.303)

Whereas the instrumental approach interprets “networks” as a collection of actors and relations (Campana 2016; Lindquist and Zenou 2019; von Lampe 2003). Within this approach, networks can transcend all organizations' models, and even formal hierarchy may emerge from a set of actors and relations (Morselli 2009, p.10; von Lampe 2003). Therefore, hierarchical models' important role is not reduced because hierarchical organizations may be clarified more with the values of SNA, such as relational data and centrality (Le 2013, p.42). This interpretation stands at the foundation of SNA as a useful network analysis technique.

SNA is not a formal theory but relatively a strategy for clarifying social structures (Otte and Rousseau 2002). SNA provides a view towards understanding human behaviors based on social relations; besides, it also offers a set of analytic tools that assist the investigation of these social relations (Campana 2016; McGloin and Kirk 2010; Morselli 2009, p.161). Some researchers proved that SNA could become an effective tool for LEAs to understand criminal phenomena as well as developing tactics for crime intervention and investigation (Carrington 2016; Lindquist and Zenou 2019; Malm and Bichler 2015; McGloin 2005; McGloin and Kirk 2010; Morselli 2009; Sparrow 1991). Morselli (2009, p.161) evaluated the important role of SNA in criminology as follows:

> Social network analysis is not simply a set of methodological tools - it is a perspective, a way of seeing and approaching specific problems. The contributions from research within this perspective are wide and their impact in criminology has become increasingly pronounced with novel applications in areas…

SNA possibly is somewhat novel to criminology compared to other fields; however, it is not a new approach or technique (Carrington 2016; McGloin and Kirk 2010). SNA has emerged as an interdisciplinary technique and gained significant popularity across many disciplines such as economics, sociology, computer science, communication studies, and psychology (Zhang 2010). According to Freeman (2004), SNA could be paved by *Sociomery Method* created by Jacob Levy Moreno – a social psychologist in the 1930s. However, SNA was not universally recognized in social research until the end of the 1970s when important research on social networks was conducted by Harrison White and other scholars of the Harvard school (Freeman 2004). Subsequently, in the 1980s, several sociologists began to adopt SNA as an analytical tool to investigate social structure (Freeman 2004). After the 1990s, SNA has attracted scholars' attention from various fields (Freeman 2004). These study streams collectively result in the refinement and development of theoretical, methodological, and analytical approaches of network analysis, which becomes a foundation for applying SNA into criminology.

Within criminology and criminal justice, SNA is regarded as the most "fruitful" instrument to understand criminal phenomena inside criminal network research (Campana 2016, p.1). The development of SNA in criminology has established core concepts and their roles within the strategic analytical framework (see Appendix 6), as follows:

Actor: As a fundamental unit of any network, actors are participants or members in the collaboration or competition within a social network (Campana 2016; Lindquist and Zenou 2019; von Lampe 2003; Zhang 2010). They can be called nodes within a network graph or vertices when relational data are calculated (Lindquist and Zenou 2019; Sparrow 1991, p.252). Actors or nodes are most popularly individuals, groups, or organizations – or any form of related entities (Zhang 2010). Criminals or suspects are regarded as actors when they participate in a criminal network.

Relation: Relations can be called relationships, ties, edges, or links that connect actors in a social network (Campana 2016; Lindquist and Zenou 2019). These relations are the unit of analysis in social network research (Campana 2016; McGloin and Kirk 2010). They can exist under various forms such as co-membership, co-offending, communication, and peer relationship (McGloin and Kirk 2010). In some cases, based on research questions and their nature, relations can be divided into directed and undirected ones (Lindquist and Zenou 2019; McGloin and Kirk 2010). A directed relation implies an asymmetric tie with a flow or direction between a "sender" and a "receiver," whereas an undirected link means that two actors are mutual (McGloin and Kirk 2010). They can be interpreted as binary numbers at network measures when each relation among nodes has a value of 1 (McGloin and Kirk 2010).

Density: Density, one of the most widely used in graph theory, shows the general level of connectedness among nodes in a graph (Otte and Rousseau 2002). The density is calculated by the number of actual ties divided by the possible ties within a network (Morselli 2009, p.47; Otte and Rousseau 2002). The value of density can vary from 0 (no ties between nodes) to 1 (all actors are linked together). When the value is close to 1, the network is dense.

Centrality: The measures of centrality clarify the most prominent members, regarded as key or "star" actors who are greatly associated with others (Zhang 2010). According to Morselli (2009, p.12), centrality "could be measured simply as the number or proportion of contacts with whom a participant is directedly connected within a network." Centrality is a significant ingredient in identifying network vulnerabilities (Morselli 2010; Sparrow 1991, p.264; van der Hulst 2009). In considering to take down criminal networks, one of the most effective approaches is to clarify central actors and target them for surveillance and arrest (Sparrow 1991, pp.263, 264). Moreover, existing research contains different notions of centrality. Three notions, including degree centrality, closeness centrality, and betweenness centrality, were recommended by Freeman (1978), then they have been reaffirmed by various scholars in criminology and policing (see Appendix 6).

Broker: A network can possess "structural holes" representing unconnected parts between actors (Burt 1992). To maintain the whole network's operation, brokers (or brokerages, bridges, middlemen, or boundary spanners) connect these unconnected parts (Burt 1992; Yang, Keller, and Zheng 2019). In other words, brokers refer to intermediary actors who assist transactions and the flow of information or resources between unconnected actors within a network (Marsden and Lin 1982). A broker is also considered a trustworthy middle-person by two actors lacking trust in each other. Brokers can be in charge of resource distribution and coordination inside the network (Morselli 2009, p.16). Therefore, their disappearance can impact the network's operation (Lindquist and Zenou 2019). Although the measures of brokers possibly vary, betweenness centrality is often used to identify these "bridge spanning" actors.

Leader: Leaders hold a principal role in organizations' success (Calderoni and Superchi 2019). It does not mean that leaders always exist within all criminal networks (Klein 1971, p.96). Calderoni and Superchi (2019) stated that criminal leaders are strategic brokers within the network, often receiving a higher value of betweenness centrality. However, many scholars argued that leaders should be distinguished from central participants or brokers (Carley, Lee, and Krackhardt 2001; Morselli 2009, p.14). Even leadership in criminal networks may be transient and flexible (Morselli 2009, p.143; Weisel 2002, p.152). A leader can be the powerful actor with the "highest cognitive load" or the member who shows the most qualities concerning leadership capacity like prior influence experiences, verbal skills, social capacities, talents, and opportunisms (Klein and Maxson 2006, p.195; Morselli 2009, p.14). In a criminal network, leadership and centrality can belong to two different actors; hence, the removal of a central node may not cause the expected disruption of this network, and the arrest of the leader may not result in pushing the central actor to the leadership position (Morselli 2009, p.14).

SNA is beneficial for examining criminal organizational systems (Bruinsma and Bernasco 2004; Morselli 2009, p.9). It has been used extensively to identify crime's nature, especially the evolving operation and structure of networks. Concerning crime prevention and investigation strategies, SNA can provide insight into how criminal networks cope with LEAs' intervention and how criminal networks adjust after members join or quit (McIllwain 1999, p.319). Such knowledge becomes the ground for forming counter-crime policies.

By emphasizing relational data, SNA investigates criminal structures via diagramming and measuring criminal networks' relationships (McGloin and Kirk 2010; Sparrow 1991). Descriptive graphs, also called "sociograms," is a visual illustration of a network, wherein individuals (or other types of actors) are symbolized by nodes, and relations are shown by lines between two nodes (McGloin and Kirk 2010). The visualization of networks can be implemented by various methods with analytic software. Data exploration can be done via graphical displays in different layouts, colors, directions, or thickness of lines (McGloin and Kirk 2010). Hence, descriptive graphs can provide insights into the operation and structure of criminal networks (e.g., Finckenauer and Waring 1998; McGloin 2005; Morselli 2009; Papachristos, Hureau, and Braga 2013), then guide the design of counter-crime policies (e.g., Lindquist and Zenou 2019; McGloin 2005; Morselli 2009; Papachristos et al. 2013).

Besides descriptive graphs, scholars also use network measures to understand criminal networks' characteristics. Network measures keep a central role in describing criminal networks' overall structure, especially clarifying central or key members inside these networks (International Association of Crime Analysts 2018, p.7). The popular measures of SNA can include vertices, density, degree centrality, closeness centrality, betweenness centrality (McGloin and Kirk 2010). Some measures (such as density, average centrality values) can be useful for understanding the nature of networks, whereas some specific measures can provide information about individuals (McGloin and Kirk 2010). Scholars can use network measures to identify and understand central actors' characteristics (Lindquist and Zenou 2019; McGloin and Kirk 2010; Morselli 2009; Scott 2000). These central actors can be considered vulnerable positions that LEAs should pay attention to when conducting counter-crime policies (Lindquist and Zenou 2019; Morselli 2010; Sparrow 1991, p.264; van der Hulst 2009).

Recently, SNA has been increasingly applied to the study of different types of crimes and criminal groups such as human trafficking (e.g., Mancuso 2014; Morselli and Savoie-Gargiso 2014), drug-related crimes (e.g., Calderoni 2012; Giommoni, Aziani, and Berlusconi

2017; Le 2013; Luong 2017; Malm and Bichler 2011a; Malm, Kinney, and Polland 2008; Natarajan 2006), property offenses (e.g., Beavon, Brantingham, and Brantingham 1994), juvenile delinquency (e.g., Bichler, Christie-Merrall, and Sechrest 2011; Bichler, Malm, and Enriquez 2014), terrorism (e.g., Qin, Xu, Hu, Sageman, and Chen 2005; Sageman 2004). Consequently, vulnerabilities inside criminal networks can be identified, which helps LEAs design and implement counter-crime strategies effectively (Lindquist and Zenou 2019; Morselli 2010; Sparrow 1991, p.264; van der Hulst 2009). Perhaps one of the topics best known for embracing sociograms of SNA is the study on street gangs (McGloin and Kirk 2010). Many empirical studies were conducted to clarify street gangs' characteristics: flexibility, decentralization, uncertainty, non-leadership (e.g., Curry and Decker 2002; Decker 1996; Klein and Maxson 2006; McGloin 2005; Weisel 2002). In contrast, some proved that street gangs could be structured like a business model (Padilla 1992; Taylor 1990). Based on the knowledge about street gangs, counter-crime strategies could be designed, such as removing or targeting brokerage positions and reducing criminal networks' cohesion (McGloin 2005).

SNA is also used to understand hierarchical criminal organizations (Calderoni 2012; Calderoni and Piccardi 2014; Campana and Varese 2013; Varese 2006). Calderoni (2012) suggested the measures of betweenness centrality to identify core leaders at Mafia meetings. This application of SNA can help LEAs identify better who should be focused on in their investigation activities (Calderoni 2012). Moreover, in hierarchical organizations like Mafia, arresting a single boss may not influence the whole organization as a lower-level leader is ready to replace the unoccupied position (Lindquist and Zenou 2019). Therefore, LEAs should adopt a key group strategy that emphasizes the arrest of a large group of leaders (Borgatti 2006). Whereas, for non-hierarchical criminal groups, arresting key individuals (as opposed to key groups) is likely to dismantle the whole network (Lindquist and Zenou 2019).

In cyber criminology, Décary-Hétu (2014), Dupont (2014), and McGuire (2012) are three of a few scholars applying SNA. Décary-Hétu (2014) and Dupont (2014) analyzed chat rooms' data to explore the structure of hackers' social networks. Dupont (2014) proved a significant lack of trust within these hacking groups, which can support LEAs to design counter-strategies to attack the vulnerabilities of these groups. Coping with these vulnerabilities, hackers are inclined to engage in small hacking communities rather than larger ones as there is a higher trust with security inside these small groups (Décary-Hétu 2014). LEAs and researchers face difficulties in understanding close hacking groups (Décary-Hétu 2014). However, the closeness and trust within these small groups may also be the weakness that LEAs can exploit to monitor them via undercover hackers (Décary-Hétu 2014). Moreover, McGuire (2012) used SNA to refine the emerging cybercrime group models based on data collected from case studies. As a result, a typology with three main models was proposed; each model brings about difficulties and opportunities for LEAs' disruption policies (McGuire 2012).

SNA is beneficial to interpret criminal networks; however, it also possesses potential pitfalls. Data-related problems are among the greatest challenges faced by researchers (Campana 2016). More particularly, they can include the missing data and bias in secondary sources, boundary-specification issues, errors in extracting, coding data, and wrong attributions of actors and ties (Campana 2016; McGloin and Kirk 2010). To deal with these problems, external and/or internal validity checks are recommended (Campana and Varese 2012). Moreover, both qualitative and quantitative evidence should be mixed to grasp criminal networks' full knowledge (Campana 2016; Campana and Varese 2012). Hence, with researchers' cautiousness, these potential difficulties can be overcome.

To sum up, SNA is more than a set of research methods. It can provide researchers with a "lens" to understand criminal behaviors based on social relationships. Moreover, it can be regarded as a set of tools that help researchers study social relations and their outputs. It can be adopted as an analytical technique to investigate criminal networks' structure and vulnerable positions. More importantly, SNA becomes a valuable approach to help LEAs design counter-crime strategies. Identifying central actors can assist LEAs in conducting effective disruption strategies targeting the vulnerabilities of criminal networks. However, the strict requirements related to relational data are likely to make researchers consider whether and how they should apply SNA into their studies. In comparison with other disciplines of criminology, cyber criminology is relatively new. Data limitation is one of the most severe hurdles of cybercrime studies (Bossler and Berenblum 2019; Ngo and Jaishankar 2017). Researchers can meet difficulties accessing data about cybercriminal networks such as the database of high-security underground forums or investigation files and log files saved by LEAs. These reasons possibly lead to the fact that despite numerous advantages, SNA has not yet been used much to study the nature of cybercrime networks. This study is among pioneering research to investigate cybercrime networks under the SNA approach.

2.4. The characteristics of cybercrime networks

2.4.1. The transformation of cybercrime networks

Cybercrime has experienced a transformation process from fragmented behaviors conducted by “lone wolf” hackers to increasingly professional and coordinated activities (Tropina 2012). Despite the emerging phenomenon of cybercrime networks, there is a substantial lack of scientific research on how cybercrime networks are structured and operated (Lavorgna 2016; Lavorgna and Sergi 2016; Tropina 2012). There are still debates among scholars about the nature of cybercrime networks. Generally, cyber criminologists have focused on the notion of traditional “organized crime.” Consequently, studies often argue about the characteristics of cybercrime networks similar to or different from traditional criminal organizations. Moreover, the majority of existing studies on cybercrime networks have formulated cybercrime as including a broad range of crimes in the North American and European context.

Lavorgna and Sergi (2016) criticized the emerging narrative of cyber-organized crime in policy documents. They argued that the juxtaposition of two terms, “serious” and “organized” in criminal justice policy-making, can result in the increasing narrative of this term in the UK as well as other countries (Lavorgna and Sergi 2016). The “organized” aspects often connect to the “seriousness” of online criminal behaviors, which is reinforced by difficulties in investigating and prosecuting cybercriminals (Brown 2015). As a result, cybercrime needs to be “organized” to fall within the crucial disruption policies of LEAs (Lavorgna 2016; Lavorgna and Sergi 2016). Consequently, cybercrime can be assumed to possess certain manifestations of organized crime. According to Lavorgna and Sergi (2016), this claim lacks strong evidence as only a few empirical studies focus on criminal groups' nature in cyberspace. Therefore, scholars, policymakers, and practitioners should be cautious about being misled by statements concerning “organized” cybercrime. The scarcity of strong evidence about cybercrime networks results in the requirement for more empirical studies on this issue.

Although anecdotal or circumstantial evidence suggests that cybercriminal groups may have a similar operational structure to traditional organized crime groups such as the Mafia, there is little empirical evidence that this is the case (Grabosky 2001; Lavorgna and Sergi 2016; Tropina 2012). Grabosky (2001) referred “virtual criminality” as “old wine in new bottles,” as far as it possesses aspects of terrestrial crime. The scholar argued that despite certain new elements concerning technological mediums, cybercrime is “fundamentally familiar” with traditional crime (Grabosky 2001, p.243). Cyberspace possesses the same function as physical places (e.g., the clubs, schools) in which interpersonal interactions occur and impact Internet users (Grabosky 2001). Besides, criminal motivations are not new as cybercriminals are driven by financial benefits, sexual desire, revenge, ideology, power, curiosity, and the desire for adventure and exploration (Grabosky 2001; Li 2017). The term "old wine in new bottles" has been used by some other scholars to identify the nature of cybercrime (e.g., O'Neill 2000; Omotubora 2019; Weir, Toolan, and Smeed 2011).

Moreover, traditional organized criminal groups are often believed to use cyberspace to conduct their illegal business (Glenny 2018; Goodman 2010; INTERPOL n.d.; Tropina 2012; UNODC 2010; Williams 2002). To reduce risks and generate high profits, traditional organized criminal groups must seek safe places such as territories with political tensions or weak governments (Williams 2002). Cyberspace, including anonymous, fast-connected, and borderless factors, is likely ideal for them to operate illegal activities (Goodman 2010; Tropina 2012; Wall 2015). Logically, traditional criminal organizations possibly shift their criminal activities to cyberspace (Brenner 2002). If this phenomenon exists, cybercrime networks can be structured and operated under traditional organized criminal groups' hierarchical models.

However, Tropina (2012) argued that although obviously cyberspace can bring many benefits for traditional organized criminal groups, there is still an absence of empirical evidence about this phenomenon's extent. Moreover, some examples of this phenomenon, such as using cryptocurrencies in drug-related transactions of Mafias (Glenny 2018), should not be regarded as cybercrime in nature. In such cases, traditional organized criminal groups may only use cyberspace simply for communications and/or transactions serving their territorial criminal activities. Therefore, there are still questions concerning the extent and characteristics of migration of traditional criminal groups to cyberspace (Tropina 2012; Wall 2015).

Consequently, Tropina (2012) distinguished between two categories of criminal networks in cyberspace: traditional criminal organizations using cyberspace and online criminal groups as a new form of criminal networks. Both can be considered "two sides of the coin" of criminal networks in cyberspace (Tropina 2012, p.159). The latter groups implement crimes mostly or only in cyberspace; their criminal activities have led to online underground marketplaces for illegal services and products such as malicious software, stolen credit card data, cyberattacks (The European Cybercrime Center 2014, p.19). Here cybercriminal networks are increasingly adopting business models of legitimate companies in their operation (The

European Cybercrime Center 2014, p.20; Tropina 2012). Like legitimate businesses, cybercriminal networks also have “customers” who buy illegal services and products; besides, they also employ business policies and principles like price differentiation with discounts and bonuses or various packages of products and services (Tropina 2012). Moreover, cybercrime networks possibly have a clear division of labor and defined roles (Rush et al. 2009, p.42; Wall 2015). These imitations seem similar to Mafias or other traditional criminal enterprises' methods to operate their business. Traditional criminal organizations also established companies and managed their illegal activities under the business model (Cressey 1969; Paoli 2004).

While some argue that organizations do exist in cyberspace, however, cybercrime networks tend to be constructed loosely, unlike the traditional crime structures (Brenner 2002; Hutchings and Holt 2014; Leukfeldt, Lavorgna, and Kleemans 2017; McGuire 2012). It is often argued that relationships between members are transactional or temporary within flexible cybercriminal networks (Brenner 2002; Hutchings and Holt 2014; Leukfeldt, Lavorgna, and Kleemans 2017; McGuire 2012). Moreover, the strength of online criminal groups depends on the quality of software rather than the number of individuals (Brenner 2002; Choo and Smith 2008). Additionally, violence and monopoly to control geographical markets do not seem to exist in borderless cyberspace (Tropina 2012).

Wall (1999) evaluated cybercrime as a new form of crime in borderless virtual space, like “new wine, no bottles.” Cybercrime can transform from single, fragmented behaviors to sophisticated models mimicking corporate business (Rush et al. 2009, p.42); however, the structure of cybercrime networks is still far from formal hierarchies (The European Cybercrime Center 2014, p.9; Tropina 2012). A new organizational model has emerged in cyberspace: namely, a disorganized or distributed criminal organization without agreed-upon leaders (Brenner 2002; Nurse and Bada 2018; Wall 2015). Wall (2015, p.73) focused on the transformative characteristics of cybercrime: “more professional,” “more stealthy,” “more automated,” “much larger,” “more complex,” then concluding that novel forms of online criminal groups are likely to differ much from the pyramid mafia structure. Cybercriminals are distributed across different countries and do not gather in a limited location; and their bonds via the Internet are transitory, based on the rank of reputation respect (Wall 2015). Brenner (2002, p.50) used the title of “swarming” model to describe this transformation of online criminal networks:

> …we will see the evolution of new and different modes of criminal organization in cyberspace; indeed, criminal organization in cyberspace may well be a situational concept. Specifically, instead of assuming stable configurations that persist for years, online criminal organization may incorporate the "swarming" model, in which individuals coalesce for a limited period of time in order to conduct a specifically defined task or set of tasks and, having succeeded, go their separate ways.

This nature is different from the traditional characteristics of geographically and socially rooted criminal groups (Brenner 2002; Wall 2015). Moreover, unlike traditional gangs, hacker groups seldom have an identified leader; hackers are typically responsible for their own illegal behavior and lack a clear leadership structure (Nurse and Bada 2018; Wall 2015). For example, in the *Anonymous* hacker group, members follow the same direction regarding their intentions without a stated leader (Nurse and Bada 2018; Wall 2015). Many members think of themselves as "crusaders for justice," and the structure of Anonymous is evaluated loosely as "a series of relationships" with a free membership fee (Nurse and Bada 2018, p.702).

Some scholars have examined trust between cybercriminals on the basis of online dimensions. Soudijin and Zegers (2012) referred carding forums as "virtual offender convergence settings" to clarify cybercriminal networks' vulnerabilities. In other words, online forums have become meeting points for cybercriminals to meet one another (Hutchings and Holt 2015; Soudijn and Zegers 2012). The anonymous characteristic of virtual forums can cause a large deficit of real trust between members (Décary-Hétu and Dupont 2013; Dupont 2014; Lusthaus 2012; Nurse and Bada 2018). Dupont (2014), being one of a few scholars applying SNA into cyber criminology, found out that the lack of trust makes cybercrime networks ephemeral and vulnerable to LEA's disruption. Consequently, this situation results in cybercriminals developing a range of online trust mechanisms (Décary-Hétu and Dupont 2013; Lusthaus 2012; Nurse and Bada 2018). Discounts or bonuses can be offered to attract "customers" and build the first trust within underground markets (Holt and Lampke 2010). Furthermore, a verification process can be used as the quality of products and services is verified, tested by middle-men or moderators (Holt 2013; Yip, Webber, and Shadbolt 2013). Votes or feedback from other actors contribute to one member's trust degree (Hutchings and Holt 2015; Lusthaus 2012). Besides, hackers are inclined to participate in small hacking groups with a higher level of trust and security (Décary-Hétu 2014).

Alongside online components, offline and local dimensions retain an essential position in cybercrime networks, with cybercriminal groups even thriving in offline social networks in some instances (Leukfeldt, Kleemans, and Stol 2017; Leukfeldt 2014; Lusthaus and Varese 2017). Lusthaus and Varese (2017) examined Romania's case – a cybercrime hub to prove that offline cooperation becomes a primary form of Romanian cybercriminal groups. In this case, cybercriminals often develop networks from existing relationships (such as schoolmates and neighborhood) which establish and enhance trust among members (Lusthaus and Varese 2017). Moreover, the scholars explored that violence and corruption still exist here, although the degree is not as high as the level of drug syndicates and Mafias (Lusthaus and Varese 2017). Similarly, offline and local dimensions are also important within an Amsterdam phishing network as members know and contact each other in the real world (Leukfeldt 2014).

Generally, certain studies have explored the nature of cybercrime networks; however, most of them are based on circumstantial or anecdotal evidence or a broad range of cybercrimes in the North American and European context. There is a lack of empirical research on specific cybercrime, especially in the Asian context. Existing research often focuses on clarifying cybercrime networks' characteristics on the notion of traditional "organized crime." The evolution of online criminal activities may have resulted in cybercrime networks having less formal hierarchical organizational structures. However, there are still arguments among scholars about cybercrime networks' characteristics. To understand the phenomenon of cybercrime networks, some criminologists have come to develop typologies of cybercrime groups. This literature will be reviewed in the following subsection.

2.4.2. Typologies of cybercrime networks

Developing criminal organizations' models is one efficient method to understand their structures and activities, then support LEAs to design counter-crime policies (Le 2012, 2013, pp.3,4; UNODC 2002, p.33). By adopting a social opportunity structure perspective, Leukfeldt, Lavorgna, and Kleemans (2017) analyzed phishing and banking malware networks in the Netherlands based on the characteristics of their modus operandi. Accordingly, they suggested a taxonomy of cybercrime networks, including four overlapping categories, ranging from low-tech networks with a high degree of direct offender-victim interactions to high-tech networks without such interactions. They identified clear differences between these categories when evaluating them with local and international components. Moreover, the scholars also examined four organizational positions within cybercriminal networks: "*core members,*" "*professional enablers,*" "*recruited enablers,*" and "*money mules*" as detailed below:

- *“Core members”* play an essential role in criminal groups, insofar as they initiate, direct and/or control other members to implement cybercrime.
- *“Professional enablers”* supply core members with high-quality services such as hacking tools.
- *“Recruited enablers”* provide core members with simple services such as information concerning potential victims.
- Finally, “*money mules”* are recruited for receiving illegal money, helping core members avoid financial investigations.

Leukfeldt, Lavorgna, and Kleemans (2017) argued that although the composition of cybercrime networks varies regularly, these four positions are likely to be recognized within all cybercrime networks. Moreover, sophisticated cybercrime networks might have a clear division of labor with defined positions (Rush et al. 2009, p.42; Wall 2015). These cybercrime networks can be structured by individuals and subgroups with different specialized roles and sometimes keeping multiple roles (Chabinsky 2010). More particularly, rather than having a large number of members, the most professional cybercrime networks may only need ten subject matter experts (SMEs) (Chabinsky 2010), as shown below:

- “*Coders*” or *“programmers”* specialize in writing and designing malware and tools to commit cybercrime.
- “*Distributors*” or *“vendors”* are responsible for trading, selling illegal products and software (e.g., stolen data), and guaranteeing these goods provided by others.
- “*Techies*” are in charge of technical infrastructures such as servers, encryption, and bulletproof hosting.
- “*Hackers*” search for and exploit vulnerabilities of information systems and applications to get illegal access.
- “*Fraud specialists*” design and conduct social engineering schemes consisting of spamming, phishing, and domain squatting[21].
- “*Hosts*” supply the hosting services of illegal content servers and websites such as elaborate botnets[22] and proxy services.

[21] Domain squatting refers to the behaviors of registering, purchasing, and using domain names in order to profit from the goodwill of other individuals or companies’ trademark (Hogue 2017).

[22] Botnet is a collection of infected computers that are under the remote control of an attacker (Milkovich 2020).

- "*Cashers*" handle accounts of drops and provide information about these drops to other criminals for a fee, also manage the operation of money mules.
- "*Money mules*" receive and transfer illegal money from victims to a secure location.
- "*Tellers*" support core cybercriminals to transfer and launder illegal proceeds via digital money services and different national currencies.
- "*Leaders*" keep the highest position on the specialty list as they choose targets, recruit members, manage the operation of the whole group, distribute sources and benefits.

Furthermore, based on the modus operandi and structure of criminal groups, some scholars have identified different typologies of cybercrime-related networks. Choo and Smith (2008) observed that the Internet has impacted organized crime and the criminal marketplace. Accordingly, technology-enabled crime has become more organized and sophisticated since the difference between traditional criminal groups and cybercriminal groups converges. Based on the modus operandi of crime, they clarified the differences between three general categories of cybercrime-related groups.

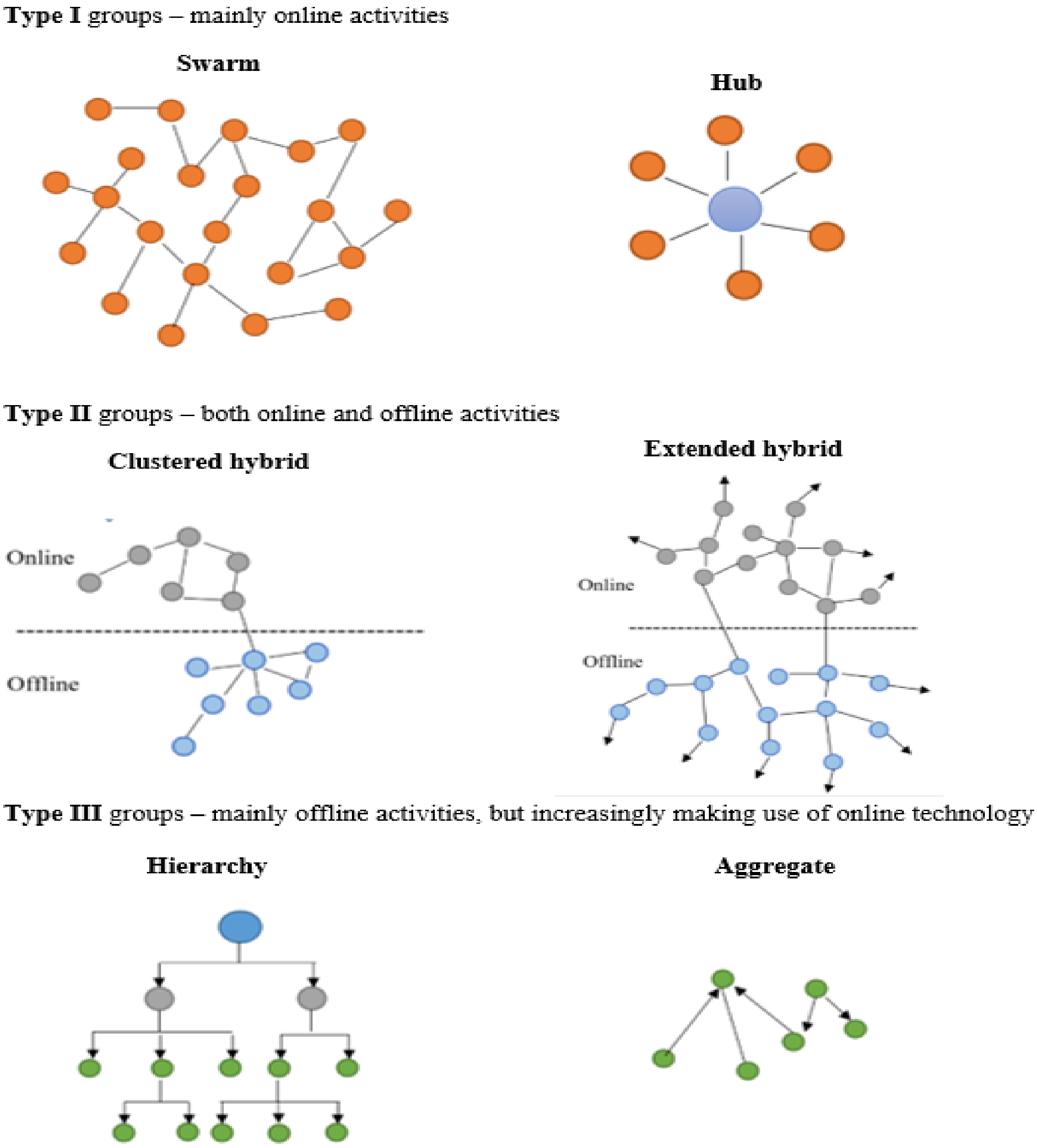
- *"Traditional organized criminals"* take advantage of cyberspace and technology to enhance their offline criminal behaviors.
- *"Organized cybercriminal groups"* such as underground credit card fraud groups or underground phishing groups often only operate online.
- *"Ideologically and politically motivated organized cyber groups"* include terrorists and hacktivists who use the Internet and ICTs as a medium for propaganda or to raise funds, collect information as well as recruiting members.

In the context of increasing state-related criminal acts, Broadhurst et al. (2014) examined the enterprise or profit-oriented cybercrime activities conducted by state actors. In addition to the three types put forth by Choo and Smith (2008), they recommended a fourth category involving "*state-sponsored cybercrime"* operations. This category involves state-private interactions, ranging from state's monopoly on cyberattacks to state's ignorance of private cyberattacks. In this respect, US agencies allege that North Korean state-sponsored hacking groups are behind a series of global cyberattacks, including the 2016 Bangladesh's bank heist, in which US$81 million were stolen, as well as the 2017 WannaCry 2.0 ransomware attacks around the world (Perez and Shortell 2019). Such cybercriminal networks require leadership, structure, and specialization (Broadhurst et al. 2014).

Using SNA to examine the structure of digital crime groups, McGuire (2012) examined a large sample of cases and concluded that about 80% of cybercrime could be involved in organized activities. He argued that some characteristics of traditional organized criminal groups should be reconsidered when groups operate online. For example, many relationships within online crime networks are extremely transitory, and the size of networks does not correlate with the consequence and scope of deviant behaviors. Furthermore, the scholar proposed a typology of cybercrime groups consisting of three main types based on groups' modus operandi. While this categorization is identical to that put forth by Choo and Smith (2008), McGuire expanded the typology by adding two subgroups to each category based on the relationship between members (see Figure 2.2).

- Type I operates primarily online, and its members often trust one another based on their online reputation. This type can further be divided into "swarms" and "hubs."
    - ✓ *"Swarm groups"*—such as the hacktivist group, Anonymous—are disorganized networks; while they have no clear leadership, they share a common purpose (Sands 2016).
    - ✓ *"Hub groups"* possess a command network, with a hub of core actors surrounded by more peripheral players.
- Type II involves groups engaging in both online and offline activities, and can be further divided into "clustered" and "extended" hybrids.
    - ✓ *"Clustered hybrids"* involve criminals gathering around a small group of individuals and conducting online and offline criminal activities.
    - ✓ *"Extended hybrids"* are less centralized and more diffuse, and comprise of many members and subgroups.
- Type III consists of groups that operate predominantly offline, but make use of online technology to facilitate their crimes. This type is subdivided into "hierarchies" and "aggregates."
    - ✓ *"Hierarchies"* are like traditional criminal groups—such as the Mafia—but transfer their illegal activities to cyberspace.
    - ✓ *"Aggregates"* are loosely organized and constitute themselves as short-lived groups without clear targets.

Figure 2.2. McGuire's typology of cybercrime networks
Source: McGuire (2012)


Type I groups – mainly online activities
Swarm
Hub
Type II groups – both online and offline activities
Clustered hybrid
Online
Offline
Extended hybrid
Online
Offline
Type III groups – mainly offline activities, but increasingly making use of online technology
Hierarchy
Aggregate

As such, following the literature on criminal networks, some researchers also suggested specific typologies to clarify the nature of cybercrime networks. The typologies can be identified based on members' specific roles, the modus operandi, and relationships within cybercrime networks. Certain important positions within cybercriminal networks are presented; however, the role of central actors within cybercrime networks has been relatively overlooked. Central actors hold a vital role inside criminal networks, which LEAs can exploit to design counter-crime strategies. Furthermore, scholars often interpret networks based on the substantive approach when clarifying cybercrime networks. It means that network models rather than hierarchical models characterize cybercriminal groups. More empirical research using the instrumental approach of SNA should be conducted to clarify specific types of cybercrime.

Meanwhile, little is known about specific cybercrime networks in the Asian context. The present study aims to provide more understanding of the structure of cybercrime networks via examining TCF, as one specific type of cybercrime in Vietnam. The study clarifies the distinguishable characteristics of TCF networks' structure and members who occupy the central points within these networks. Before exploring the structure of cybercrime networks committing TCF, it is necessary to understand TCF's modus operandi in the Vietnamese context by adopting crime script analysis. Crime script analysis is a prevalent approach to elicit criminal behaviors. Moreover, TCF's process has information about various roles that individual members adopt to implement crime. The analysis of TCF's specific stages can help the researcher identify actors, their relationships, and their roles within TCF networks. The existing literature on computer fraud and crime script analysis will be examined in the following section.

2.5. Computer fraud and crime script analysis

2.5.1. Computer fraud

Cybercrime can be viewed as a continuum, where some crimes feature only minor technological elements and others almost entirely technological elements (Gordon and Ford 2006). As presented in Section 2.2, representing one specific type of cybercrime, computer fraud can possess two levels of cybercrime: cyber-dependent and cyber-enabled aspects. Cyber-dependent crimes can be conducted only with the use of ICT, while cyber-enabled ones are traditional crimes that can be transformed in their scale and consequence by the adoption of ICT. Computer fraud behaviors are often considered the final stage after a series of earlier deviant acts. In particular, fraudsters gain access to cardholder funds after completion of a hacking, phishing[23], or skimming[24] case aimed at stealing bank card data (Peretti 2008). Similarly, with phone scams, victims lose money following fraudulent calls in which phishing techniques are often applied to steal victims' information (Choi Lee and Chun 2017; Lee 2020). In some situations, therefore, phone scams may be known as "voice phishing" or

[23] Phishing is a cyberattack technique that often uses disguised emails to obtain sensitive information (Milkovich 2020).

[24] Skimming is a method of capturing data from a bank card's magnetic stripe when the card is scanned via a swiping device ("skimmer") (VISA 2014)

“vishing” (Lee 2020). Therefore, computer fraud is often considered cyber-enabled crime, as the second aspect of cybercrime, wherein cybercriminals use ICTs to facilitate criminal behaviors. However, when examining the entire process of computer fraud: before, during, and after computer fraudsters obtain money, it may provide a more comprehensive understanding of cybercrime networks with both aspects of cybercrime.

Computer fraud has become a global threat due to the widespread application of ICTs (The National Fraud Center 2000). The unprecedented ICT revolution has allowed the remote commission of computer fraud, via the Internet and wireless communications. Computer fraudsters no longer need to travel cross-border with visas and passports to approach victims, but can still cause serious financial losses (Goodman 2010). One type of computer fraud, bank card fraud, for example, led to the global loss of more than US$27 billion in 2018 and is predicted to reach over US$35 billion in losses by 2023 (HSN Consultants 2019). Previous international studies have provided notable insights into the commission of crimes in other regions. Certain works (for example, Choi et al. 2017; Holt and Lampke 2010;; Hutchings 2014; Hutchings and Holt 2015; Lee 2020; Leukfeldt 2014; Leukfeldt, Kleemans, and Stol 2017; Peretti 2008; Shin 2018; Soudijn and Zegers 2012;) have shown that cybercriminals participating in networks use various forms (e.g., phones, emails, and banking) and aspects of technology to defraud their victims. As Grabosky (2001) discussed, the unprecedented capacity of technology to facilitate criminal behaviors has resulted in the novelty of cybercrime.

At least two types of criminal networks commit computer fraud. Technology maintains an important position in the first group, described by Soudijn and Zegers (2012); whereas social ties play a more significant role in the second, analyzed by Leukfeldt (2014). The difference between these cybercriminal networks is further highlighted by the degree of their technology use, from high-tech to low-tech networks (Leukfeldt, Kleemans, and Stol 2017). However, few studies have presented an in-depth discussion of the role of technology in defrauding the cross-border victims of TCF, particularly in the Asian context.

Bank card data fraud is among the prevalent forms of computer fraud that have received scholarly attention. It can be replaced by the term “carding” which refers to the unauthorized use of debit and credit card data for buying products and services (Meijerink 2013, pp.5,6; Peretti 2008). For example, Peretti (2008) presented a general background on notorious carding organizations in Europe and North America and their methods of committing bank card fraud. Carders (referred to individuals conducting criminal carding activities) can use many methods to obtain account information, including phishing, skimming, “dumpster diving,”[25] or “old-fashioned stealing”[26] (Peretti 2008, p.381). Besides, fraudsters use online forums as “offender convergence settings,” where cybercriminals meet to buy and sell stolen data (Holt and Lampke 2010; Holt 2013). Then, fraudsters can obtain money from victims’ bank card accounts by specific methods: “carding online,”[27] “cashing,”[28] “in-store carding,”[29] and “gift card vending”[30] (Peretti, 2008, p.390). Data extracted from online forums, as well as certain crime scripts of bank card fraud, have been analyzed by many Western researchers (Hao et al. 2015; Holt and Lampke 2010; Holt 2013; Hutchings and Holt 2015; Soudijn and Zegers 2012) to reveal insights regarding their content.

Although phone scams have become a growing social problem in Asia, few studies have examined this type of computer fraud (Choi et al. 2017). Shin (2018) noted that phone scams developed by Taiwanese criminal gangs continue to evolve and pass through China, Southeast Asia, Africa, and even South America. Such phone scams have unique characteristics compared with traditional fraud (Choi et al. 2017). These characteristics can be shown via specific activities implemented by fraudsters (Choi et al. 2017). Additionally, Lee (2020) explored the paths taken by money mules from pre-criminal behaviors to their participation in phone scams in Korea; however, the author did not discuss much how victims are defrauded, which is one of the main stages of computer fraud.

As one type of transnational cybercrime, computer fraud attacks can be conducted from anywhere in the world through network systems (Goodman 2010). It is argued that innovations driven by the Internet and modern technology will move from developed areas with strong digital economies in North America and Europe to emerging countries in Latin America, Africa, and Asia (The Internet Society 2017). Accordingly, criminals can increasingly exploit ICT innovations to defraud victims in these developing countries. TCF has become a real threat to some developing Asian countries like Vietnam (Broadhurst and Chang 2012; Lusthaus 2020).

[25] “Dumpster diving” is to search garbage cans or trash for copies of checks, bank card statements, and other sensitive information (Peretti 2008).

[26] “Old-fashioned stealing” methods involve, for example, stealing wallets, personnel records from bosses, bank card statements (Peretti 2008).

[27] “Carding online” means using stolen bank card data for online purchases (Peretti 2008).

[28] “Cashing” refers to using fake cards to withdraw cash at ATMs (Peretti 2008).

[29] “In-store carding” refers to the process of using counterfeit bank cards for paying products and services at physical store locations (Peretti 2008).

[30] “Gift card vending” refers to using fake bank cards for purchasing gift cards from merchants and reselling them (Peretti 2008).

Foreign computer fraudsters attack Vietnamese victims, while domestic fraudsters attack foreign victims. Understanding the nature of cybercrime is necessary to develop strategies against such behaviors (Bossler and Berenblum 2019; Ngo and Jaishankar 2017). Contributing to the existing knowledge about computer fraud, the present study uses crime script analysis to clarify two forms of TCF in the Vietnamese context: bank card fraud and phone scams. Subsequently, understanding the modus operandi of TCF in the Vietnamese context is the foundation for applying SNA to identify TCF networks' structure.

2.5.2. Understanding computer fraud under crime script analysis

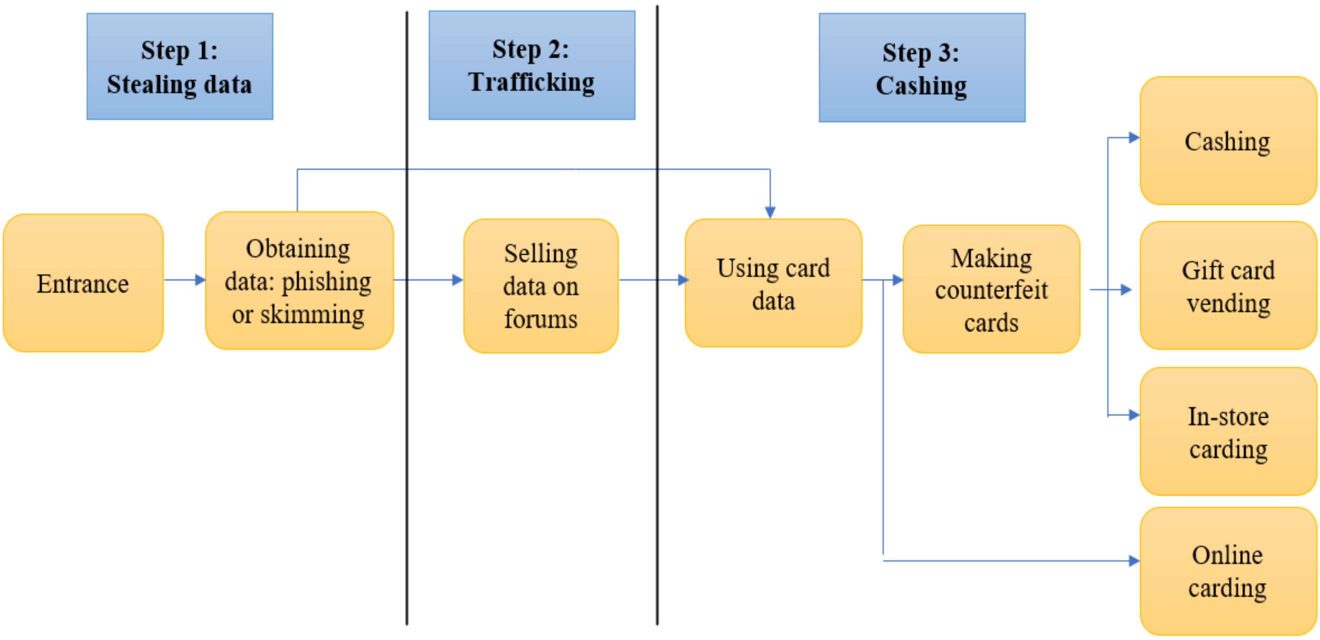
Crime script analysis was developed by Cornish (1994) and provides an effective framework for understanding all stages of the crime commission process. It identifies a crime as a process occurring over time, rather than a single event, to better clarify criminal opportunities that offenders use during the commission of a crime (Dehghanniri and Borrion 2019). Crime scripts function in stages (or “script scenes”) from preparation to post-activity, and include offenders (or “actors”) and “scripted actions” (Cornish 1994; de Bie et al. 2015; Lee 2020). These components generalize the modus operandi of a crime with a sequential flow (Cornish 1994). Crime script analysis is not merely a descriptive tool, but it also supports the development of effective situational crime prevention strategies (Dehghanniri and Borrion 2019). By identifying key scenes, this technique supports LEAs to clarify and intervene in a crime’s weak spots with the purpose of changing potential offenders’ acknowledgement of its rewards and risks (Dehghanniri and Borrion 2019).

In addition to exploring the structure of criminal networks through the SNA approach, crime script analysis offers insight into actors' roles within criminal networks (Duijn and Klerks 2014, p.129). SNA views criminal phenomena in terms of network theory, including nodes (or actors) and ties (or relationships between nodes) (Campana 2016; Lindquist and Zenou 2019; von Lampe 2003). Crime script analysis provides researchers with a systematic blueprint to identify these nodes with their roles and ties during the different crime phases (Duijn and Klerks 2014; Sparrow 1991). Moreover, one of the advantages of crime script analysis is the capacity to reveal the variation, flexibility, and evolution of crime, suitable for identifying criminal networks' nature (Dehghanniri and Borrion 2019). Therefore, crime script analysis is useful for combining SNA to expose criminal networks' nature.

Due to these advantages, crime script analysis has been increasingly applied to analyze both territorial crime and cybercrime (see Dehghanniri and Borrion 2019). It has also been adopted in the analysis of some forms of computer fraud with various criminal processes. Focusing on bank card data fraud, Meijerink (2013) used crime script analysis to highlight carding processes in order to propose effective counter-strategies. Using online news data, which is not highly reliable, the scholar described specific processes and models of carding. Meijerink (2013) analyzed the carding script with the process of stealing data, trafficking, and cashing (see Figure 2.3). Meijerink (2013) and Peretti (2008) shared many similarities about carding's modus operandi. Among them, phishing and skimming are popular methods that carders use to steal bank card data. Subsequently, stolen bank card data can be traded online before being used to obtain money from victims' bank accounts (Meijerink 2013; Peretti 2008). Based on the results of carding processes, Meijerink (2013) developed barrier models and techniques of situational crime prevention. Using limited data from online news, Meijerink tried to provide some information about the commission of bank card data fraud. As he admitted the limitations of this study, future research based on more reliable data sources should be implemented to update and expand the modus operandi of bank card data fraud.

Crime script analysis also supported Hutchings and Holt (2015) to explore the online underground economy relating to stolen data. Credit card details are only one type of stolen data sold on these virtual forums. The research data was extracted from English and Russian-speaking underground forums. Their study clarified "dark" marketplaces' actors and their illegal

Figure 2.3. Carding scripts identified by Meijerink (2013)

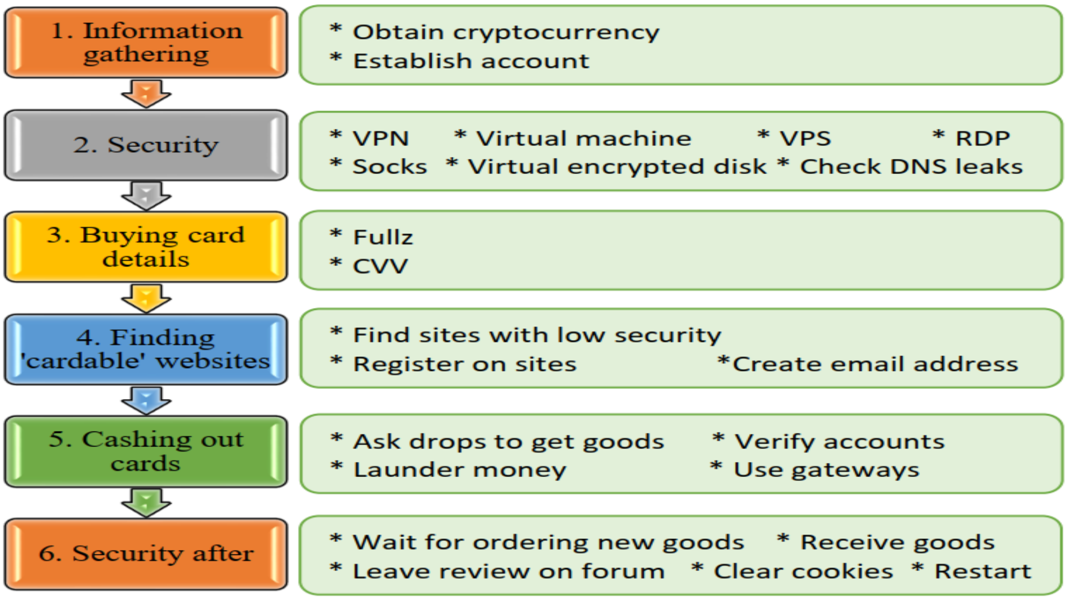


processes. Marketplaces can involve the participation of many actors, such as sellers, buyers, moderators, suppliers, administrators, and teachers with different roles. They conducted specific scripts which can be organized from the preparation stage to post-condition and exit.

From the analysis of online tutorials published by hackers, van Hardeveld et al. (2016) proposed a six-step process with the most popularly advised carding scripts (see Figure 2.4). After preparing cryptocurrency and pseudonymous accounts, carders are advised to enhance security to prevent the detection of LEAs. Subsequently, carders should buy credit card data on trustworthy hacking forums before finding "cardable" websites where card data can be used to order products or services. At the post-activity stage, carders are recommended to delete evidence. Crime script analysis also assisted the scholars in developing preventive measures based on the situational crime prevention approach. However, van Hardeveld et al. (2016) only focused on the most common carding paths described in tutorials. Further research based on other data sources should be required to spot anomalies of bank card data fraud.

Additionally, Leukfeldt (2014) applied crime script analysis to an Amsterdam case in which fraudsters used fraudulent emails and a phishing website to access victims' online bank accounts. After gaining access to victims' bank accounts, fraudsters made a phone call to trick the victims into obtaining transaction codes. When receiving these codes, computer fraudsters immediately transferred money from victims' bank accounts to money mules' accounts. Besides, he discussed three layers of members inside this phishing network, including core members, facilitators, and money mules. Move valuably, the crime scripts of this phishing case provided

Figure 2.4. Carding scripts identified by van Hardeveld et al. (2016)



capacities for situational crime prevention. Accordingly, Leukfeldt suggested prevention strategies focusing on the crime's weak spots concerning fraudulent telephone calls, phishing signals, money mules, or banks' preventive measures.

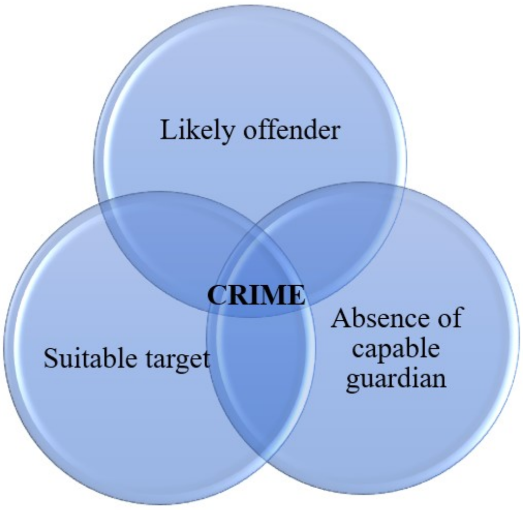
Concerning phone scams, Lee (2020) utilized crime script analysis to understand each phase of offenders' actions better. Lee's work is among a few studies on computer fraud in the Asian context. The analysis drew upon the author's ethnographic data, revealing the path of transnational phone scams targeting Korean victims. The scripts of phone scams were divided into several main steps: recruitment, migration, training, calling victims, and withdrawing money. However, the study mainly focused on criminal activities conducted by money mules, while the process of calling victims was still unknown because of a lack of information. She collected ethnographic data via interviewing money mules who were regarded as low-level members inside fraudulent networks. They did not clearly know other activities implemented by core members. Therefore, there is a missing scene that should be clarified by further research.

As a follow-up to the extant studies on computer fraud, one crucial part of this study utilizes crime script analysis to clarify two types of TCF in the Vietnamese context: bank card data fraud and phone scams. In particular, it aims to explore how computer fraudsters are involved in criminal activities, as well as what tools and techniques are used to defraud transnational victims in Vietnam. Crime script analysis is appropriate for combing SNA to explore the nature of TCF networks. Examining the modus operandi and structure of TCF networks may assist LEAs in designing and applying counter-crime strategies. Besides SNA and crime script analysis, one part of this thesis adopts RAT to analyze the reasons for cybercrime in Vietnam. Therefore, it is important to review RAT and check suitability to cooperate RAT with SNA and crime script analysis. This content will be presented in the following section.

2.6. Routine activity theory and its application in cyber criminology

Felson and Cohen firstly presented RAT for analyzing predatory crime rate change in the US in the 1947-1974 period (see Figure 2.5). Subsequently, RAT has been broadly applied to the examination of a wide range of crimes. The theory elucidates that crime occurs when three factors — likely offenders, suitable targets, and the absence of capable guardians — appear together in one space and time (Cohen and Felson 1979). Offenses are neither random nor trivial incidences, but they happen in social situations in which there is an interdependent relationship between inclinations for committing crimes, attractive targets appearing from routine activities, and the degree of deficient protection and surveillance given by guardians for

Figure 2.5. Three main factors of RAT developed by Cohen and Felson (1979)



all levels (Cohen and Felson 1979). In other words, if there are an unprotected target and a sufficient benefit, a motivated offender will conduct illegal behaviors.

At the time RAT was firstly recommended by Cohen and Felson (1979), the Internet did not appear. Originally, RAT focuses on a physical location where likely offenders, suitable targets, and the absence of capable guardians meet. When being adapted to the examination of cybercrime, RAT is modified without the requirement of a physical meeting between offenders and victims. The integrity of RAT is shown by the interaction between them via a network (Eck and Clarke 2003; Reyns 2013). Therefore, RAT is valuable to both traditional crime and cybercrime.

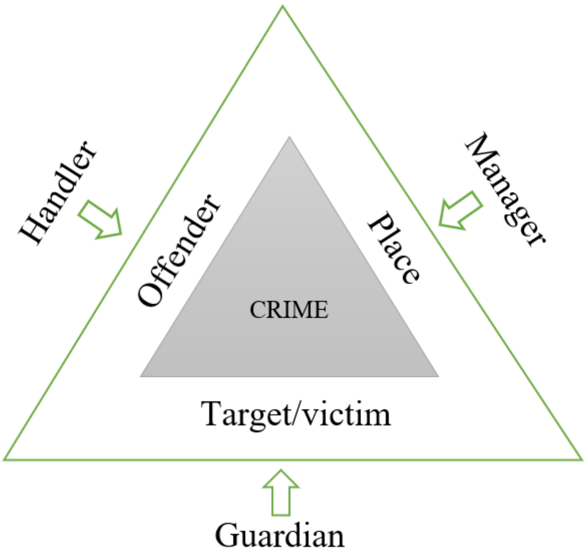
Likely offenders are individuals who are willing to commit criminal behaviors and are capable of doing so (Miró 2014). Likely offenders have various reasons and motivations for committing crimes. Despite rapid changes of technology, human nature does not alter as motivations of likely cyber offenders are nothing new (Grabosky 2001; Navarro and Jasinki 2012). Likely offenders are motivated by many reasons like financial benefits, political movement, curiosity, or revenge (Grabosky 2001; Li 2017). Moreover, the expansion of networks and communication leads to increasing opportunities and decreasing risks for potential offenders (Grabosky 2001; Navarro and Jasinki 2012). High opportunities and low risks contribute to the motivation of likely offenders. Besides, likely offenders must have the capacity to conduct criminal behaviors, physically and mentally (Miró 2014).

Suitable targets refer to any individual, property, and place that can be threatened by likely offenders (Miró 2014). The probability that targets become suitable for being attacked by likely offenders is impacted by four dimensions (value, inertia, visibility, and access) (Miró 2014). The valuation of targets is a critical factor for cybercrime as the possible rewards far outweigh the potential punishment and consequences (Yar 2005). Inertia refers to the physical properties of objects or persons. Applying this dimension to cybercrime seems more ambiguous because the targets of cybercrime are often digital "weightless" information (Yar 2005). Visibility means that potential offenders must recognize the existence of targets (Bennett 1991). If the visibility of traditional targets is often limited by barriers of physical distance, the targets of cybercrime can be known widely by many potential offenders owing to ICT networks (Yar 2005). The last dimension is accessibility which is explained as characteristics of targets influencing the capacity of offenders to get to the target and then escape from the scene (Felson 1998).

The final factor of RAT is the absence of capable guardians. The definition of guardians should not be restricted to LEAs or security guards (Miró 2014). This concept has been updated practically since its first formulation. Guardians can be individuals (e.g., police, security guards, place managers), objects (e.g., security cameras, gates, firewalls, anti-virus software), or social control that can intervene and deter crime from occurring. The absence of these capable guardians can increase the chances of crime. Therefore, control is a critical element in preventing crime (Cohen and Felson 1979).

Since its initial formulation, RAT has contributed much to situational crime prevention that aims to increase risks and reduce opportunities of crime (Miró 2014). Clarke and Eck (2016) summarized prevention measures into a problem triangle including three elements (offenders, targets/victims, and places) (see Figure 2.6). Crime occurs when three factors - likely offenders, suitable targets, and the absence of capable guardians – appear together in

Figure 2.6. The crime triangle suggested by Clarke and Eck (2016)



one time and space (Cohen and Felson 1979). Hence, concerning crime prevention, offenders, targets/victims, and places should be under control (Clarke and Eck 2016; Miró 2014). The triangle has "controllers" responsible for supervising behaviors relating to each element. More particularly, handlers control offenders, guardians are responsible for targets/victims, and managers supervise places (Clarke and Eck 2016).

Given the emerging risks of cybercrime, scholars have utilized RAT to understand cybercrime. For example, Choi (2008) proved the parallel relationship between risky online behaviors and the odds of virus victimization. Additionally, Pratt, Holtfreter, and Reisig (2010) explained that the long online time increases the capacity for computer fraud targeting. Online-shopping and forum participation increase the odds for computer fraud victimization (van Wilsem, 2013). Kigerl (2011) used RAT to explain cybercrime at the national level with two important conclusions. First, nations with higher Internet penetration had more cybercrime activities, and second, high unemployment may increase cybercrime activities. These results have proved the value of RAT when it is modified to examine crime in cyberspace.

The RAT approach is at the core of environmental criminology (Wortley and Mazerolle 2008). In history, understanding criminal behaviors via interactions between suspects and their social situations established the foundation for studies on criminal organizational systems (Morselli 2009). Moreover, in terms of counter-crime policies, RAT is strongly linked to situational crime prevention, which can help LEAs design preventive methods against crime by reducing crime opportunities (Wikström 2009). This idea shares suitability for the meaning of crime script analysis. Crime script analysis also supports the clarification of weak spots and the design of situational crime prevention (Dehghanniri and Borrion 2019). In this study, RAT is used to understand cybercrime at the macro-level (or national level) in Vietnam. SNA and crime script analysis are adopted to understand specific TCF cases. Moreover, in Chapter VII, these three analytical approaches cooperate in assisting the researcher in presenting recommendations for countermeasures, particularly prevention and investigation strategies.

2.7. Conclusion

The state of research on cybercrime networks and TCF provides certain understandings of the structure of cybercrime networks and TCF's modus operandi. Existing research mainly focuses on the North American and European contexts. Despite some debates, cybercrime networks are often evaluated to operate within loose structures differing from traditional hierarchical models. However, much past research on cybercrime networks is based on anecdotal or circumstantial evidence or cybercrime as including a broad range of behaviors. There is still a lack of empirical studies that clarify TCF networks as one specific type of cybercrime, especially in Asia. Besides, some scholars have proposed some typologies of cybercrime networks based on actors' role, the methods conducted by criminals, and the structure of criminal networks. More research should be done to examine the extent to which these typologies are applied to cybercrime groups in other contexts.

This chapter has also reviewed the development of the criminal network perspective and SNA in criminology. Under the "coming of networked criminology," SNA is beneficial for assisting scholars in understanding crime networks. However, the SNA approach has not been adopted much to understand online crime networks. This study is one of the first works using SNA to explore the organizational structure and central actors of cybercrime networks. Besides, the crime script analysis approach is used to investigate the modus operandi of TCF in the Vietnamese context, providing the foundation for study on TCF networks' structure. It helps the researcher identify actors, roles, and relationships, which are core units of SNA. RAT has been examined to understand three necessary factors of crime, namely likely offenders, suitable targets, and the absence of capable guardians. The next chapter presents a general picture of cybercrime and its regulations in Vietnam, which provides a background for identifying the nature of TCF networks.

CHAPTER III. CYBERCRIME AND CYBERSPACE REGULATION IN VIETNAM

3.1. Introduction

This chapter examines the general context of cybercrime and cyberspace regulation in Vietnam, which provides a background for clarifying the modus operand and structure of TCF networks. Furthermore, the knowledge of Vietnam's cybersecurity regulation is essential for the researcher to recommend counter-crime strategies. This chapter has five major sections. After the introduction, the second section presents the cybercrime context of Vietnam. It starts with a brief picture of Vietnam's negative reputation on cybersecurity, then admits the iceberg of cybercrime and computer fraud in Vietnam. To cope with cybercrime, Vietnam must enact cyberspace regulation, which will be explained in detail in the third section. Subsequently, the fourth section examines Vietnam's international cooperation policy against cybercrime. The last section concludes this chapter by highlighting the main points of cybercrime and cyberspace regulation in Vietnam.

3.2. Vietnam's cybercrime context

3.2.1. Vietnam with a negative reputation concerning cybersecurity

Within two decades of the Internet officially launching in Vietnam, the penetration rate reached 70.4% of the total population, or about 68.5 million users in December 2018 (Internet World Stats 2020). Moreover, based on Resolution 52-NQ/TW (2019), the Vietnamese Government has identified ICT as a key factor in developing the country and has clarified specific targets to transform Vietnam into one of the leading modern technology centers by 2045. Primarily driven by the growing number of Internet users and ICT applications, the 2018 Internet economy of Vietnam was leading among all Southeast Asian nations with the highest percentage of gross merchandise value to GDP (at 4% of GDP) (Google and Temasek 2018). However, the expansion of ICTs and increased Internet penetration have also raised concerns about cybercrime (Symantec 2018).

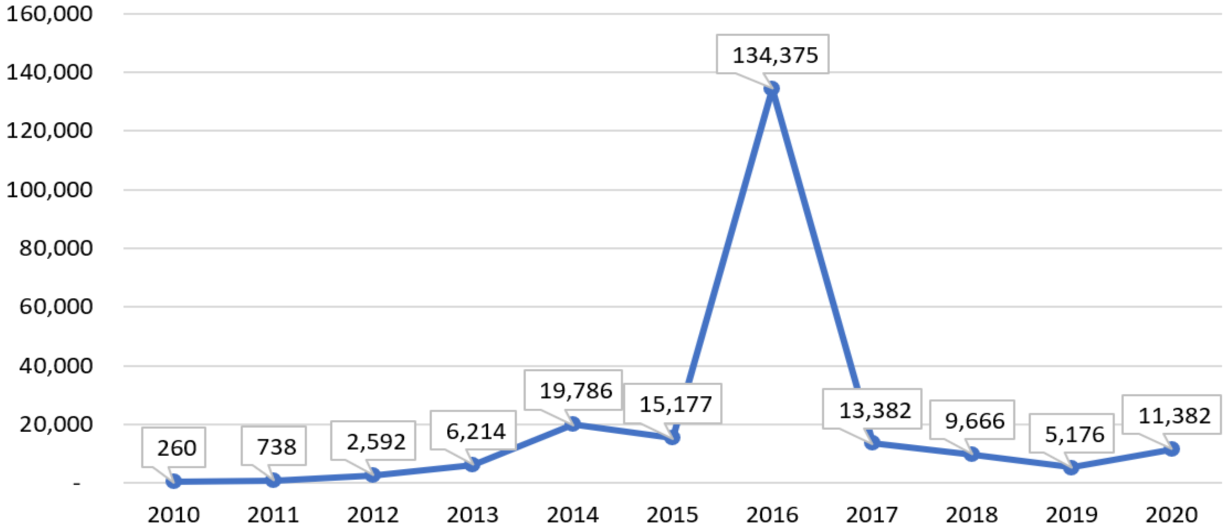
Vietnam is among the top countries in the world to suffer a negative reputation concerning cybersecurity. In February 2018, the Center for Strategic and International Studies (CSIS), in collaboration with McAfee, released a report which characterized Vietnam as a new cybercrime center, along with other countries, including Brazil, India, and North Korea (CSIS and McAfee 2018). In the period from the fourth quarter of 2017 to the end of 2018, Vietnam belonged to the top ten global attack source distribution countries and was ranked No. 1 in Southeast Asia (Nexusguard 2017, 2018a, 2018b, 2018d, 2018c). The country was listed among the top ten positions in the world concerning the highest malware encounter and infection rates for the period from July 2015 to June 2016 (Microsoft 2015, 2016). It maintained the third position among the top 25 countries in the world with the highest number of suspected botnet IPs in 2016-2017 (Botnet-tracker 2017, 2018). It was ranked third in 2017, fourth in 2018 in the list of spamming countries, and sixth among countries targeted by malicious mailshots in 2018 (Vergelis, Shcherbakova, and Sidorina 2019).

Additionally, as a victim of cybercrime, Vietnam is among the countries hardest hit by targeted attacks. Symantec (2018) ranked Vietnam ninth among the top ten countries affected by targeted attacks between 2015 and 2017. In the Kaspersky Security Bulletins of recent years, Vietnam was considered infamous for some categories of statistics concerning cybersecurity, including crypto-ransomware and infection. Crypto-ransomware attacks are evaluated as an emerging cyber threat to critical infrastructure and industrial control systems (Zimba, Wang, and Chen 2018). In 2017, Vietnam was ranked third among countries attacked by encryptors, with 1.95% of users attacked, and sixth among nations where users faced the greatest risk of online infection, with 35.01% of users attacked (Kaspersky 2017). In 2018, Vietnam continued to remain at the top among countries attacked by encryptors, holding the fifth position (2.12% of users attacked), and the 11th position among countries under the greatest risk of online infection (34.45% of users attacked) (Kaspersky 2018). Moreover, Vietnam led the list of countries where users faced the highest risk of local infection both in 2017 and 2018 (Kaspersky 2017, 2018).

In addition to the data from international sources, some domestic organizations in Vietnam also monitor and produce statistics on malicious activities in cyberspace. The VNCERT recorded 218,738 cyber-attacks on Vietnamese websites from 2010 to 2020 (see Figure 3.1). In 2016, when the information systems of Vietnam's airports were first

Figure 3.1. Cyber-attacks on Vietnamese websites recorded by VNCERT (2010-2020)

Note: Data from (APCERT 2019, 2020, 2021)



compromised, cyber-attacks spiraled upwards to 134,375 incidents. On July 29, 2016, airport screens and speakers of two major airports in Vietnam were controlled by hackers to post derogatory messages against the claims of Vietnam and the Philippines in the sea-related dispute with China (HTCP Department 2016). More than 100 flights were delayed, and the data of over 400,000 members of Vietnam Airlines' fliers club, Golden Lotus, were leaked online (HTCP Department 2016). One year later, Vietnam airports' information systems were attacked again by two domestic hackers (HTCP Department 2017). The websites of many airports were defaced to change their visual appearance (HTCP Department 2017).

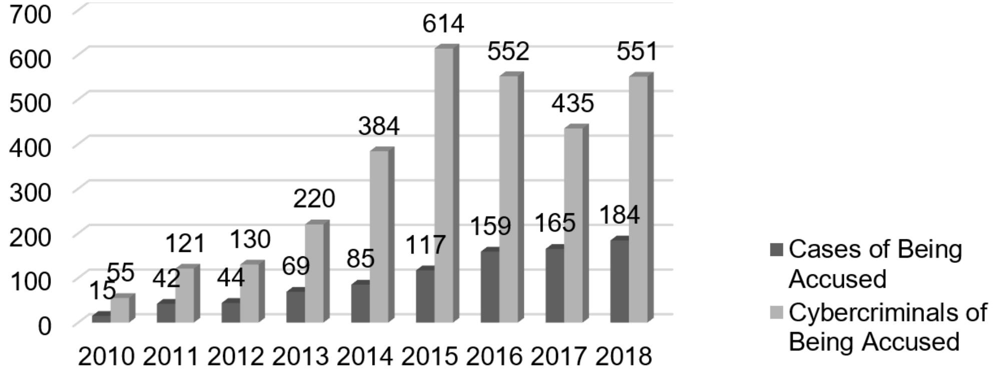
3.2.2. "Iceberg" of hidden cybercrime and computer fraud in Vietnam

The number of cybercrime cases investigated by the HTCP is very low when compared to the number of cyber-attacks in Vietnam. The number of "cases of being accused" rose steadily from 15 in 2010 to 184 in 2018 (see Figure 3.2). This statistic is only like the "iceberg" of hidden crimes, as many cases have not been detected by LEAs. It may result from the fact that cybercrime is seldom recognized by victims (ISACA 2019a, 2019b; Standler 2002). Cybercrime victims do not often detect that their computer is hacked, or their bank account data is stolen until serious consequences happen or investigators inform them. Besides, cybercrime is among the most unreported forms of criminal cases (Gercke 2012; ISACA 2019a, 2019b). The fear of damaging reputation or the lack of belief in LEAs can restrict victims from reporting cybercrime to authorities (Gercke 2012; Kshetri 2010).

On average, the number of accomplices was more than three persons per accused case during the 2010-2018 period. The standard interpretation of "organized crime" regulated in the

Figure 3.2. The number of cybercrime cases and cybercriminals being accused in Vietnam (2010 – 2018)

Note: *Data from HTCP Department (2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017) & Department of Cybersecurity and Counter High-tech Crime (2018)*



UN Convention against Transnational Organized Crime was formed on the basis of the participation of three or more persons. Hence, analyzing the average number of cybercriminals per case can prove the organizational characteristic of cybercrime in Vietnam. It reflects the characteristic that cybercrime is highly coordinated as cybercriminal networks are established to commit computer crime (Hutchings 2014; Lusthaus 2012; Nurse and Bada 2018).

During the 2010-2018 period, Vietnamese HCTP investigated many different types of cybercrime such as illegal access, data or system interference, online gambling, extortion, and child pornography. Computer fraud is among the most popular cases processed by Vietnamese HTCP, and it causes severe financial loss (HTCP Department 2015, 2016). The Vietnamese central statistical system on crime cannot provide the exact number and consequences of computer fraud cases; however, infamous cybercrime cases are listed in HTCP's annual reports. In the 2010-2018 period, 45 out of 81 listed cases belong to computer fraud. Accordingly, in computer fraud cases investigated by Vietnamese cyber police, criminals conducted various fraudulent methods, including phishing, online "Ponzi scheme", Internet banking service-related techniques, bank card data fraud, and phone scams.

More specifically, computer fraud with various crime scripts has become an increasing threat in Vietnam (Ministry of Public Security 2020). In coping with phishing fraud, many Vietnamese banks have warned about this technique in which fraudsters use emails or message services to lure victims to fake bank websites. For example, one Vietnamese victim lost VND848 million (about US$42,400) in 2020 after accessing a fraudulent website (Hai 2020). Moreover, in online "Ponzi scheme" cases, victims could be defrauded after investing huge money into online services concerning virtual currency or e-commerce. These services focus on attracting new investors by the promises of high profits with little or no risk. After a period, the whole system would collapse as investors could not withdraw their profits. In the *muaban24* case, fraudsters used the online "Ponzi scheme" technique to cause the financial loss of VND631 billion (about US$31.5 million) (HTCP Department 2012). In 2016, Vietnamese cyber police arrested three cybercriminals who had exploited the errors of Internet banking service to obtain VND3 billion (about US$150,000) (HTCP Department 2016). In these phishing, "Ponzi scheme," or Internet banking service-related cases, both fraudsters and victims often are Vietnamese.

Whereas the transnational dimension is prominent in the cases of bank card data fraud and phone scams. Concerning bank card data fraud, Vietnam is one of the top countries in terms of hacking capabilities, in which the local community of "black hat" hackers[31] poses dangerous transnational threats (Lusthaus 2020). Vietnamese hackers have attacked and used a foreign credit card database to steal money (HTCP Department 2010, 2013, 2014, 2015). The *mattfeuter* websites, operated by Vietnamese hackers from 2007 to 2013, were regarded as one of the world's major carding forums (FBI 2013; HTCP Department 2013); they had approximately 16,000 members who made at least US$200 million in bank card charges (HTCP Department 2013). Many other Vietnamese carding forums, such *vefamily, hkvfamily*, and *vietexpert,* were used as "virtual meeting points" for hackers and potential criminals (HTCP Department 2010, 2011, 2014, 2015). More recently, Vietnam has had to cope with an increasing number of phone scams (Ministry of Public Security 2020). These phone scams have originated from or targeted Vietnam from the outside. In the first half of 2020, the country's police forces received 776 reports about computer fraud, which caused the loss of thousands of billions of Vietnamese Dong (Ministry of Public Security 2020). Remarkably, 65% of these reports were related to phone scams in which offenders pretended to be law enforcement officials in order to defraud victims (Ministry of Public Security 2020).

In conclusion, Vietnam could become both a host to, and a victim of cybercrime. Based on some reports of international organizations, Vietnam has a bad reputation for certain criteria of cybersecurity (e.g., sources of cyber-attacks or spam, countries targeted by malicious mailshots, and malware infection). The data provided by domestic and international organizations show that Vietnam has faced cybercrime threats from both within its territory and outside. Within cases investigated by HCTP, computer fraud is among the most popular cases in comparison with other cybercrimes, causing serious financial loss. Bank card data fraud and phone scams are two common types of infamous TCF cases. Undoubtedly, the Vietnamese Government does not want the country to become a "safe haven" or "center" of cybercrime, especially when more and more cybercrime cases have been solved by HTCP. Nevertheless, the number of real cyber-attacks is extremely higher than the figure of processed cases. It means that a large number of cybercriminals have still hidden in the darkness. Countermeasures should be designed and adopted to bring them to justice and prevent cybercrime occurrence.

[31] "Black hat" hackers refer to hackers who attack information systems, steal sensitive information with the aim of harming the owners or users (Milkovich 2020).

3.3. Cyberspace regulation in Vietnam

3.3.1. Cybersecurity policy: Central players of cyber police and joint liability of other stakeholders

As analyzed above, Vietnam has coped with malicious acts in cyberspace from both internal and external territory. Although the Vietnamese Government has stepped up efforts to secure national information systems, the ability to defend against cyber-attacks is still evaluated as weak, especially in the event of persistent cyber-attacks (Ministry of Public Security 2017). Vietnam can be evaluated as a cybercrime center and among countries hardest hit by targeted attacks, but the Government of Vietnam surely does not want the country to turn into a "safe haven" of cybercrime. The assurance of cybersecurity is the priority shown through many specific strategies of the Vietnamese Government (Lam 2020). To ensure cybersecurity, Vietnam has enacted many policies and laws, especially Resolution 52-NQ/TW, dated 27 September 2019 of Political Bureau of the Party Central Committee about "Guidelines, Policies on the Nation's Proactive Involvement in the Fourth Industrial Revolution," the 2018 Law on Cybersecurity, the 2015 Law on Network Information Security, the 2015 Penal Code and the 2015 Criminal Procedure Code.

Resolution 52-NQ/TW (2019) affirms that Vietnam has taken decisive actions to make good use of the Fourth Industrial Revolution. Moreover, this document clarifies specific targets through 2025, 2030, and vision toward 2045. More specifically, Vietnam has determined to rank the top three of ASEAN nations in the Global Innovation Index report by 2025, with the digital economy making up 20% of GDP. Furthermore, Vietnam targets the top 40 global nations in the Global Innovation Index rankings, with the digital economy accounting for 30% of GDP by 2030. The vision toward 2045 identifies Vietnam as one of the leading modern technology centers in socioeconomics, environment, national defense, and security. Resolution 52-NQ/TW identifies two guidelines and six central policies to achieve the objectives. Accordingly, Vietnam implements sustainable development by accelerating digital transformation and ensuring cybersecurity.

There is a difference between the two terms "cybersecurity" and "information security" in Vietnamese legislation. Based on Article 2 of the 2018 Law on Cybersecurity, "cybersecurity" means "the assurance that activities in cyberspace do not cause harm to national security, social order and safety, rights and legitimate interests of agencies, organizations, and individuals." Whereas, "information security" is regulated by Article 3 of the 2015 Law on Network Information Security. "Information security" is the protection of information and network information systems against unauthorized access, use, disruption, modification, or destruction to ensure the integrity, confidentiality, and availability of information. While "information security" focuses on operating information systems stably, "cybersecurity" ensures activities to operate legally in cyberspace.

In Vietnamese cyberspace policy, cybersecurity is one significant part of national sovereignty (Quyen 2020). 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 (Lam 2020). At the 8th Seoul Defense Dialogue 2019, Vietnamese Deputy Defense Minister Nguyen Chi Vinh confirmed that cyberspace becomes "a new strategic space, a special sovereignty area" (Trung 2019). The former Vietnamese President Tran Dai Quang (2015, p.76) emphasized the national territory in cyberspace[32], which bears "cyber borders,"[33] "cyber border gates,"[34] and "cyber border guards."[35] All these statements prove that cyberspace activities must be under the Vietnamese Government's management with the principle of national sovereignty.

The Ministry of Information and Communications presides over information security, whereas the central actor of ensuring cybersecurity is assigned to the Ministry of Public Security. Based on Article 8 and Article 36 of the 2018 Law on Cybersecurity, Article 16 of the 2018 Law on Ministry of Public Security, police forces are in charge of presiding over coordination with other Ministries to protect cybersecurity and combat cybercrime. Before 2018, the Ministry of Public Security had two main entities dedicated to cybercrime and cybersecurity, including the HTCP Department and the Cybersecurity Department. HTCP Forces were specialized in preventing and investigating cybercrime, including, for example, computer fraud, malware distribution, and DDoS

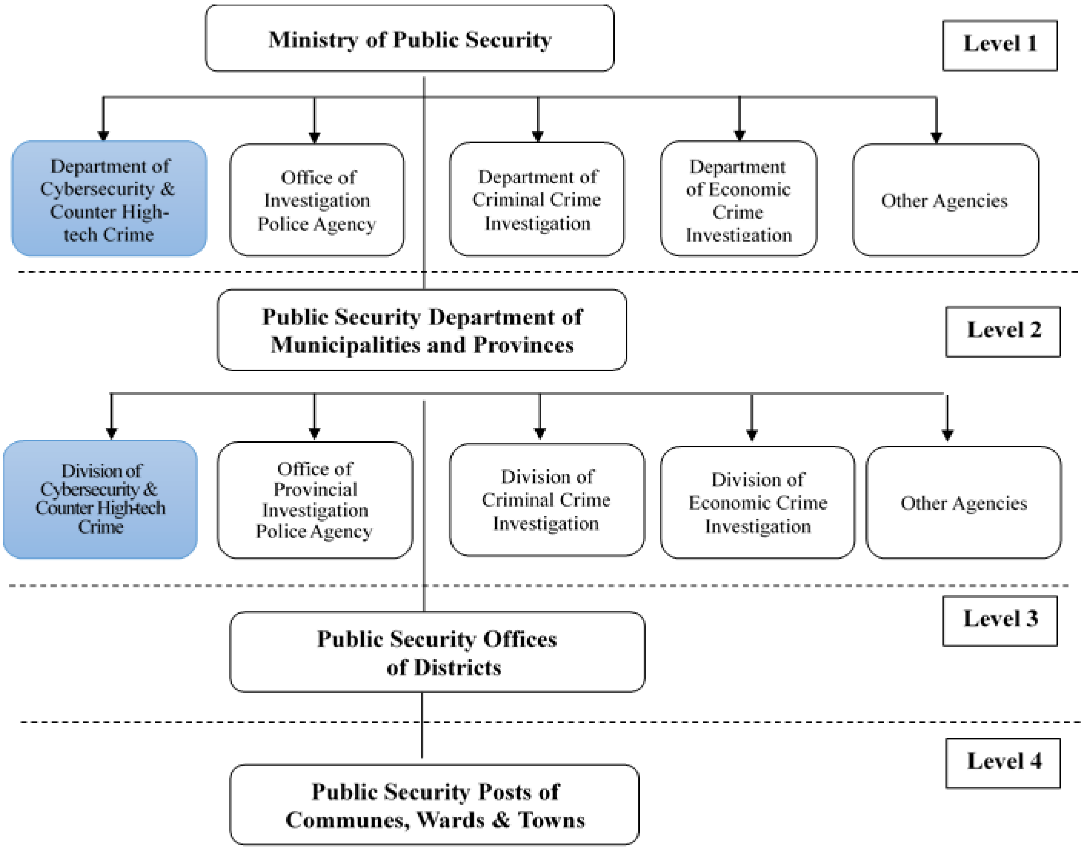
[32] National territory in cyberspace (or cyberspace territory) includes information areas that the State manages, controls directly or indirectly with policies, regulations, and technology capacities; it is a part integrating into the national territory (Dai 2015, p.66).

[33] Cyber border is clarified by factors including but not limited: cyberspace infrastructure operating inside the national territory and owned by organizations, individuals of that country; all activities of using, exploiting, and applying ICT via this cyberspace infrastructure; all network resources such as IP addresses; all national domain names and others domain names owned by organizations, individuals of that country; all other property, information, and information systems owned and managed by that country (Dai 2015, p.76).

[34] Cyber border gate is an element of cyber border. Therein lie the activities of exchanging network traffic between the national territory and the global network area. Cyber border gates are set up at national connection gateways (Dai 2015, p.77).

[35] Cyber border guards are in charge of implementing government management functions, enforcing national regulations at cyber border via policies, regulations, and technical tools (Dai 2015, p.78).

Figure 3.3. The organizational structure of Ministry of Public Security


Ministry of Public Security
Level 1
Department of Cybersecurity & Counter High-tech Crime
Office of Investigation Police Agency
Department of Criminal Crime Investigation
Department of Economic Crime Investigation
Other Agencies
Public Security Department of Municipalities and Provinces
Level 2
Division of Cybersecurity & Counter High-tech Crime
Office of Provincial Investigation Police Agency
Division of Criminal Crime Investigation
Division of Economic Crime Investigation
Other Agencies
Public Security Offices of Districts
Level 3
Public Security Posts of Communes, Wards & Towns
Level 4

attacks. The HTCP Department in 2010 officially marked a milestone in combating cybercrime. Subsequently, the HTCP Forces were established at the Provincial Police level of 31 provinces (in all 63 provinces of Vietnam) (as of November 30, 2017) (HTCP Department 2017). The Cybersecurity Department, founded in 2014, oversaw the management and administration of information system security and cybersecurity concerning sovereignty. In 2018, the Cybersecurity Department and the HTCP Department merged into the Department of Cybersecurity and Counter High-tech Crime. At present, cyber police officials work at two levels, including the Department of Cybersecurity and Counter High-tech Crime at the central level, and Divisions at the provincial one (see Figure 3.3).

Prevention and investigation are two core aspects of cybercrime countermeasures under the duty of the Ministry of Public Security. This content is regulated by Article 36 of the 2018 Law on Cybersecurity, Article 15, and Article 16 of the 2018 Law on Ministry of Public Security. Crime prevention includes measures and strategies that aim to reduce the possibility of crimes happening, as well as their potential influences on individuals and society (Nghia and Binh 2014; UN Economic and Social Council 2002). Criminal investigation is the process of gathering facts (or evidence) to identify the offenders of a crime or an intended crime (Nghia and Binh 2014; UNODC 2006, p.1).

In Vietnam's criminal policies, prevention is a core content of the fight against crimes. More particularly, crime prevention is a significant part of maintaining security stability, and it requires a duty of all individuals, organizations in which LEAs keep a central position (Quang 1999; Yem 2001). Crime prevention is often viewed with two levels: broad and narrow ones (Nghia and Binh 2014; Viet 2008). At the broad level, crime prevention activities are implemented by all members of society. The narrow level focuses on the duty of LEAs to eliminate or reduce reasons for crimes. At this scope, in counter-cybercrime policies, cyber police, as a central actor, need to implement various techniques to prevent cybercrime from occurring and reduce consequences on victims.

Strategically, criminal investigation is a process of generating and testing investigative hypotheses[36] to find the truth of criminal cases (Ask 2006, p.3; Greenwood et al. 1977; Nghia and Binh 2014; Sunde 2020). Through this process, investigators must collect facts to answer main questions: how, why, where, when, and by whom a crime was conducted (Greenwood, Chaiken, and Petersilia 1977; Thuat 1998). In Vietnam, criminal investigation includes a process with three stages: "initial investigation," "subsequent investigation," and "the end of investigation" (Nghia and Binh 2014, Thuat 1998). Accordingly, "initial investigation" starts when LEAs receive information about crimes. LEAs conduct investigative techniques to verify whether there are enough foundations to file criminal charges. After the crime is charged[37], police investigators conduct the "subsequent investigation" stage. The second stage involves official investigation activities[38] to clarify the case, based on Article 85 of the 2015 Criminal Procedure Code. Lastly, at "the end of investigation," investigators must

[36] Investigative hypotheses mainly consist of assumptions about modus operandi (how), likely offenders (by whom), motives of criminal behaviors (why), crime scenes (where), incident time (when) (Ask 2006, p.3; Nghia and Binh 2014).

[37] In Vietnamese criminal policies, a criminal charge shall only be conducted upon the ascertainment of signs of criminal behaviors. Signs of crime are ascertained by 1. An individual's denunciation; 2. Information provided by agencies, organizations, individuals; 3. Information provided via media 4. A government agencies' requisitions for criminal charges; 5. LEAs' direct exposure of signs of crime; 6. Suspects' confession (Article 142, the 2015 Criminal Procedure Code).

[38] In Vietnamese criminal policies, there is a difference between official investigation and unofficial investigation. Official investigation is regulated by the Criminal Procedure Code. Official investigation aims to find evidence in order to solve criminal cases publicly. Unofficial investigation (or in another name: secret investigation) is regulated by documents that are often enacted by the Ministry of Public Security. Information or fact collected via unofficial investigation cannot be used to prosecute criminals. Unofficial investigation aims to assist LEAs in conducting official investigation activities.

conclude the truth of the case before sending it to the equivalent procuracy. Cybercrime investigation also follows this process.

Article 37 of the 2018 Law on Cybersecurity regulates the role of the Ministry of National Defense in combating cyberattacks. However, the Ministry of National Defense is responsible for military information systems, which differs from the Ministry of Public Security. Additionally, the Ministry of Information and Communications has some agencies that perform government administration in cybersecurity. For example, the VNCERT formally established under the Prime Minister's Decision No. 339/2005/QĐ-TTg of December 20, 2005 has the main function of monitoring, warning, coordinating, and rescuing computer incidents. It plays a role as an operational cybersecurity unit in administrative agencies, and unlike the police, it does not have the function of investigating cybercrime cases. Therefore, it only has the duty of cooperating with the Ministry of Public Security, which implements the official investigation of cybercrime cases.

Joint liability is a core of the mechanism of protecting cybersecurity. Cybersecurity Task Forces are organized under the Ministry of Public Security and the Ministry of National Defense. Besides, based on Article 30 of the 2018 Law on Cybersecurity, other cybersecurity-related forces should be arranged at central and local agencies that directly manage important information systems. Organizations and individuals can be mobilized to participate in protecting cybersecurity. Service providers are responsible for coordinating with and facilitating Cybersecurity Task Forces to conduct the activities of protecting cybersecurity. As such, cybersecurity protection requires all organizations and individuals to cooperate with Cybersecurity Task Forces.

The principle of mobilizing all individuals and organizations inside counter-crime strategies is relevant to the national movement *"All citizens participate in the national security protection"* [Vietnamese: Phong trào Toàn dân bảo vệ an ninh Tổ quốc]. According to Decision 623/QĐ-TTg issued on April 14th 2016 by the Prime Minister, cybercrime suppression is one part of this movement[39]. The movement focuses on educational activities to raise citizens' awareness against crime and other illegal activities (Quangbinh Provincial Police Station 2021). Additionally, it helps citizens and organizations establish and conduct various counter-crime models (such as counter-crime clubs, online counter-crime forums, CCTV systems, counter-

[39] Cybercrime suppression is emphasized by Project 12: Enhance the effectiveness of combating illegal activities and crime on the Internet, National Strategies against Crime in the Period 2016-2025 Directions to 2030 (Decision 623/QĐ-TTg issued on April 14th 2016 by the Prime Minister).

crime Zalo[40] chatting rooms, or self-managed residential areas against crime) (Department of Movement of Protecting National Security 2021). Citizens are instructed to protect their property and report deviant behaviors or suspects to LEAs. This movement is conducted at all Vietnamese administrative levels under the core management of the Ministry of Public Security.

One of the most controversial contents about cybersecurity policy is related to service providers' obligations. Cyberspace rules involve the interests of three major cyberspace actors: the national-state, the citizen, and the international community (Yeli 2017). There is often a controversy between protecting national security and ensuring social order with personal freedoms (Yeli 2017). In this regard, there is a concern about the obligations that require service providers for data localization and establishing offices in Vietnam[41]. On the one hand, it has been criticized that these regulations may increase censorship on personal freedoms; besides, technology companies must spend more fees on operating their business in Vietnam (Cooper and Le 2018; SaveNET 2018). On the other hand, these regulations are evaluated positively as creating a legal foundation for protecting individual and national data, ensuring rights and legitimate interests in cyberspace (Chinh 2019; Dong 2020; Hoa and Long 2020). Moreover, such legislation supports cybercrime prevention and investigation as Vietnamese LEAs can request service providers for cooperation conveniently (Chinh 2019).

Overall, cybersecurity assurance is considered a priority in developing digital society in Vietnam. Cybersecurity must be under the principle of national sovereignty. The Ministry of Public Security is responsible for presiding over coordination with other actors to ensure cybersecurity, combat cybercrime. Among the primary duties of the Ministry of Public Security are the prevention and investigation of cybercrime. Besides, the assurance of cybersecurity requires all organizations and individuals' joint liability. Cybersecurity policy is a foundation for Vietnam to combat cybercrime behaviors in cyberspace.

3.3.2. The development of cybercrime regulations in Vietnam

In coping with the negative reputation of cybercrime, Vietnam has recently paid attention to cybercrime regulations. Both terms of "cybercrime" and "high-tech crime" can be used popularly

[40] Zalo is a messaging application owned by Vietnamese Internet company VNG Corporation.

[41] Domestic and foreign service providers on telecommunications networks, the Internet, and other value-added services in cyberspace in Vietnam which collect, exploit, analyze, process the data of personal information, the data of users' relationships, the data created by users in Vietnam must store such data in Vietnam in a specific period of time stipulated by the Government. Foreign service providers must establish the branches or representative offices in Vietnam (Article 26, the 2018 Law on Cybersecurity).

by Vietnamese LEAs and media, which illustrates two different layers of cybercrime conception in Vietnam. High-tech crime is a “crime implemented with using knowledge, skills, tools about information technology at a high level to illegally affect digital information which is stored, processed or transmitted in computer systems, violating information security, harming the interests of the State, rights and legitimate interests of organizations and individuals” (Nghia and Binh 2014, p.7). This perspective emphasizes the role of technological factors in high-tech crime, which infringes the legitimate rights of citizens and organizations. Only criminal behaviors with technological factors at a high-level degree are regarded as high-tech crimes. The term “cybercrime” is defined at the 2018 Law on Cybersecurity; accordingly, cybercrime involves a broad scope of “behaviors using cyberspace, information technology or electronic means to commit crimes regulated in the Penal Code.” Based on this definition, “cybercrime” is an umbrella term that covers all behaviors of “high-tech crime” and other behaviors that use technology to implement crimes.

If one country has an inadequate cybercrime law, a big obstacle may impact the efficiency of investigating and prosecuting the perpetrator (Singh and Singh 2007). Under the civil law tradition, according to the criminal principle of Vietnam, only behaviors that are regulated by the Penal Code are crimes. Before 2010, some dangerous cyberspace-related behaviors were not regulated under the Penal Code. For example, sharing and purchasing private information of identity cards or bank cards could cause serious consequences, but was not covered by the old Penal Code. However, since 2010, when the 1999 Penal Code (amended in 2009) became valid, many dangerous cyberspace-related behaviors were regulated by the legal systems of Vietnam. The update was an important foundation for LEAs to investigate and prosecute cybercrime and establish international cooperation with foreign counterparts. The period after 2010 has witnessed the dismantlement of many hacking forums such as *vefamily, mattfeuter, vietexpert,* and *hkvfamily.*

The 1999 Penal Code (amended in 2009) was valid from 2010 to 2017. This penal code added some articles on cybercrime, in comparison to the older version[42]. However, this version

[42] The 1999 Penal Code was valid from 2000 to 2009. It had only three articles on cybercrime (Article 224: “Creating and spreading computer virus programs;” Article 225: “Violating regulations about operating, exploiting, and using digital computer networks;” Article 226: “Illegally using information on networks and in computers”). Afterward, the 1999 Penal Code (amended in 2009) was valid from 2010 to 2017. In this version, the number of articles on cybercrime increased from three to five (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 networks;” Article 226a: “Illegally accessing computer networks, telecommunications networks, Internet or digital devices of another person;” Article 226b: “Using computer networks, telecommunications networks, Internet or digital devices to appropriate property”).

still had feasibility issues (HTCP Department 2011, 2012). For example, the act of stealing bank card data was not regulated strictly in this version. Subsequently, 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 that are often recognized as high-tech crime or cybercrime. Besides these, many other criminal behaviors related to cyberspace, such as infringement upon copyright and child pornography, are regulated in other sections of the penal code.

Compared with the Budapest Convention, which has been regarded as the first international convention to combat cybercrime, the newest Penal Code of Vietnam appears adequate (see Appendix 13). The Budapest Convention recommends samples of criminal offenses that should be adopted by each party under domestic law. Vietnam is not a member of the Budapest Convention, and the approach of Vietnam emphasizing national sovereignty in cyberspace is different from the convention. However, the current Vietnamese Penal Code of 2015 covers the core cybercrimes of the Budapest Convention. Among the most common cybercrimes investigated by HTCP, computer fraud is regulated by Article 290: "Using computer networks, telecommunications networks, or digital devices to appropriate property." Another dangerous behavior related to computer fraud is updated by Article 291: "Illegal collecting, storing, exchanging, trading, and publishing information about bank accounts," which is supplemented from the older versions of Penal Code.

Vietnamese criminal policy clearly distinguishes computer fraud from traditional fraud. Computer fraud, regulated by Article 290 of the 2015 Penal Code, involves technological factors. Unlike old-fashioned fraud regulated by Article 174, computer fraud is driven by sophisticated techniques of ICT to trick victims and gain benefits. For example, if normal calls are used to defraud victims, the suspects are charged with traditional fraud under Article 174. Whereas, if VoIP calling systems are applied, phone scammers may be prosecuted for computer fraud under Article 290, which carries a more severe punishment. Technological factors mean cybercrime can fall under stricter penalties compared with respective traditional crime.

Besides, certain cyber offenses 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 behaviors, cyber offenses of the Budapest Convention can be prosecuted based on Articles of traditional crime under Vietnamese legislation. For example, "illegal interception" of the Budapest Convention is covered by two Articles of the 2015

Vietnamese Penal Code. “Illegal interception” regulated by Article 3 of the Budapest Convention rules the violation of the confidentiality of computer data and systems. Meanwhile, in Vietnam, the behaviors of “illegal interception,” include listening, monitoring, surveillance or recording of conversations illegally, through technical means. This could be prosecuted by Article 159 or Article 289 of the 2015 Penal Code. Therefore, if these behaviors are not implemented with complicated techniques, “illegal interception” can be solved 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. Whereas, if “illegal interception” is a subsequent step of illegal access at a high degree of technology, this behavior can match with Article 289 of the 2015 Penal Code, which states: “Illegal infiltration into the computer network, telecommunications network, or electronic device of another person.”

Concerning regulations about procedure, since 2010, investigations and proceedings against cybercrime of 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 ruled out in the 2003 Criminal Procedure Code. Since 2018, the 2015 Criminal Procedure Code has been implemented. Both codes have an important role in regulating matters of international cooperation in criminal proceedings. This includes Articles of 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, extradition, and transfer of convicts.

One primary challenge related to procedure law is that there is no term “digital evidence” in the 2003 Criminal Procedure Code. Therefore, before the 2015 Criminal Procedure Code was valid, 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 (Desnoyers 2013; UNODC 2013, p.165). The Budapest Convention, which opened for signature in 2001, suggests that each state adopts legislative and other measures to preserve, search, and collect digital evidence. After nearly two decades, digital evidence was officially regulated in the 2015 Criminal Procedure Code of Vietnam, which has been valid since 2018.

Accordingly, preservation, search, access, and collection of digital data are under Articles 88, 99, 107, and 196 of the 2015 Criminal Procedure Code.

The above analysis illustrates that the update of regulations on cybercrime in Vietnam has been implemented to cope with the emerging threats of transnational cybercrime. Before 2010, only several dangerous behaviors related to information communications technology were regulated as cybercrime. Since 2010, the number of cybercrime articles have increased. Especially with the application of the 2015 Penal Code and Criminal Procedure Code, the substantive criminal law and procedural law of Vietnam can be regarded as sufficient, which is expected to create a legal foundation for Vietnamese LEAs to fight cybercrime.

3.4. International cooperation policy against cybercrime in Vietnam

"No crime is as borderless as cybercrime," which was highlighted by the European Commission (2012, p.2). INTERPOL (2017) evaluated cybercrime as one of the fastest increasing forms of transnational crime. In a study by UNODC (2013, p.55), over half of responding countries admitted that between 50% and 100% of cybercrime behaviors investigated by police forces consisted of a "transnational element." The physical distance between offenders and victims in the territorial world is deleted in the cyberworld (Scholte 2005). Computer fraudsters no longer travel cross-border with visas, passports, and border gates to obtain victims' money. The unprecedented ICT revolution allows cybercrime to be implemented remotely, via the Internet and wireless communications. Grabosky (2001, p.247) focused on the transnational dimension of cybercrime as follows:

> One of the greatest challenges posed by the advent of digital criminality is the enormously enhanced potential for transnational offending. Many, if not most, cybercrimes can now be committed from the other side of the world as easily as from the building next door. Not only will this tend to make identification of the perpetrator somewhat more difficult, it will greatly impede prosecution of the offender.

While the fight against cybercrime requests international cooperation, the lack of mutual understanding among countries negatively impacts its efficiency (United Nations 2019; UNODC 2013). The Budapest Convention on Cybercrime could be a milestone of harmonizing the international community against cybercrime as it is the first international binding legal instrument (Boni 2001; Peters and Jordan 2020). It was opened for signature by all States two decades ago; as of January 2021, roughly 70 nations have signed and ratified the Convention (The Council of Europe 2021). Among the ASEAN countries, only the Philippines joined the

Budapest Convention (The Council of Europe 2021). Additionally, some countries like China, Russia, and India have refused to adopt the Convention, opposing it as an infringement of national sovereignty (Mehrotra 2019). They proposed a new UN treaty on cybercrime in 2019, despite strong oppositions from major Member States of the Budapest Convention (Stolton 2020). Moreover, the concept of cyber sovereignty, as a significant factor in establishing cyberspace regulations, is still controversial with three main disputes over its contradiction with the spirit of the Internet, with human rights, and with the involvement of multi-stakeholders in governance (Yeli 2017). Furthermore, there has been an increase in the operation of "state and state-sponsored cybercrime" groups such as PLA Unit 61398, Unit 8200, which indeed causes many countries to turn a "blind eye" to such cybercrime (Broadhurst et al. 2014). The international community's different opinions about cyberspace may result in delays or failures of prosecuting transnational cybercriminals.

The Vietnamese Government regards international cooperation as one of the central state policies on cybersecurity, which is regulated by Article 3 of the 2018 Law on Cybersecurity. Then, Article 7 clarifies the principle and contents of international cooperation about cybersecurity. Accordingly, the Ministry of Public Security holds the main role of presiding over coordination in implementing international cooperation on cybersecurity, excluding international cooperation activities under the authority of the Ministry of National Defense. The contents of international cooperation include four main groups: the exchange of information and experiences in combating cybercrime; mutual legal assistance; education and research; finance, equipment, and tools of fighting cybercrime (Nghia and Binh 2014).

The Vietnamese Government has recently implemented many efforts of international cooperation against cybercrime. There are two mechanisms of international cooperation, including bilateral and multilateral levels (Calcara 2019; Guille 2010; United Nations 2004). As an enthusiastic member of the international community against transnational crime, Vietnam had signed 21 bilateral treaties regarding mutual legal assistance and 11 bilateral treaties about extradition as of July 2017 (Vietnam Ministry of Foreign Affairs 2017). Additionally, Vietnam has participated in multilateral instruments on criminal matters (e.g. the UN Convention against Transnational Organized Crime, the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters, the 2003 Cybersecurity Strategy of 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, especially cybercrime.

Under the Government's direction, the Ministry of Public Security has emphasized the significant role of international cooperation in preventing and investigating cybercrime. International cooperation is highlighted in the annual reports of the HTCP Department. Between 2010 and 2018, the HTCP Department has gained many positive results when cooperating with counterparts to investigate cybercrime cases. More particularly, Vietnamese cyber police forces have cooperated with many counterparts such as ASEAN countries, Mainland China, Taiwan, the UK, the US, Korea, Russia, Australia, India, Turkey (HTCP Department 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017). For example, in 2013, the *mattfeuter* carding forums, run by Vietnamese fraudsters, were shut down by the joint Operation 226T between Vietnamese HTCP Department, SOCA of the UK, and FBI of the US (FBI 2013; HTCP Department 2013). In Operation TQ2015, Vietnam established cooperation with Chinese and Taiwanese counterparts to arrest and deport 24 foreign phone scammers back to their countries (HTCP Department 2015). Other contents of international cooperation such as education, finance, equipment, and tools have also been conducted by Vietnamese cyber police forces and counterparts (Luong et al. 2019).

The INTERPOL channel is used popularly by Vietnamese cyber police in sharing investigative information. In Vietnam, to some extent, the evidentiary requirements of investigations and prosecutions may be admitted using the INTERPOL channel (Anh 2011). However, the efficiency of international cooperation via INTERPOL could become doubtful, as in some cases, there are no responses from counterparts when Vietnamese police forces send requests. With the acknowledgement of a call for a 24/7 network that specialized in cybercrime, the 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 five requests from their counterparts via the G8 24/7 network (HTCP Department 2016). In 2017 and 2018, the number of requests processed were seven and four, respectively (Department of Cybersecurity and Counter High-tech Crime 2018; HTCP Department 2017). The participation of the Vietnamese cyber police in the G8 24/7 network shows the strong commitment of Vietnam in international cooperation against transnational cybercrime.

3.5. Conclusion

Vietnam can be evaluated as being infamous for certain cybersecurity criteria, but the Vietnamese Government definitely does not want Vietnam to become a "safe haven" for online criminals. The update and amendment of cyberspace regulations prove a strong commitment of Vietnam to ensure cybersecurity and combat cybercrime. Before 2018, serious loopholes existed in Vietnamese cybercrime legislation. However, since 2018, substantial adjustments have been conducted to fill these gaps. Significantly, the 2018 Law on Cybersecurity, the 2015 Penal Code, amended in 2017, the 2015 Criminal Procedure Code create a legal basis for Vietnamese LEAs to prevent and investigate cybercrime and other risks of cybersecurity. As a specialized agency under the Government's management, the Ministry of Public Security has founded cyber police forces at central and provincial levels. Other stakeholders' joint liability is required to support Vietnamese cyber police to prevent and investigate cybercrime. Moreover, international cooperation is considered one of the central state policies on cybersecurity. Such policies are expected to help Vietnam secure cyberspace and reach specific targets listed at Resolution 52-NQ/TW. The next chapter will examine the causations of cybercrime in Vietnam before the thesis focuses on clarifying TCF.

CHAPTER IV. THE REASONS FOR CYBERCRIME IN VIETNAM: AN ANALYSIS BASED ON ROUTINE ACTIVITY THEORY

4.1. Introduction

This chapter will adopt RAT for analyzing the causation of cybercrime in Vietnam's social situation. RAT is essential for the development of environmental criminology, which is one of the main foundations for criminal network perspective. Using published as well as unpublished reports with specific cybercrime cases, this chapter will adopt some results of research of RAT to explain the occurrence of cybercrime in Vietnam based on the existence of all three necessary factors: *likely offenders, suitable targets,* and *the absence of capable guardians.* This chapter has five sections. Following this introduction, the second section analyzes likely offenders as the first factor of RAT. Subsequently, the third section clarifies suitable targets including with four dimensions — value, inertia, visibility, and accessibility. Lastly, the chapter focuses on the third factor of RAT: the absence of capable guardians with three levels — national, organizational, and individual ones before concluding with important ideas.

4.2. Likely offenders

Everyone has the potential to indulge in illegal behaviors and people make rational choices based on the benefits and risks of bad outcomes (Cohen and Felson 1979). It means that there are potential offenders out there looking for suitable opportunities to commit crimes. If they meet a suitable target without capable guardians, they will indulge in a criminal activity. Likely offenders or potential offenders must bear two dimensions, including the capacity and motivation to commit crimes. Capacity can include ICT knowledge, skills, and tools that help potential offenders commit cybercrime easily (Nghia and Binh 2014). The motivation of cybercrime involves, but is not limited to, the following: financial gains, political movement, recreation, curiosity, and self-defense (Li 2017).

Vietnam is among the top countries in the world for earning a negative reputation. Analyzing the first factor of RAT, it can be interpreted that there may be many likely offenders in Vietnam. Kigerl (2011) emphasizes that Internet penetration is positively associated with spam, and he provides one of the interpretations that Internet users can mean more likely offenders. Additionally, the number of Internet users can be linked with the number of Internet-connected devices that are possibly used as hosts for malware (Kigerl 2011). This argument holds true for Vietnam's social situation. The country has experienced a rapid development of the Internet and is ranked 14th rank in the world and the 3rd in Southeast Asia with the highest number of Internet users (Internet World Stats 2020). The Internet provides cybercriminals not only cyberspace where they commit cybercrime, but also knowledge, skills, and tools, which make them capable of committing the crime.

The availability of online information about hacking skills can equip potential offenders with knowledge and tools of hacking. There were infamous online criminal forums that were cracked down by HTCP in Vietnam in the 2010-2018 period. *Mattfeuter.cc* is one of the most major hacking forums that was investigated by the Vietnam police. It had approximately 16,000 members, operating under the administration of V.T.T from 2009 to 2013 (HTCP Department 2013). Besides, *vefamily.com* operated from 2008 to 2010 with over 2,000 members and about 500,000 reports (HTCP Department 2010). Additionally, v*ietexpert.info* which was managed by H.P.M from 2011 to 2014 had about 3,000 members (HTCP Department 2014). The site had nine sub-forums with over 955,000 reports which helped members discuss hacking skills and exchange tools of cybercrime (HTCP Department 2014). *Hkvfamily.info* which was managed by P.T.T from 2011 to 2014 had about 1,930 members, with over 142,000 pieces of information about instructions for attacking websites and committing computer frauds (HTCP Department 2014). The availability of online hacking forums could provide members with a tremendous source of knowledge and tools to commit cybercrime.

RAT assumes that there is no lack of motivation available for illegal activities. Although the theory does not explain how offenders become motivated, it does not reject the argument that social, economic, and other structural elements could motivate them. Kigerl (2011) proves that the influence of unemployment and Internet usage on spam activities is substantial at the national level. One of his explanations is that countries with many Internet users with IT backgrounds but few IT jobs can be motivated to earn money through illegal activities (Kigerl 2011). However, this conclusion of Kigerl is not appropriate in Vietnam's social context considering that the rate of unemployment in Vietnam is very low, below 2%, in comparison with the average world unemployment figure of over 4.5% in the 2010-2018 period (The World Bank 2019). However, Vietnam is notorious for the source of cyber-attacks and spam Asia (Nexusguard 2017, 2018a, 2018b, 2018d, 2018c; Vergelis et al. 2019). Therefore, unemployment is not significantly related to cybercrime in Vietnam.

RAT is combined with Rational Choice Theory which suggests that people freely choose their behaviors and they are motivated by the benefits and risks of the actions (Miró 2014).

Therefore, motivations can be influenced by the benefits and risks that an offender can gain by committing crimes (Miró 2014). At an annual global cost of US$600 billion, cybercrime ranks 3rd, behind government corruption and narcotics, in the perspective of a global economic scourge (CSIS and McAfee 2018). The European Cybercrime Center (2014) evaluates cybercrime among the list of the most profitable crimes for criminals known in human history. In Vietnam, financial gain is a common motive for cybercriminals. Computer frauds related to bank card information and phone scams are often among the most lucrative black markets in Vietnam. In the *vefamily* case, over US$1.2 million was appropriated; however, a potential gain could be extremely huge because the total number of pieces of stolen bank card information was about 49,000 (HTCP Department 2011). In Operation HQ2015, Korean fraudsters entered Vietnam, then used transnational phone scams to steal over US$3.6 million from Korean victims (HTCP Department 2015).

However, the financial incentive is not the only reason for cybercrime. The surge in the 2016 cyber-attacks coincided with the heightened geopolitical tensions of the South China Sea dispute involving China, Vietnam, and the Philippines. It is assumed that the cyber-attacks on Vietnam's airports were "politically-colored" (Goel 2016). A China-based hacking group named 1937CN, which had previously attacked websites in the Philippines and Vietnam, claimed responsibility for the incident (Davis 2016). It occurred 17 days after the Permanent Court of Arbitration ruled that China has no "historic rights" based on the "nine-dash line" map (PCA 2016). Soon after the airport cyber-attacks, Vietnam's Minister of Information and Communication Truong Minh Tuan urged the domestic technology community to remain calm and avoid any retaliatory attacks (Nguyen 2016). Meanwhile, two teenagers launching cyber-attacks on the websites of five Vietnam airports in 2017 wanted to explore new things and show off to the hacker community (HTCP Department 2017). In such cyber-attacks, disabled computer systems may not bring any financial benefit to a cybercriminal, but they can cost victims a substantial loss of finance, fame, and customers.

Despite huge benefits, cybercriminals face a low risk of detection and punishment by LEAs. The nature of cybercrime, which is committed through cyberspace, reduces the ability of prosecution for cybercriminals (Granja and Rafael 2017). Cybercrime is significantly under-reported across the globe (ISACA 2019a, 2019b). PwC (2018) — a global network of firms — provides that about half of the Vietnamese respondents admitted that their agencies had been targeted by cyber-attacks in 2017 and 2018. The research has raised questions regarding the rate of respondents, with 15% saying "don't know" and 38% saying they were not subject to a cyber-attack. They possibly may not have recognized cyber-attacks of which they may have become victims (PwC 2018). Besides, the low risk of cybercrime also results from the lack of capable guardians which will be analyzed later. Hence, likely offenders can be motivated to reach their decision to commit cybercrime when estimating the benefits and risks of illegal behaviors.

Analyzing the first component of RAT, it suggests that proximity to high concentrations of potential cyber offenders with capacity and motivation increases the likelihood of victimization in Vietnam. Unemployment is not clearly relevant to cybercrime in the country, although Kigerl (2011) proved a significant relationship. Internet penetration, the availability of hacking knowledge and tools, and the benefits and risks can be considered to result in an increase in potential offenders to commit cybercrime in Vietnam. The expansion of ICT leads to an increasing number of Internet users and online benefits. Consequently, the number of likely offenders can increase in the future. Suitable countermeasures should be conducted to reduce the threat of cybercrime.

4.3. Suitable targets

Incitement of likely offenders cannot supply a sufficient condition for turning criminal intentions into illegal activities (Cohen and Felson 1979). The key condition is the social situation where unprotected targets exist and potential offenders themselves reach decisions about whether or not they will translate their criminal inclinations into action. RAT clarifies suitable targets as a person, an object or a place with four dimensions — value, inertia, visibility, and accessibility (Miró 2014).

The valuation of likely targets in cybercrime can include both the financial value of rewards and the potential influence of victims. RAT emphasizes that high value is a desirable target characteristic in property-related crimes (Cohen and Felson 1979). In bank card data fraud, Vietnamese hackers possibly did not exactly identify the valuation of bank card accounts; however, they were surely aware that foreign credit card data could bring them a huge amount of money. Each *alive* foreign card data could cost US$0.3-3 and they could be used to get the money of card owners (HTCP Department 2010). Another facet of valuation in cybercrime could be the potential influence of victims. For example, in the cyber-attacks on Vietnam's airports in 2016 and 2017, offenders could understand that cyber-attacks would result in chaos given the important positions of the targets. Therefore, it was ideal for

Vietnam's airports to be considered suitable targets by hackers with political motivations and those who wanted to demonstrate their talents.

The second dimension of suitable targets is inertia which seems ambiguous when applying to cybercrime (Yar 2005). Maybe Yar distinguished between targets and victims in this dimension. For example, in computer frauds, targets are the property which are illustrated through digital information such as credit card and bank account data. Victims are individuals, or organizations facing the consequences of crime such as credit card owners and banks. If this opinion is acknowledged, it is true that the targets of cybercrime are often "weightless." However, the term "targets" should be understood in a broader meaning in which the targets should merge with victims, and it includes property, individuals, organizations, and even places. The broad scope can make the inertia of targets unambiguous in cyberspace.

From 2014 to 2018, there were many Facebook love scam cases occurring in Vietnam (Department of Cybersecurity and Counter High-tech Crime 2018; HTCP Department 2014, 2015, 2016, 2017). Scammers pretended to fall in love with victims through Facebook, then they would claim to have sent luxury items or large sums of money to the victims. The scammers' accomplices pretending as courier staff members or government officials would contact the prey and claim that the goods had been detained for inspection by authorities. They would persuade the victims to transfer money to receive the goods. A common characteristic is that the victims are vulnerable females, and the lack of their confidence about physical appearance and private life reduces their capacity of resistance against scammers.

The expansion of the Internet makes suitable targets more visible to potential offenders (Grabosky 2001; Navarro and Jasinski 2012). Kigerl (2011) proves that the proportion of Internet users has a positive relationship with cybercrime activities. Internet users themselves can also become prospective victims of cybercrime because of their online activities (Kigerl 2011; Yar 2005). For example, with just a few "clicks" on the Internet, users can be easily redirected to websites that are managed by hackers, placing potential victims in close proximity with the hackers (Yar 2005). Vietnam ranks 14th worldwide based on the number of Internet users, which stands at about 68.5 million users (Internet World Stats 2020). Vietnam demonstrated impressive progress in the number of social media users, with an annual 20% increase, ranking 6th worldwide (We Are Social and Hootsuite 2018). The popularity of the Internet is an important factor for increasing the visibility of suitable targets in Vietnam.

Routine activities such as online shopping, visiting forums and social network sites lead to more incidents of online threat victimization (Choi 2008; Kigerl 2011; Pratt et al. 2010; van Wilsem 2013). Pratt et al (2010) prove the association between the hours spent online and the odds of computer fraud targeting. The time spent per day on the Internet and social media sites by Vietnamese users is nearly 7 hours and 2 hours 37 minutes, respectively, ranking 15th globally (We Are Social and Hootsuite, 2018). It suggests that the long duration of Internet use by Vietnamese citizens increases the chances of them being targeted while they are online. However, almost all victims of bank card frauds which Vietnamese police investigated are not Vietnamese, but from foreign countries such as the US, the UK, Australia, Canada, and China (HTCP Department 2010, 2013, 2014). This can be explained by the payment habits of Vietnamese citizens. Although the Government of Vietnam has established many policies to turn Vietnam into a cashless society, credit/debit card usage remains very low and cash continues to be a favorite mode of payment (VECITA 2017). About 90% of individuals chose cash-on-delivery, only about 20% of e-commerce customers used credit/debit cards in 2015 and 2016 (VECITA 2017). On the contrary, the US, the UK, Australia, Canada, and China are in the list of the most cashless countries in the world (Forexbonuses n.d.). Consequently, without capable guardians, online customers of these developed countries face a risk of victimization of global credit card frauds.

Corresponding to the last dimension of suitable targets (accessibility), Yar (2005) argues that it appears inappropriate to apply this aspect to virtual space. Yar (2005) stated that that hackers can jump from any one point to the other within the cyberspace and escape easily by ending a connection. However, popular hacking techniques must be based on the errors and weaknesses of both information systems and humans (Ahmed et al. 2012; Chowdappa et al. 2014). Therefore, the design of information systems surely influences the risk of cyber-attacks. The errors and weaknesses can result in more chances of accessibility for likely offenders.

The negative routine of users such as using pirated software and media will create more chances of accessibility, increasing the odds of becoming a victim of malware infection (Bossler and Holt 2009). Unlicensed software contains errors which hackers can exploit to commit cyber-attacks. Vietnam is located in the Asia-Pacific area, which has the highest average rate of unlicensed software use. Although there was a decline in the rate of unlicensed PC software installations in Vietnam, figures show that it was still very high at 74% in 2017, compared with the average figure of the Asia-Pacific area (57%) (BSA 2018). Using unlicensed software has a strong correlation with malware infections (BSA 2018). Vietnam is listed among the top countries in the world with the highest malware encounter and infection rates (Kaspersky 2017, 2018; Microsoft 2015, 2016).

To summarize the second factor of RAT, there are attractive targets and victims with four core dimensions in Vietnam's social situation, although each dimension may have a dissimilar impact on the occurrence of cybercrime. In the future, the number of suitable cybercrime targets will be expected to expand as Vietnam and other countries have applied additional ICT to many aspects of the society. Expanding information systems without capable guardians will result in more suitable targets for likely offenders to execute cyber-attacks.

4.4. Absence of capable guardians

The presence of capable guardians is believed to prevent likely offenders from deciding to commit crimes (Cohen and Felson 1979). Guardianship can be the physical presence of a person or in the form of technical tools such as anti-virus software, firewalls or in the form of macro-level policies such as legal frameworks. The lack of guardianship that can be divided into three levels, governmental, organizational, and individual, will bring in more choices for victimization (Bossler and Holt 2009; Williams 2016).

Although the development of Vietnam's 2020 Global Cybersecurity Index (GCI) illustrates an increasing commitment to cybersecurity (ITU 2021), vulnerability to cyber-attacks was still grave in the absence of national guardians. In 2017, Vietnam (global rank:101) was listed in the "initiating stage" group of countries for introducing moves to preserve cybersecurity (ITU 2018). According to an evaluation of the 2017 GCI, Vietnam had only four indicators labelled "green" (good), two indicators classified as "yellow" (medium), and the 19 remaining indicators tagged "red" (bad) (ITU 2018). The progress of Vietnam in 2018 when some cybercrime-related law started to be valid helped the country to be categorized among the "medium countries" group, ranking 50th worldwide (ITU 2019). The positive progress coincided with a reduction in the number of cyber-attacks recorded by VNCERT in 2018 and 2019 (APCERT 2019, 2020). After two years, Vietnam positively jumped 25 places, ranking 25th globally in the 2020 GCI (ITU 2021). The improvement means that at the national level, the government has raised awareness of implementing legal, technical, and organizational measures; capacity building; and cooperation against cyber risks. In summary, the GCI of Vietnam can prove that in general, before 2018, the country-level guardianship of Vietnam had not been strong enough to defend Vietnam's information systems against cyber risks.

Cohen and Felson (1979, p.605) suggest that the lack of proper mechanisms for social control and punishment would lead to "vast increases in the certainty, celerity, and value of rewards" through illegal behaviors, subsequently resulting in more crimes. The Vietnamese legal framework has some loopholes related to cybercrime. According to the country's criminal law, an act which is regarded as a crime must be prescribed by the Penal Code. In the 2010-2017 period, Vietnam used the 1999 Penal Code, amended in 2009, following which the number of articles on cybercrime rose from three to five. The amendment updated certain dangerous behaviors as cybercrime, but there were feasibility issues (HTCP Department 2011, 2012). For example, before 2018, collecting and storing illegal bank card data could be very difficult to be processed under the Penal Code. Despite the potential dangers, these behaviors are not included in the 1999 Penal Code, amended in 2009. If law enforcement forces want to curb these illegal activities, they must prove that the rationale behind these behaviors is to gain money. In certain cases, it is challenging to investigate the motivation of collecting and storing illegal band card data because of the lack of evidence (HTCP Department 2014).

Additionally, the 2003 Criminal Procedure Code states that law enforcement forces must clarify the identity of victims and interview them in fraud cases. However, Vietnamese investigators have met many challenges to clarify and interview foreign victims in credit card fraud cases (HTCP Department 2014). Furthermore, the acceptance of digital evidence caused a debate because there is no such term as "digital evidence" in the 2003 Criminal Procedure Code (HTCP Department 2011, 2012). Such loopholes had led to many challenges, even failures during investigations and prosecution of cybercriminals in Vietnam before 2018.

Subsequently, the 2015 Penal Code (amended in 2017), the 2015 Criminal Procedure Code, and the 2018 Law on Cybersecurity closed the loopholes, which may create a positive country-level guardianship against cybercrime in Vietnam. They represent three types of cybercrime law: substantive criminal, procedural, and preventive law. Being substantive criminal law, the 2015 Penal Code (amended in 2017) updates and covers the core cybercrimes of the Budapest Convention. Moreover, the 2015 Criminal Procedure Code regulates digital evidence, investigations, and proceedings against cybercrime. While substantive criminal and procedural laws aim to bring suspects conducting criminal behaviors to justice, preventive law focuses on preventing cybercrime or reducing risks/damages of cybercrime. Accordingly, the 2018 Law on Cybersecurity is expected to become an effective "guardian" to prevent or mitigate the consequences of cybercrime and other cyberspace-related violations. As analyzed in Chapter III, this law reflects Vietnamese cybersecurity policy with the central players of cyber police and the joint liability of other stakeholders.

In the fight against cybercrime, with the leadership role, the Vietnamese police have faced challenges including technical snags, lack of human resources, financial problems, and cooperation issues (HTCP Department 2017). These difficulties have negatively impacted the fight against cybercrime in the country. As discussed earlier, the number of processed cases accounts for a small percentage of overall cyber-attacks. Moreover, in some cases, despite Vietnamese authorities' success in apprehending cybercriminals, the punishment includes only fines and/or incarceration within a short time. This penalty may not serve as a deterrent to restrain cybercriminals. The lack of adequate mechanisms for punishment would result in more crimes (Cohen and Felson 1979). In the *mattfeuter* case, regarded as one of the most notorious cybercrime cases in Vietnam, the maximum sentence which was applied to the ringleader was only a four-year imprisonment for sharing and using stolen bank card data (Chau 2016; HTCP Department 2013), while many offenders in the ring, with about 16,000 worldwide members, have not been identified and punished. In cyber-attacks on Vietnam's airports in 2016 and 2017, despite extremely serious consequences, no one has been held or jailed (HTCP Department 2016, 2017). Two 15-year-old hackers launching cyber-attacks on Vietnam's airports in 2017 were only charged with administrative violations (HTCP Department 2017).

However, the significant role of the HTCP Forces to combat cybercrime is ostensible. Since the foundation, the HTCP Department has cracked down many hacking forums of criminal syndicates such as the groups of *vefamily, mattfeuter, vietexpert,* and *hkvfamily*. In 2009, using stolen credit card data to purchase flight tickets on the website of Vietnam Airlines was a very serious issue, constituting about 6% of overall online purchases (HTCP Department 2010). In 2010, Bank Card Associations such as VISA and MasterCard warned that if the rate could not be restrained to below 5%, VISA and MasterCard would decline transactions using their bank cards on the website of Vietnam Airlines (HTCP Department 2010). The Vietnamese police established and employed two investigative operations to arrest nine culprits (HTCP Department 2010). Subsequently, the rate of frauds reduced visibly, and VISA and MasterCard continued to accept transactions (HTCP Department 2010). Therefore, the strong suppression of HTCP has a clear relationship with the situation of cybercrime in Vietnam.

The organizational-level guardianship must be in line with the governmental-level one. Vietnam's Information Security Index of each year between 2013 and 2018 was only at an average level (VNISA 2014, 2015, 2016a, 2017, 2018, 2019). It means that the organizations of Vietnam do not care much about measures to ensure their information systems. In 2018, there was no administrative agency at rank "A" (good), 70% of administrative agencies were labelled "C" (average), only 9.2% of organizations had cybersecurity surveillance systems, and only 35.7% had a criteria process of Incident Response (VNISA 2019). As a result, organizations in Vietnam are still weak at handling cybersecurity, making it is easy for them to become victims of cybercrime.

One typical example is related to the information systems of Vietnam airports which were the targets of cyber-attacks in 2016 and 2017. According to Article 10, 2018 Cybersecurity Law and Decree No. 85/2016/NĐ-CP, the information systems of Vietnam airports are listed among the most important national information systems with the highest priority of securing systems. However, the IT-systems of Vietnam airports failed to cope with two serious cyber-attacks in 2016 and 2017. In the 2016 case, the systems could have been illegally accessed since 2014, but the hacking was not discovered until 2016 (VNISA 2016b). The hackers used spyware which could not be detected by the anti-virus software, then infiltrated in both "deep" dimension (important servers) and "broad" dimension (many computers in many agencies) (VNISA 2016b). This spyware also appeared in the information systems of many other Vietnam agencies (BKAV 2016). One year later, the information systems of Vietnam airports were attacked again. Two teenagers defaced the websites by exploiting the loopholes in the IT-systems which existed in about 40% of Vietnam websites (BKAV 2017). The two cyber-attacks on the IT-systems of Vietnam airports proved that the level of protection is not strong enough to combat the same.

In addition to social guardians at the country and organization levels, cyberspace can be secured by private protection mechanisms. Cohen and Felson (1979, p.591) emphasize the importance of "attached or locked features of property inhibiting its illegal removal." In cyberspace, "attached or locked features" can be understood as passwords and other authentication measures (Yar 2005). In 2018, over 160 million accounts of VNG Cooperation, one of the biggest Vietnamese technology companies, were leaked (Hung 2018). By analyzing the database of these leaked accounts, it can be concluded that authentication measures of VNG Cooperation are not complex and that Vietnamese users are habituated to using simple passwords such as 123456 (rank: 1st, 58%), 123456789 (rank: 2nd, 15%), and 123123 (rank: 3rd, 8%) (Hung 2018). Such behaviors would increase the likelihood of becoming victims of cybercrime in Vietnam. Additionally, personal-level guardianships can include firewalls, intrusion detection systems, and anti-virus software (Choi 2008; Yar 2005). Choi (2008) concludes that individuals with a technically-capable guardian (such as anti-virus software) have a lower possibility of virus victimization. However, in Vietnam, Internet users do not often pay much attention to using licensed software, especially anti-virus software (ICTNews 2018). These negative behaviors place Vietnamese Internet users at a high risk of victimization of cybercrime as the nation is notorious for online and local infection.

The absence of capable guardianship, whether it is at the governmental, organizational or individual level, can lead to increasing the capability of turning likely targets into victims in cyberspace. The guardianship is the most critical for deterring likely offenders from deciding to commit cyber-attacks on victims. While it is difficult to change factors reducing the digital convergence of likely offenders and suitable targets, the combination of both macro- and micro-guardianship will result in more success of governance of cybersecurity.

4.5. Conclusion

The reasons for cybercrime in Vietnam have been explained with three main factors of RAT. Each dimension inside each factor has dissimilar importance to the occurrence of different types of cybercrime, but when all three factors — likely offenders, suitable targets, and the absence of capable guardians — come together in time and space, cybercrime is bound to occur. The expansion of ICT results in more convergence of likely offenders and suitable targets in Vietnam. Therefore, it is imperative to use capable guardians as a “shield” against cybercrime. Understanding the picture of cybercrime in Vietnam provides a context for analyzing the modus operandi and structure of TCF networks. Two next chapters focus on exploring and discussing TCF networks' nature before the thesis suggests policy and practical recommendations for counter-crime measures.

CHAPTER V: THE MODUS OPERANDI OF TRANSNATIONAL COMPUTER FRAUD: A CRIME SCRIPT ANALYSIS IN VIETNAM

5.1. Introduction

The chapter provides the findings and discussion of Question 1: "How is TCF implemented in the Vietnamese context." In particular, it aims to explore how computer fraudsters are involved in criminal activities, and what tools and techniques are used to defraud transnational victims in Vietnam. It consists of five main sections. After the introduction, the second section presents the descriptive statistics of 20 case studies. It provides the main information about the background of selected cases, the characteristics of suspects, victims as well as the consequences of TCF. The third section illustrates the key findings of TCF modus operandi in Vietnam with two types: bank card data fraud and phone scams. Subsequently, the final two sections discuss the remarkable characteristics of TCF in Vietnam, then concluding this chapter with restating important results.

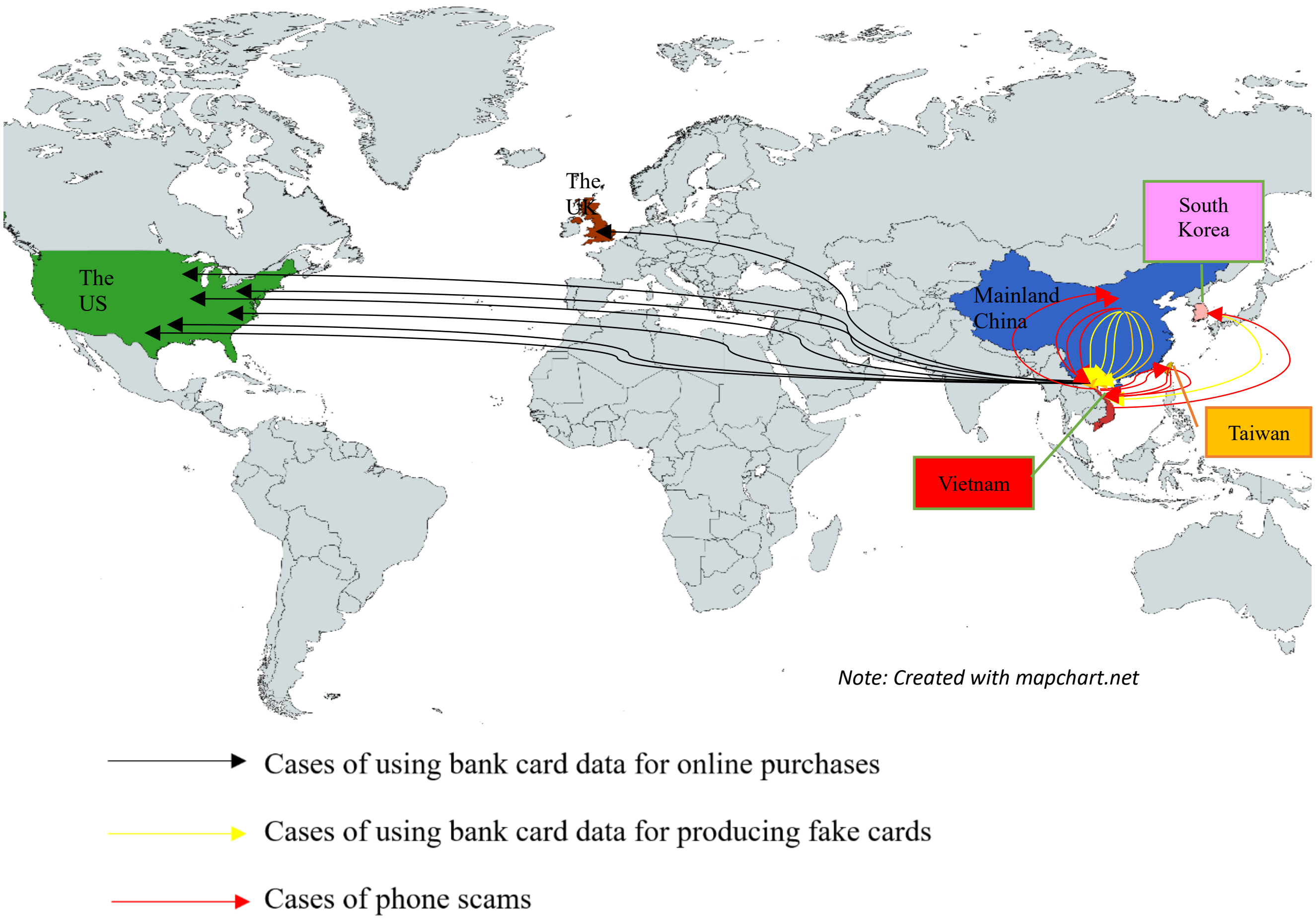
5.2. Descriptive case studies

5.2.1. Background of selected cases

As mentioned in Chapter I, this study collected data via 20 TCF cases and interviews with 14 investigators who directly involved in these cases. These twenty cases were investigated by HTCP between 2010 and 2018, consisting of nine cases disrupted by the department headquarters and 11 by provincial polices. At present, Vietnamese cyber police forces are organized at two levels inside the Ministry of Public Security: the department headquarters and provincial police agencies. According to Vietnamese regulations, the department headquarters are responsible for investigating highly-complicated cases that cause extremely serious consequences or are relevant to many provinces and countries. They are also in charge of solving cases that local police forces cannot investigate.

All these cases are transnational, based on the definition of the UN Convention against Transnational Organized Crime (2000). As presented in Figure 5.1, there is a clear difference in the main directions of transnationality between the three types of cases. All cases of using bank card data fraud for online purchases originated from Vietnam and mainly attacked foreign victims of the US and the UK. Whereas all cases of using bank card data to produce fake cards

Figure 5.1. The main directions of transnationality of 20 cases


The UK
South Korea
The US
Mainland China
Taiwan
Vietnam
Cases of using bank card data for online purchases
Cases of using bank card data for producing fake cards
Cases of phone scams

Note: Created with mapchart.net

started from Mainland China, Taiwan, and Korea; foreign culprits entered Vietnam to commit crimes. Victims of these cases were both Vietnamese and foreigners. Cases of phone scams could originate from Vietnam to attack Chinese, Taiwanese, and Korean victims, or they started from Mainland China and Taiwan to defraud Vietnamese victims.

Vietnamese LEAs often cooperated with counterparts to solve these transnational cases. For example, the successful disruption of the *mattfeuter* gang (in C03) resulted from the unprecedented cooperation between the Vietnamese Ministry of Public Security, SOCA of the UK, FBI of the US. This cooperation lasted for a long time, from 2009 to 2013. Besides, foreign groups of phone scams were arrested in Vietnam due to collaboration between Vietnam with China and Taiwan (C02 and C18) or Korea (C15). In these phone scams, after arresting foreign scammers, Vietnamese LEAs cooperated with the counterparts to deport them back to their countries. The cases were transferred to the counterparts that were responsible for the subsequent investigation.

5.2.2. Characteristics of suspects

Characteristics of fraudsters in the 20 cases are different in size, nationality, gender and age, occupation, and criminal records. Based on demographic data analysis, suspects' following characteristics can be clarified.

Size: All cases were committed by at least four suspects. If the size of networks only limits to identified-culprits[43], ten cases comprised six or more criminals, accounting for 50% of the sample. Four networks consisted of more than ten members, making up 20% of the sample. However, if all unidentified suspects and related individuals[44] are added, the number of persons involved in TCF groups is much higher.

In all six groups using bank card information for online purchases, LEAs could not clarify many foreign culprits' identities because of international cooperation difficulties. In all six networks printing fake bank cards, investigators successfully clarified Vietnamese followers and foreign culprits who entered Vietnam. Whereas overseas facilitators providing card samples, card printers, software, and stolen bank card data could not be tracked down. Additionally, in all eight networks of phone scams, LEAs only managed to crack down one of two groups: callers or money mules. In three networks (C02, C15, and C18), Vietnamese police arrested foreign fraudsters who entered Vietnam to implement VoIP calls to Chinese, Taiwanese, and Korean victims. In contrast, the identity of money mules was not detected by Vietnamese LEAs. In the remaining networks of phone scams, some groups of Vietnamese money mules were brought to justice, but core members and caller groups were under the darkness.

Furthermore, if cybercrime networks expand to include online hacking forums, groups' size could reach thousands of members in one network. *Mattfeuter.cc* is one of the most major hacking forums investigated by Vietnam police. It had approximately 16,000 members. The forum *vefamily.com* attracted over 2,000 members. After *vefamily.com* had been closed down by LEAs, C05-No.01 – a technical administrator of *vefamily.com* used its source code to design another hacking forum *vietexpert.info*. The new version had about 3,000 members.

The data analysis of 20 cases with 181 identified-culprits is presented in Table 5.1.

[43] Identified-culprits are criminals who LEAs made their identity clear. Whereas unidentified suspects include individuals who LEAs could not investigate their identity clearly. Unidentified suspects could be shown via the information of phone numbers, mail addresses, nick-names, or names.

[44] Related individuals are involved in criminal activities; however, LEAs cannot prove their criminal behaviors beyond a doubt. In some situations, their behaviors are dangerous, but they do not recognize the criminal purpose.

Table 5.1. Characteristics of identified-culprits

Sum	Nationality		Gender		Age			Occupation					Criminal Record	
	Vietnamese	Foreigner	Male	Female	Under 25	25 - 35	Over 35	Unstable	Business	Student	Technician	Others	Yes	No
181	88	93	156	25	73	81	27	134	14	10	7	16	13	168

Nationality, gender, and age: With respect to culprits' nationality, there is no significant difference between the number of Vietnamese culprits (88 offenders) and foreign ones (93 offenders including 83 Chinese and Taiwanese ones, 10 Korean ones). However, the category of offenders by gender indicates an imbalance between males and females in committing TCF. Offenders were mostly males, with 156 ones (86%) compared to only 25 females (14%). Regarding age, offenders are separated into three groups including "under 25," "from 25 to 35," and "over 35." The number of "under 25" culprits (73 offenders with 40%) is nearly equivalent to the number of "from 25 to 35" ones (81 offenders with 45%). Whereas only a small percentage of offenders, 15 % or 27 persons, were over 35 years old.

Occupation: Concerning occupations, offenders have been divided into five groups, namely "unstable," "business," "student," "technician," and "others." There were 134 offenders (74%) in the "unstable" group which consists of unemployed individuals and people having a temporary job that is likely to end at any time. Next, only 14 culprits belonged to the group of "business," accounting for 8% of the total number. Business is not an official job but is a broad term covering small scale entrepreneurs (such as a mini-shop owner C02-No.25) to large scale businesspersons (such as company directors C03-No.04, C04-No.01, or a hotel manager C15-No.01). Only ten students (6%) and seven technicians (4%) participated in the TCF networks. In the "others" group, 16 remaining culprits were a bank officer, a logistics officer, a teacher, a translator, a hotel receptionist, a farmer, a fisher, or a company worker.

Criminal record: Additionally, almost all offenders, 168 ones (93%), committed the crime for the first time. A small number of TCF offenders (13 fraudsters, accounting for 7%) were recidivists. In cases using bank card data for online purchases, only one of 56 identified-culprits (C05-No.08) was a recidivist. In comparison, nine of 100 identified-culprits of phone scams had at least one previous conviction. Among them, two Korean fraudsters (C15-No.1 and C15-No.02) received "Red Notices" issued by INTERPOL, which means that they were international wanted fugitives. They fled to Vietnam and established a transnational criminal network, including seven Korean criminals. Additionally, three other Korean suspects in a card cloning network (C13-No.01, C13-No.03, and C13-No.04) had been charged by Korean courts before entering Vietnam for committing crimes.

5.2.3. Characteristics of victims

In the selected cases, victims can be divided into two categories: organizations and individuals. Organizations could be foreign companies managing e-commerce websites which hackers attacked to steal their customers' bank card data. They often operated small-scale businesses via e-commerce websites. Their websites existed serious security errors that hackers exploited to access their database. Besides, banks could also be regarded as victims of TCF cases. Their ATMs could become targets where fraudsters conducted skimming techniques to collect bank card data. Vietnamese banks' POS terminals were used by fraudsters to make fake transactions with counterfeit cards. Moreover, fraudsters obtained illegal money from bank card owners or banks' customers. This situation possibly led to damage to their reputation. Therefore, banks may be considered organizational victims of TCF.

In the sample cases, individuals were the main victims of TCF networks as fraudsters aimed to obtain money from individuals' bank accounts. All cases using bank card data for online purchases possessed foreign victims. In these cases, bank card information proves that these cards belonged to foreign users, mainly in the US and the UK. Only one of six card-cloning cases (C20) had Vietnamese victims, whereas five remaining cases appropriated money of foreign bank card owners. In three of eight phone scam cases (C02, C15, and C18), all victims were foreigners locating in Mainland China, Taiwan, and Korea. In these cases, all culprits also were foreigners. After arresting fraudulent foreign callers, Vietnamese LEAs cooperated with counterparts to deport criminals and transfer the cases to counterparts. Five remaining phone scams attacked Vietnamese victims.

5.2.4. Consequences

There are two clear categories of consequences of the selected TCF cases: reputational damage and financial loss. Although investigation files have not provided detailed information about reputational damage to companies and banks, TCF could seriously affect their business. In bank card fraud cases, cyberattacks or skimming could be conducted to steal customers’ bank card data. These activities could damage banks and companies' reputation and erode their customers' trust. In turn, this situation could cause companies and banks to lose customers and finance.

Moreover, for individual victims, financial loss was the main consequence in the 20 cases. On average, the amount of stolen money that was clarified was about US$570,000 per case. The cases causing the most serious financial loss were phone scams conducted by foreign callers. In C15, Korean victims were defrauded about US$4 million by Korean fraudsters operating from Vietnam. In C18, Chinese and Taiwanese fraudsters obtained about US$2.7 million from Chinese victims. Whereas the highest financial loss of bank card data fraud was about US$1.5 million (C04), and next was about US$1.2 million (C03). However, a potential financial loss of bank card data fraud could be much huger. Underground forums had many members who could not be identified. Besides, the total number of pieces of stolen bank card data was extremely large. In C03, for example, about 49,000 pieces of bank card data were obtained by Vietnamese fraudsters.

5.3. Findings

The crime scripts of the two forms of TCF in Vietnam can be presented as shown in Table 5.2.

Table 5.2. Modus operandi of TCF

Stage	Scripted actions: Bank card data fraud	Scripted actions: Phone scams
Preparation	Source bank card data - Skimming - Hacking - Purchasing or obtaining data online Recruit money mules and other members - Online recruitment - Offline recruitment Prepare tools - Prepare tools for masking real identity	Recruit members - Online recruitment - Offline recruitment Prepare tools and locations - Prepare tools for setting up VoIP systems - Prepare locations with high security and little attention

	- Prepare tools for obtaining illegal money	
Activity	Online purchases - Buy and ship carded products from the US to Vietnam - Buy software and domains Counterfeit cards - Withdraw cash directly at ATMs - Implement transactions via POS terminals	Make fraudulent calls to victims - Pretend to be LEAs to threaten victims - Implement e-commerce fraud Receive illegal money - Transfer via many intermediate bank accounts
Post-activity	Flee	Flee

5.3.1. Bank card data fraud

Source bank card data

Sourcing bank card information is usually only the first step in a series of illegal activities in the underground economy (Hao et al. 2015). Among the list of identity theft methods revealed by Peretti (2008), fraudsters carried out skimming and hacking techniques in Vietnam. Phishing, which was evaluated as the main method of obtaining bank card data by European and American fraudsters (Leukfeldt et al. 2017; Peretti 2008), did not exist among the Vietnamese sample cases in the present study. In Vietnam, culprits obtained bank card data directly from ATMs by using skimming devices or from websites via hacking techniques. However, stealing bank card data was not frequent among fraudsters in Vietnam, and most sourced this information by purchasing it online from hackers.

The skimming technique, in which fraudsters clone bank cards to withdraw cash at ATMs, only appeared in case C20. All four fraudsters in this case were Chinese. Investigation documents showed that they had brought skimming devices from outside Vietnam. After determining the location of a suitable ATM that attracted many customers, they set up these devices in the afternoon or evening. To prevent detection, they retrieved the devices after several hours before using special software to decrypt and transfer the data to cloned cards.

Apart from skimming, hackers attacked foreign e-commerce websites to collect bank card data that included card numbers, expiration dates, security codes, and cardholders' full names, addresses, and telephone numbers. This technique requires high-tech skills, so only five Vietnamese professional fraudsters in the networks in cases C03 and C05 succeeded in implementing it. Automated tools were used to test the SQL injection errors of e-commerce websites; thereafter, Vietnamese hackers exploited these errors to gain unauthorized access to websites and collect customers' bank card data. In case C03, two offenders (C03-No.01 and C03-No.13) obtained approximately 2,000 items of credit card data with the SQL injection technique. More seriously, another offender (C03-No.08) stole 100 megabytes of data which stored about 4 million pieces of card data.

While only a small number of fraudsters executed hacking techniques, many cybercriminals exchanged, purchased, and even freely received bank card data on underground websites or from other criminals via Internet communication methods. Many hacking forums that were infiltrated and closed by Vietnam's HTCP Forces from 2010–2018, such as *vefamily.com* (case C03), *mattfeuter.cc* (case C04), and *vietexpert.info* (case C05), were all managed by Vietnamese hackers. As a trustworthy member of these websites, one had the privilege to access free sources of card data, but the quality of such data was often low. There was a high probability that multiple fraudsters would use the same piece of data, therefore causing the victim to recognize the multiple suspicious transactions. If fraudsters wanted higher-quality card data, they bought them directly from trustworthy suppliers on hacking forums. The price of bank card data was often in the range of 0.3–3 USD/piece. The most popular payment method was via digital money services (e.g., LR, Western Union, WMZ, PayPal, or bank transfer services).

In all five groups that made fake transactions via POS terminals, the core fraudsters were provided with bank card data by others. However, the payment mechanism for card data providers differed from that of online purchase groups. In cases of POS transactions, culprits contacted each other mainly via QQ messaging software to obtain credit card data. Depending on the deal, card data providers often received 40% of the illegally obtained money after the fraudulent activity was complete. Within these groups, only a small amount of card data was exchanged among members in comparison with the online purchase groups.

Recruit money mules and other members

There are several positions inside cybercrime networks, including core members, professional enablers, recruited enablers, and money mules (Leukfeldt, Kleemans, and Stol 2017). Core members initiate, direct, and/or manage other members to implement cybercrime. Meanwhile, enablers are responsible for providing core members with services such as hacking tools, and money mules are recruited to receive illegal money or products to potentially interrupt LEAs' financial investigations into core members. Money mules, thus, play a very important role in fraud networks, and, in the sample cases, core offenders employed many methods to recruit the mules and other members.

In the fraudulent online purchase networks, money mules are responsible for receiving products that had been ordered with stolen credit cards. Afterward, they reship the packages to the core members; thus, they are also known as "reshipping mules," "shipping mules," "parcel mules," or "drops" (Hao et al. 2015; Hutchings 2014; Peretti 2008). In Leukfeldt, Kleemans, et al.'s (2017) model, these roles are all considered "money mules." In the present study, the term "money mules" was used to refer to any individual who receives and then transfers illegal money or products.

In bank card data fraud networks, money mules are often indispensable actors (Hao et al. 2015; Peretti 2008; Soudijn and Zegers 2012). Like any organized traditional criminal group, however, cybercriminal networks are faced with a shortage of active money mules, and many methods have been developed to recruit them (Soudijn and Zegers 2012; Tropina 2012). In fraudulent online purchase networks, the use of money mules allowed core members to reship overseas merchandise to Vietnam, as many foreign e-commerce websites did not include services that would sell valuable products directly to Vietnam. The Internet was the first choice to recruit money mules, and virtual forums became convergence settings where supply and demand could meet (Leukfeldt 2014; Soudijn and Zegers 2012). Vietnamese core fraudsters also recruited foreign money mules through online advertisements. Money mules were convinced that they could earn money easily by receiving and reshipping products. As a result, many were willing to participate in fraudulent networks without knowing the real purpose of their activities.

In contrast, offline recruitment was used mainly in the networks that produced counterfeit cards. Recruitment activities were based on real social relationships between core members, recruited enablers, and money mules. In network C13, for example, the core actors (C13-No.01, C13-No.02, C13-No.03, and C13-No.04) were close friends. One core actor (C13-No.02) asked a recruited enabler (C13-No.05) to find POS terminals, and the enabler (C13-No.05) then borrowed POS terminals from his friends. The same method was applied by other networks that used POS terminals (C10 and C19). Nevertheless, LEAs usually failed to find enough evidence to prove money mules were aware of their criminal behaviors.

Prepare tools

Apart from sourcing bank card data, computer fraudsters had to prepare the necessary tools to implement fraudulent activities. Criminals have always tried to find suitable ways to prevent detection by LEAs while gaining illegal benefits. When operating online, the computer fraudsters masked their real IP addresses, which could have revealed their physical location. Moreover, changing IP addresses also aims to prevent detection by e-commerce websites that do not allow transactions from Vietnam. Core fraudsters exploited fake IP software or virtual personal networks (VPNs) to change these IP addresses, and tools for hiding real IP addresses were provided mutually by criminals or bought from developers. Some professional core fraudsters also used stolen email accounts for fraudulent transactions, and Vietnamese hacking forums had sections where members could discuss and exchange these fake IP protocols and stolen email accounts.

In cases of counterfeit cards, fraudsters had to find card samples, card writers, and software to print them. For example, in case C06, a Chinese offender (C06-No.01) entered Vietnam in 2013, then cooperated with Vietnamese criminals to produce counterfeit bank cards using two card writers, MSR208 and M90. In case C13, criminals also used two card writers, YKL608 and MSR609. It was not difficult to find these tools because they were used frequently and legally in many areas, such as financial services, business, and education.

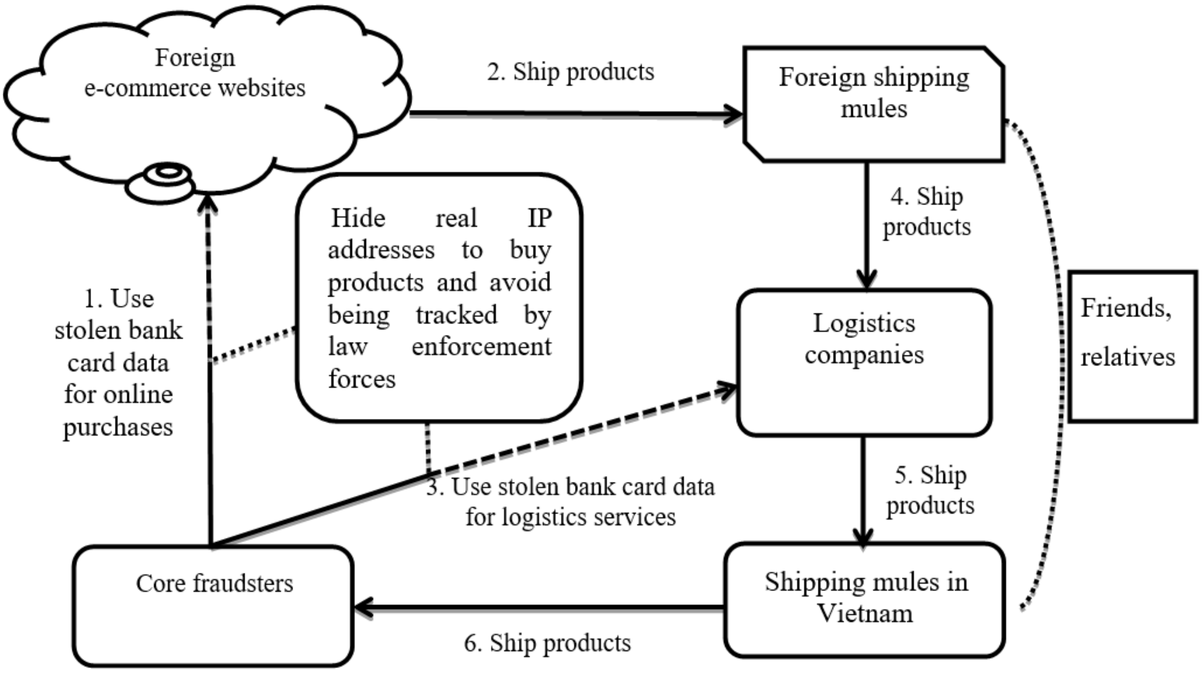
After collecting bank card data, fraudsters must find a suitable way to appropriate money from victims' bank accounts (Peretti 2008; Soudijn and Zegers 2012). Peretti (2008) clarified four types of carding: "online carding," "in-store carding," "cashing," and "gift card vending." The analysis of Vietnamese case studies showed that three forms existed in this context, each with different characteristics. In "online carding," offenders used stolen bank card data to make online purchases. They also used stolen bank card data to clone debit/credit cards to withdraw money at ATMs ("cashing") or conduct fake transactions through POS terminals ("in-store carding").

Online purchases ("online carding")

All six networks (C01, C03, C04, C05, C07, and C08) under the management of Vietnamese core fraudsters used stolen debit/credit card information to buy products, software, or services online. In these cases, the most frequent method was the use of bank card data to order high-value and lightweight products on American e-commerce websites. Figure 5.2 illustrates the basic steps of buying and shipping the carded products from the US to Vietnam.

First, using the technique of masking their real IP addresses, Vietnamese core fraudsters purchased products online on foreign e-commerce websites, such as Amazon and eBay, using

Figure 5.2. Crime scripts of bank card data fraud for online purchase at the "activity" stage


Foreign e-commerce websites
2. Ship products
Foreign shipping mules
4. Ship products
Hide real IP addresses to buy products and avoid being tracked by law enforcement forces
1. Use stolen bank card data for online purchases
Logistics companies
Friends, relatives
3. Use stolen bank card data for logistics services
5. Ship products
Core fraudsters
Shipping mules in Vietnam
6. Ship products

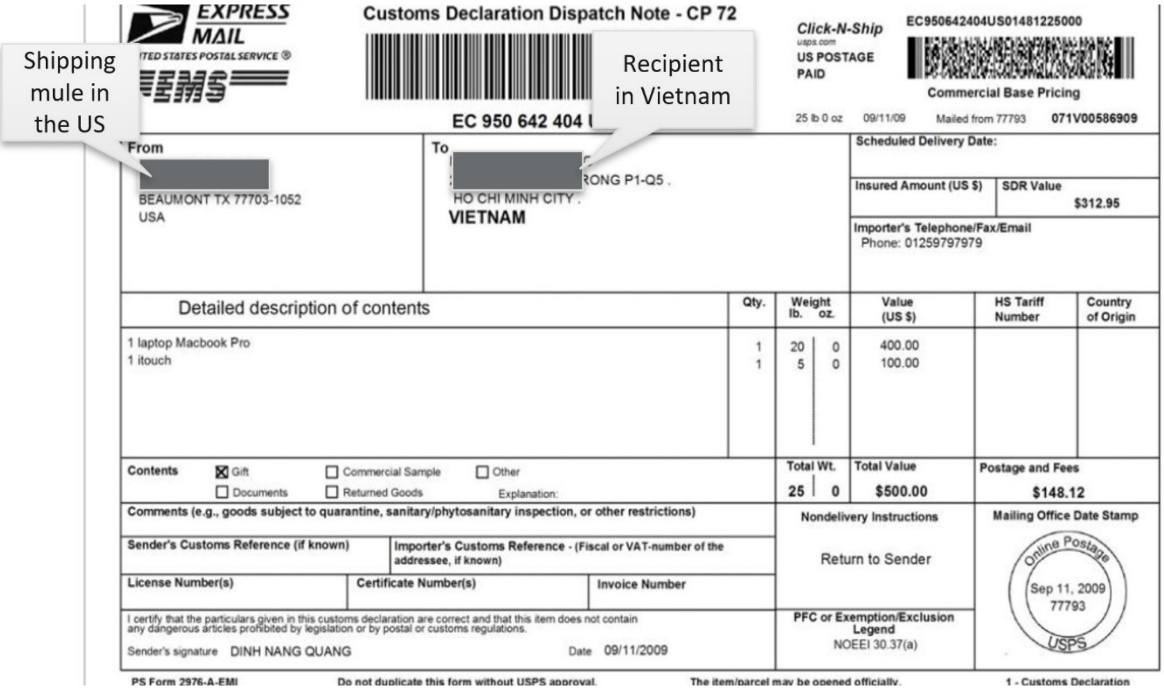
stolen bank card data (1). Foreign shipping mules then received products in the US before reshipping them to Vietnam via logistics companies (2); the core fraudsters used stolen bank card data to pre-pay shipping services from these companies (3). Subsequently, via mail, core fraudsters provided shipping mules with prepaid shipping labels that included the sender, recipient, and product information (see Figure 5.3).

Under the instruction of Vietnamese core fraudsters, foreign shipping mules repackaged the merchandise, printed labels, and attached the labels to the products before handing them to the logistics companies (4). In some circumstances, fraudsters' friends or relatives might support them by bringing products from the US to Vietnam. Shipping mules in Vietnam received the products (5) and then transported them to the addresses provided by the core fraudsters (6).

In case C08, besides buying products online, fraudsters also used bank card data to buy domain names and software. The core offender (C08-No.02) used stolen credit card data to buy the SugarCRM software and 34 domain names (including 25 international and nine Vietnamese domains (.vn)), which cost US$2,300. Almost all domains were bought via the EuroDNS.com website.

Counterfeit cards

Figure 5.3. A shipping label in case C03


Shipping mule in the US
Recipient in Vietnam

EXPRESS MAIL
UNITED STATES POSTAL SERVICE ®
EMS

Customs Declaration Dispatch Note - CP 72

EC 950 642 404 U

Click-N-Ship
usps.com
US POSTAGE
PAID

EC950642404US01481225000

Commercial Base Pricing

25 lb 0 oz 09/11/09 Mailed from 77793 071V00586909

From
[redacted]
BEAUMONT TX 77703-1052
USA

To
[redacted] RONG P1-Q5 .
HO CHI MINH CITY .
VIETNAM

Scheduled Delivery Date:

Insured Amount (US $)

SDR Value $312.95

Importer's Telephone/Fax/Email
Phone: 01259797979

Detailed description of contents	Qty.	Weight lb.	oz.	Value (US $)	HS Tariff Number	Country of Origin
1 laptop Macbook Pro	1	20	0	400.00		
1 itouch	1	5	0	100.00		

Contents ☒ Gift ☐ Commercial Sample ☐ Other
☐ Documents ☐ Returned Goods Explanation:

Total Wt. 25 | 0

Total Value $500.00

Postage and Fees $148.12

Comments (e.g., goods subject to quarantine, sanitary/phytosanitary inspection, or other restrictions)

Sender's Customs Reference (if known)

Importer's Customs Reference - (Fiscal or VAT-number of the addressee, if known)

License Number(s)

Certificate Number(s)

Invoice Number

I certify that the particulars given in this customs declaration are correct and that this item does not contain any dangerous articles prohibited by legislation or by postal or customs regulations.

Sender's signature DINH NANG QUANG Date 09/11/2009

Nondelivery Instructions
Return to Sender

PFC or Exemption/Exclusion Legend
NOEEI 30.37(a)

Mailing Office Date Stamp
Online Postage
Sep 11, 2009
77793
USPS

PS Form 2976-A-EMI Do not duplicate this form without USPS approval. The item/parcel may be opened officially. 1 - Customs Declaration

Stolen bank card data was also used to produce magnetic stripe cards to withdraw cash directly from ATMs or implement transactions via POS terminals. Five out of six cases of counterfeit card production were led by Chinese leaders. The remaining case C13 was managed by one Korean and one Vietnamese leader. Only the Chinese leader of C06 maintained residence in Vietnam, while the remaining foreign leaders entered Vietnam for short periods to operate scams. Under leader supervision, ATM withdrawals often occurred in the late evening. In case C20, for example, offenders withdrew money from an ATM at midnight. The ATM was located outside on the street and far from busy residential areas. Explaining the time of the transaction, investigator I14 said:

> In the late evening, bank card owners often sleep, so they do not read instant bank messages that inform them about transactions. They often do not find out about the fraudulent transaction until the next morning when they wake up. This late-night [activity] probably enables illegal behaviors to be undetected by victims, banks, and LEAs. Moreover, Vietnamese banks limit the maximum daily transaction; therefore, fraudsters often choose midnight to withdraw the maximum quantity of cash over two days. (Interview #14)

The crime script of "in-store carding" in Vietnam differs from the form implemented by European and American fraudsters (Peretti 2008), who use cloned bank cards to pay for products and/or services at retail stores. In Vietnamese cases, cloned bank cards were used to conduct fake transactions, which means that no products and/or services were exchanged. Instead, there was often a handshake between core fraudsters and POS owners to withdraw money from banks.

Flee

In cases of online purchases, there was no sign that criminals fled immediately after committing the crime; they only absconded when they realized their illegal behaviors might be detected by LEAs. These criminals lived and/or worked in one specific location, which they could use to commit TCF. However, in cases of counterfeit card production, fraudsters, especially core members, often did flee immediately after obtaining the money. For example, C20—one of the Chinese criminal networks—used skimming techniques to produce counterfeit cards and withdraw cash at ATMs. The Chinese offenders migrated to Vietnam and moved throughout multiple cities. As transient criminals, they only lived and operated in each city for several days before traveling to another location to continue their operation.

5.3.2. Phone scams

Analysis of the eight phone scam networks revealed two types of important actors: fraudulent callers and money mules under the management of foreign leaders. Thirteen out of 14 identified leaders were Chinese, Taiwanese, and Korean. Only one leader was Vietnamese within a subgroup of Taiwanese leaders based in Taiwan. To implement the entire phone scam process, the leaders of fraudulent networks needed to recruit both callers and money mules.

Recruit members

Fraudulent callers were hired by network leaders to carry out scam VoIP calls to victims. According to Leukfeldt, Kleemans, et al.'s (2017) model, callers can be regarded as core members who directly implement fraudulent calls to victims. Working as "employees" of a company, they received salaries from leaders after they finished a job and returned to their countries. Generally, in cases involving foreign victims, foreign callers were recruited in their home countries before arriving in Vietnam. In cases involving Vietnamese victims, Vietnamese callers were either recruited in Vietnam before moving to other countries under the direction of Chinese or Taiwanese bosses, or could be recruited from migrant laborers living in Mainland China or Taiwan.

There was little detailed information about how fraudulent callers are recruited. Among all eight sample cases of phone scams, only case C12 provided clear information about how callers were selected by the network's leaders. Recruitment occurred online via WeChat, which is a popular Chinese messaging and social media app. In 2013, the Taiwanese recruiter made acquaintance with a Vietnamese offender (C12-No.02) on WeChat. This Vietnamese offender was persuaded to go to China to become a translator for C12-No.09 with a promised salary of 15 million VND/month (equal to US$750). However, when C12-No.02 met C12-No.09 in China, C12-No.02 was trained to become a fraudulent caller. Two months later, C12-No.02 was assigned to become a recruiter of money mules after failing to carry out fraudulent calls; after all, C12-No.02 had not been aware of their real job purpose until meeting the recruiter.

Money mules were recruited to interrupt the financial trails that could lead LEAs to core members (Soudijn and Zegers 2012; Leukfeldt, Kleemans, and Stol 2017; Leukfeldt, Lavorgna, and Kleemans 2017). Many money mules who used their identity cards (cases C11, C12, C16, and C17) did not realize the true nature of their actions; whereas, criminal money mules used counterfeit identity cards (cases C11, C14, and C16) to open bank accounts. Financial benefits were the main motivation to become a money mule, as a sum of money was paid for each bank account and successful fraud case. In case C12, for example, the money mules (C12-No.04, C12-No.05, C12-No.06, and C12-No.07) were paid from 1.5 million VND (about US$75) to 2.5 million VND (about US$125) per fraudulent bank account, as well as 5% of the total fraud money, which was transferred to the money mules' own bank accounts.

Money mules were recruited through an online and offline process, mainly based on real social relationships with recruiters. The recruitment process began when network leaders employed enablers who were later responsible for recruiting money mules. In the sample cases, the interactions between leaders and enablers occurred mainly online via WeChat and Facebook. Thereafter, these enablers developed a network of money mules offline from their real social relationships, demonstrating that such relationships still play a significant role in cybercrime networks (Leukfeldt 2014; Leukfeldt, Kleemans, and Stol 2017).

Prepare tools and locations

The investigation documents contained little detailed information about how fraudsters prepared tools to set up VoIP systems. However, as shared by investigator I02, "It is not too complicated to find VoIP tools. There are legal service providers with many VoIP plans that fraudsters can buy to implement fraudulent calls to victims."

Migration is an important dimension of phone scams (Lee 2020). In cases involving foreign victims (C12, C15, and C18), foreign callers entered Vietnam to set up VoIP calling systems. In these cases, all offenders and victims were Chinese, Taiwanese, and Korean. Whereas, in cases involving Vietnamese victims, Vietnamese callers operated outside Vietnam under the direction of Chinese or Taiwanese leaders. Callers were divided into small groups living at specific locations, which were commonly houses in uncrowded neighborhoods or isolated apartments. Suspects enhanced the security at these locations by covering windows, installing CCTV cameras for surveillance, or even building iron fences around the property.

Fraudulent callers were provided with a list of potential victims' phone numbers by the network leaders. While the investigation files did not clearly show how fraudsters sourced these phone numbers, investigator I04 of case C11 revealed:

> Fraudsters can purchase lists of phone numbers online. It is easy to obtain databases of phone users in Vietnam as many providers sell them. Although Vietnamese law prohibits the acts of purchasing and sharing private information, the protection [of private information] has not been strictly guaranteed; therefore, purchasing private information, such as phone numbers, is as easy as pie. Phone scammers can make use of this situation to obtain a list of phone numbers of victims. (Interview #04)

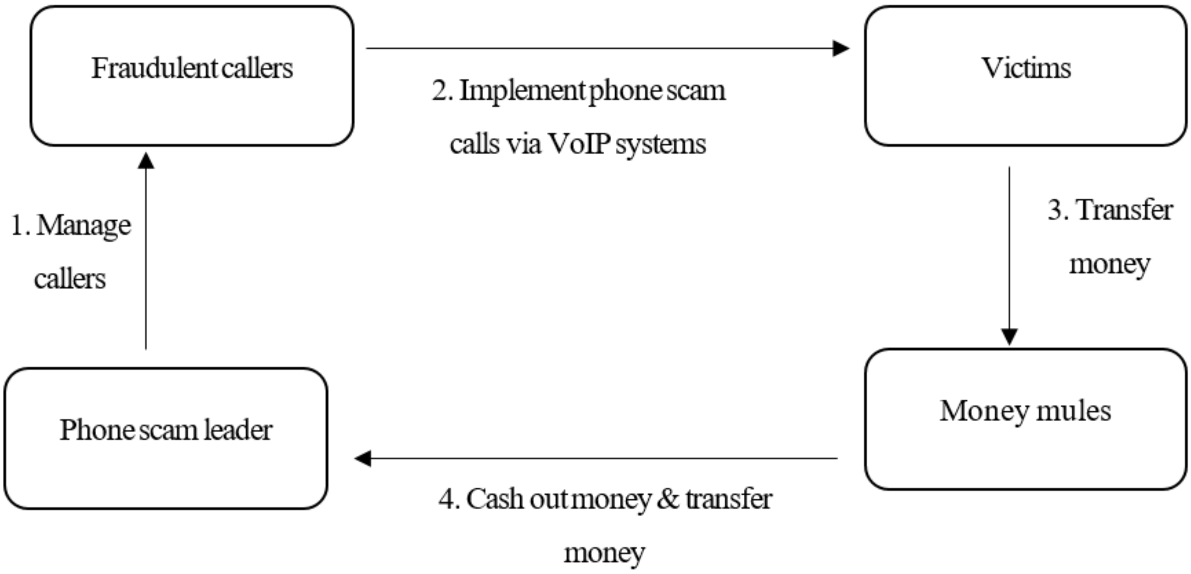
Make fraudulent calls to victims

Similar to cases in Korea (Choi et al. 2017), fraudsters used a list of phone numbers to make random calls to a large number of individuals. Under the direction of phone scam leaders, fraudulent calls were implemented based on a continuous script on which callers had been previously trained (see Figure 5.4). Pretending to be law enforcement officials, such as police officers, prosecutors, or court officials, was the most frequent trick employed among cases involving Chinese, Taiwanese, and Vietnamese victims. Fraudulent callers used VoIP calls to contact victims, pretend to be authorities, and threaten victims about suspicious financial activity. After the victims were convinced, fraudsters requested that they transfer money from their bank accounts to the money mules' accounts. After the victims had transferred the money, fraudsters could continue to extract money from the same victims until they detected the truth.

In contrast, in Korean case C15, fraudsters uploaded information about products to Korean e-commerce websites or forums. When Korean customers attempted to buy these products, fraudulent callers contacted them via VoIP calling systems from Vietnam using fake numbers that seemed to originate from Korea. After customers transferred money to purchase the goods, fraudsters ceased contact with them without sending the products.

Receive illegal money

Figure 5.4. Crime scripts of standard phone scams at the "activity" stage



After victims sent money, it was withdrawn by money mules or a money mule recruiter who played an intermediate role between money mules and phone scam leaders. Money could also be transferred via many intermediate accounts before finally being withdrawn by core members (see Figure 5.4). Unlike the Korean case analyzed by Lee (2020), in Vietnamese cases, fraudulent money was withdrawn in different ways before being transferred to gang leaders. In case C11, money mules (C11-No.03, C11-No.04, C11-No.05, C11-No.06, and C11-No.07) went to banks to withdraw the illegal money immediately after being informed that victims had made a transfer. Money mule recruiters (C11-No.01, C11-No.02) then sent this fraudulent money to Chinese core members via many different bank accounts or a gold store. In case C12, the money mule recruiter (C12-No.01) withdrew the fraudulent money at ATMs, then brought it directly to another member (C12-No.02) who transferred it to Chinese core fraudsters via intermediate banks.

Flee

There was no evidence that members of phone scam networks fled immediately after their crimes. Scam callers could live together at one specific location for three to six months without official registration. Subsequently, they moved to new locations to live and implement further phone scams under the management of leaders who could stay at these places. Therefore, these scam callers may be regarded as transient criminals. In contrast, money mule groups were based in one location as they often lived and conducted their activities around a specific area. They were in charge of opening bank accounts and withdrawing fraudulent money under the direction of their recruiters. Some money mules, who were aware of their criminal purpose, and the money mule recruiters often tried to escape when they suspected they were under investigation by LEAs.

5.4. Discussion

5.4.1. Vietnam: An operational base for domestic and foreign computer fraudsters

Vietnam can be regarded as an operational base for cybercrime, posing one of the most serious criminal threats in Southeast Asia (CSIS and McAfee 2018; Lusthaus 2020). This is a position reinforced by both local and foreign computer fraudsters operating in the country. Domestic hackers located in Vietnam can steal bank card data to obtain money from foreign victims. Only a small proportion of Vietnamese fraudsters directly steal databases of bank card information, with most buying card data in virtual domestic marketplaces or from professional hackers. The crime script of buying products online and then shipping them back to Vietnam is a frequent method of cashing out money. As foreign e-commerce sites block transactions and deliveries related to Vietnam, Vietnamese fraudsters adapt and find another suitable script to guarantee success; thus, IP-related tools and foreign shipping mules support Vietnamese fraudsters in committing transnational online purchase fraud.

Vietnam is notorious for its hacking community, since the hacking community is well-developed and certain members have become “black hat” hackers (Lusthaus 2020). In sample cases, only a small number of Vietnamese fraudsters stole bank card data themselves. However, the consequences were serious because a single Vietnamese hacker stole a large amount of bank card data, then sold it to other fraudsters. In contrast to American and European card fraud gangs (Leukfeldt, Kleemans, and Stol 2017; Peretti 2008), Vietnamese hackers focus on exploiting the SQL injection errors of foreign e-commerce sites to hack data. Owing to this technique, one Vietnamese hacker can obtain thousands, even millions, of pieces of bank card data, which can then be sold on virtual hacking forums and used to appropriate money from cardholders. Such illegal behaviors may lead to a “snowball effect” which extends computer fraud networks. Bank card data buyers can use data for online purchases, or resell it to others to get profit.

In the case of phone scams, Vietnam can be considered an attractive location for foreign culprits to enter and use the country’s sovereignty as a base for operating transnational scam calls. As border-crossing is a typical feature of transnational crime, foreign scammers immigrate to Vietnam to make fraudulent calls back to their own countries. In cases C02, C15, and C18, all offenders and victims were Chinese, Taiwanese, and Korean. In these cases, the ICT infrastructure supported foreign fraudsters in conducting phone scams from Vietnam to their home countries.

The possibility that Vietnam could become a major operational base for TCF is the result of multiple factors, such as the rapid development of ICTs and the slow progress of LEAs in crime suppression. Google and Tamasek (2018, p.7) described Vietnam's Internet economy as "a dragon being unleashed" with the annual rate of growth at over 40%. Many aspects of Vietnamese society have adjusted quickly to the development of ICT, whereas Vietnamese LEAs have faced big issues concerning policy, legislation, techniques, and human resources in fighting computer fraud (HTCP Department 2017). Some dangerous behaviors, such as collecting bank card data, were just added to the 2015 Penal Code. This means that before the 2015 Penal Code was enacted, it was difficult to prosecute suspects who only stole bank card data, but did not have any further illegal intent, or whose criminal purposes could not be proven beyond a doubt. Furthermore, Vietnamese hacking forums provided an ideal virtual setting for cybercriminals and potential criminals to discuss and share skills, tools, and bank card data. Therefore, even if only a small proportion of these domestic hackers became "black-hat" hackers, Vietnam would possess some of the most serious cybercrime threats in the region (Lusthaus 2020). The "snowball effect" can turn ordinary individuals into cybercriminals who are not specialized in ICT but can obtain illegal money via virtual space.

5.4.2. The comparison between the modus operandi of bank card fraud and phone scams in Vietnam

From the pre-crime to post-crime stage, the crime scripts of bank card fraud and phone scams in the Vietnamese context have much in common. First, in the preparation stage, fraudsters must recruit money mules and other auxiliaries to establish a fraudulent network. They also need to prepare tools for obtaining victims' assets and/or reduce the likelihood of detection. Subsequently, cybercriminals must find a way to cash out and transfer money into benefits for core fraudsters. Except for cases of producing counterfeit cards, after appropriating illegal money, computer fraudsters often do not escape immediately and seem confident that their illegal behaviors are difficult for LEAs to trace. Moreover, in both types of computer fraud networks, there are members recruited to support core fraudsters but who are unaware of the real purpose of their activities. For example, money mules are recruited to receive fraudulent products or money, but often do not recognize that these are criminal behaviors.

In general, TCF is a form of financial crime anchored at the intersection of three elements: fraud, technology, and transnationality. Among them, technology facilitates the process of defrauding victims and influences the transnational characteristics of criminal activities. In terms of technological factors, bank card data fraud is more high-tech than phone scams. In particular, sourcing bank card data requires a high level of technological skill to allow fraudsters to attack websites. Vietnamese fraudsters apply high-tech tools such as automated software to test for errors, skimming devices to capture bank card data, and fake IP tools. The automation of such tools not only improves the efficiency of experienced attackers but can also expand the potential hacker community (IMPERVA 2008). Further, technology allows core fraudsters to recruit enablers online, maintain communication, and implement online transactions. In phone scams, technology is used to enhance fraudulent activities by replacing traditional phone calls with VoIP call systems. Technology enables fraudsters to call victims from other countries using fake phone numbers. As per the continuum illustrated by Gordon and Ford (2006), TCF may also include crimes with only minor technological elements, as well as those crimes with almost entirely technological factors.

Similar to cases in The Netherlands (Leukfeldt et al. 2017), there is a strict correlation between the extent of the technology used and the interaction between offenders and individual victims. Compared with bank card fraud, phone scams require a lower degree of technology but feature a higher degree of interaction between offenders and individual victims. Offenders use VoIP calling systems to contact, persuade, and deceive victims to transfer money. However, bank card fraud cases do not require any interaction between offenders and individual victims. In ATM-related cases, attackers use skimmers to capture bank card data automatically, whereas when hackers attack websites, they can use SQL injection techniques to access customers' bank card data. Furthermore, a large number of fraudsters obtain bank card data from underground websites or other professional enablers. In terms of cashing out, bank card data can be used for online purchases or to produce counterfeit cards to withdraw cash at ATMs or perform fake transactions via POS terminals. Thus, no direct interaction occurs between fraudsters and individual victims (Hutchings and Holt 2015), which means that technology plays an important role in the indirect interaction between them (Leukfeldt, Kleemans, and Stol 2017).

Finally, there are differences in the roles of Vietnamese and foreign offenders among specific types of fraud networks. In online purchase networks, Vietnamese fraudsters are often high-level core actors within the criminal networks; foreigners who play the role of enablers support Vietnamese criminal networks to ship products. In contrast, in counterfeit card and phone scam networks, Vietnamese offenders are often low- or mid-level members, or they do not appear in criminal networks. In these cases, Vietnamese criminals maintain their roles as money mules and fraudulent callers under the direction of Chinese or Taiwanese bosses. Similar to the cases analyzed by Lee (2020) and Shin (2018), Chinese or Taiwanese leaders often remain behind the scenes to operate transnational phone scam networks. In three of the cases examined (C02, C15, and C18), all offenders operating in Vietnam were foreign.

5.5. Conclusion

This chapter elucidates the process of TCF in Vietnam using crime script analysis to examine two types of crime: bank card data fraud and phone scams. As a new emerging center of cybercrime, Vietnam is likely to become an operational base for both domestic and foreign criminals to carry out computer fraud. The study found that TCF, as an intersection between fraud, technology, and transnationality, does not require a direct interaction between offenders and individual victims. There are also certain big differences in the modus operandi between bank card fraud and phone scams: Bank card data fraud requires more technology use, and the role of Vietnamese and foreign offenders in the two types of TCF is different. Understanding the modus operandi of TCF in the Vietnamese context is the intermediate step to clarify the structure of TCF networks in the following chapter.

CHAPTER VI: THE STRUCTURE OF CYBERCRIME NETWORKS: TRANSNATIONAL COMPUTER FRAUD IN VIETNAM

6.1. Introduction

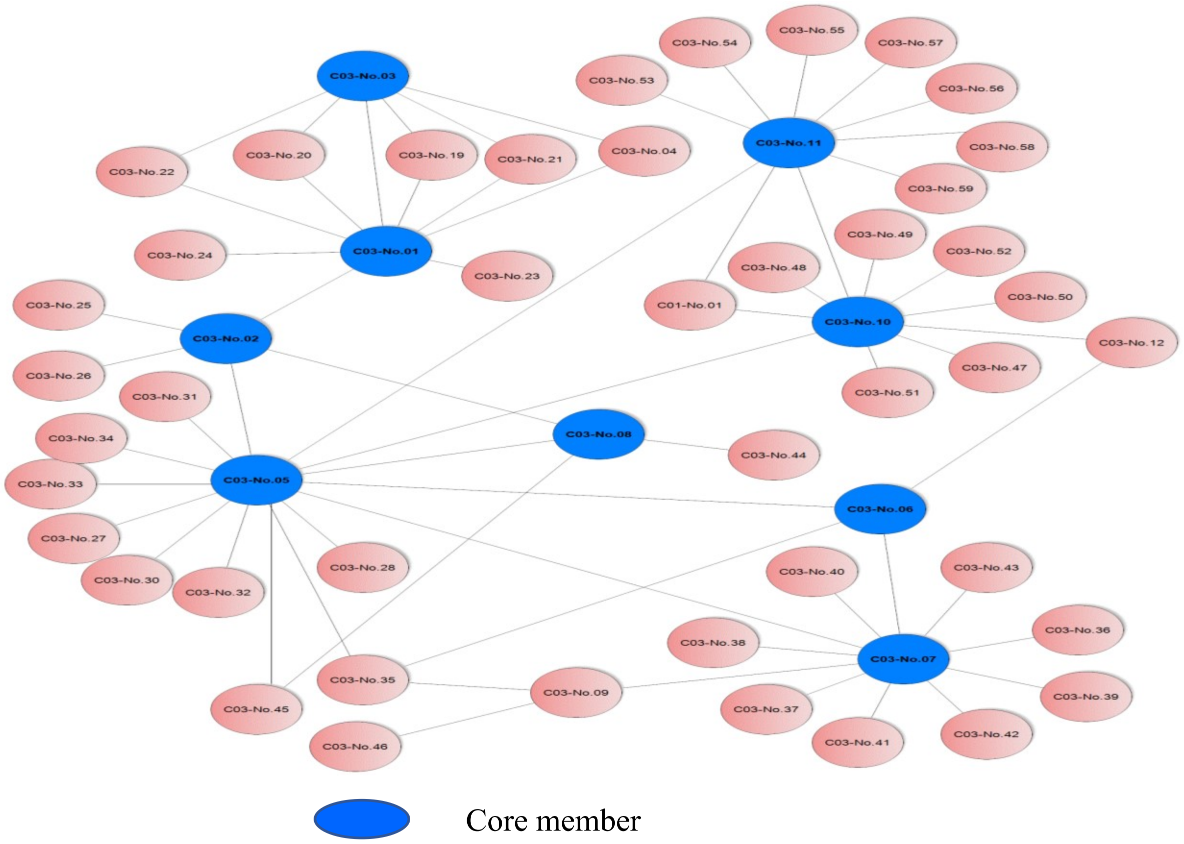
This chapter focuses on presenting the findings and discussion of Question 2: "How are cybercrime networks structured to conduct TCF." From exploring the modus operandi of TCF in the Vietnamese context, this chapter clarifies TCF networks' structure, contributing to more understanding of the nature of cybercrime networks. By examining Vietnamese TCF networks, it aims to identify the organizational structure and central actors of cybercrime networks. This chapter has been divided into four main sections. After the introduction, the second section shows the findings of exploring TCF networks' structure. This section is presented with three types of TCF networks: networks of online purchases, networks of making fake cards, and networks of phone scams. Subsequently, the third section discusses the remarkable structural characteristics of TCF networks. Accordingly, the organizational structures of TCF networks have distinctive characteristics. Moreover, this section proposes that the clear degree of leadership within cybercriminal networks can be used to construct a new typology with four categories: *"swarm networks," "distributed networks," "single-directed networks,"* and *"group-directed networks."* The last section concludes this chapter by restating important information.

6.2. Findings

6.2.1. Networks to use stolen bank card data for online purchases

Networks of online purchases comprise numerous subnetworks, with core fraudsters constituting the central hubs surrounded by other actors. However, as "disorganized" or "distributed" networks, the structure of these networks is flat and lacks a clear hierarchical command and control model (Wall 2015). For example, in Figure 6.1, C03-No.01, C03-No.02, C03-No.03, C03-No.05, C03-No.06, C03-No.07, C03-No.08, C03-No.10, and C03-No.11 are the core members who established subnetworks to obtain money via stolen bank card data. Each core member was surrounded by professional enablers, who provided the necessary hacking tools and bank card data; customers, who hired them to order products; recruited facilitators, who found the shipping mules; and shipping mules, who received products from merchants. The subnetworks merged into a whole network as a result of the cooperation between core actors.

Figure 6.1. Structure of C03 network



The whole network could include a large number of actors connected to one another by core members, while the relationship between them remains very loose (see Appendix 5). The numbers of vertices (actors) of networks C01, C03, and C07 are 30 or above. These networks also have the lowest graph density (D) and average CC in comparison to other networks: D(C01) = 0.066, CC(C01) = 0.010; D(C03) = 0.045, CC(C03) = 0.006; and D(C07)=0.069, CC(C07) = 0.011. This indicates that they were sparse, loosely connected organizations with many isolated actors and relatively few connections between members. However, these networks have the highest average BC: BC(C01) = 33.514; BC(C03) = 60.519; BC(C07) = 32.533. Within these networks, the information flow runs via central actors with a very high value of betweenness centrality; for example, BC(C01-No.01) = 533, BC(C01-No.02) = 134, BC(C01-No.03) = 177, and BC(C01-No.18) = 134. This indicates the important role played by central actors in facilitating the flow within these loose networks.

Cooperation between core members could occur consistently over a long period of time, bringing numerous advantages to the network (Nurse and Bada 2018). First, they could share hacking tools, bank card data, as well as information about trustworthy money mules and enablers. With respect to this, the position of core actors and enablers could change in subnetworks. For example, in the first subnetwork, the core member (C03-No.02) was surrounded by credit card providers (C03-No.08) and two shipping mules (C03-No.25 and C03-No.26). When sharing bank card data with C03-No.01, C03-No.02 retained the position of a professional enabler in C03-No.01's subnetwork.

Additionally, a core member could hire other core actors to order products online in the event that they received too many order requests from customers. Figure 6.2 illustrates the C01 network; in this network, the core actor (C01-No.01) advertised online the ability to buy products online. C01-No.01 received numerous requests from customers and transferred these requests to other core members, namely, C01-No.02 and C01-No.03, who were responsible for ordering the products. In the entire C01 network, C01-No.01 served as a coordinator, distributing missions and financial benefits to other core members and shipping mules.

Most fraudsters preferred operating and contacting one another online (Nurse and Bada 2018). In all five online purchase networks, almost all core members bought stolen credit card data online from professional enablers. They transferred money to other members using digital money transfer services such as Liberty Reserve, WebMoney, Paypal, and Western Union. Shipping mules were recruited via hacking forums or online advertisements. Figure 6.3 shows the C07 network; in this network, the core actor (C07-No.01) used two accounts—" root.kits" and "hackervietnams"—to contact other members online. C07-No.01 recruited three money mules (C07-No.12, C07-No.13, and C07-No.14) via the virtual forum, hkvfamily.info. The shipping mules were responsible for receiving and sending products to Vietnam using logistics

Figure 6.2. Structure of C01 network

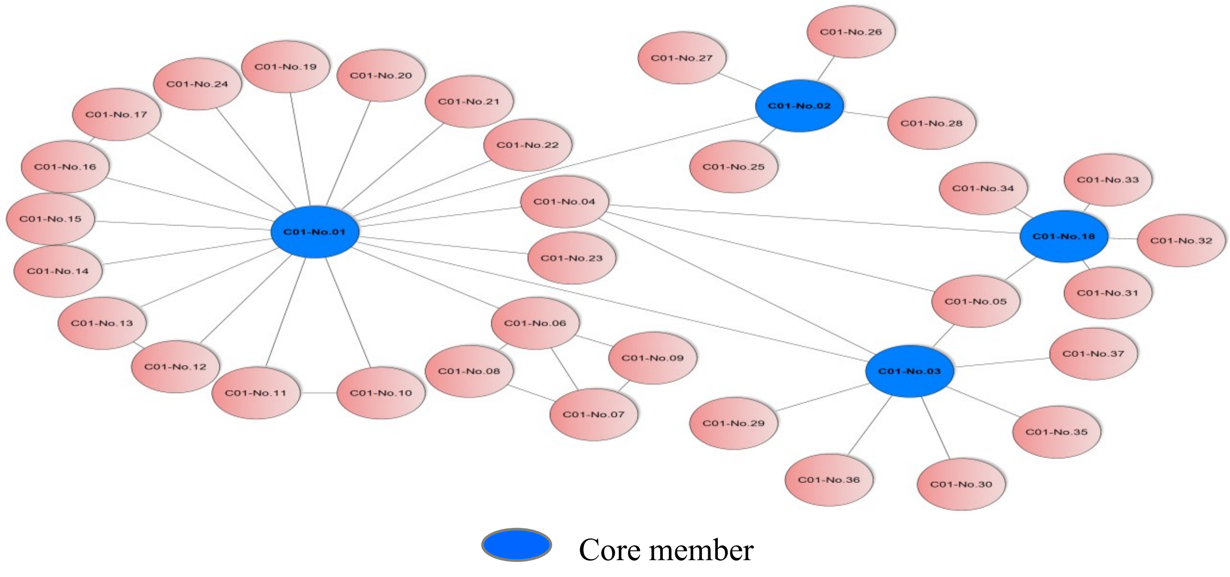
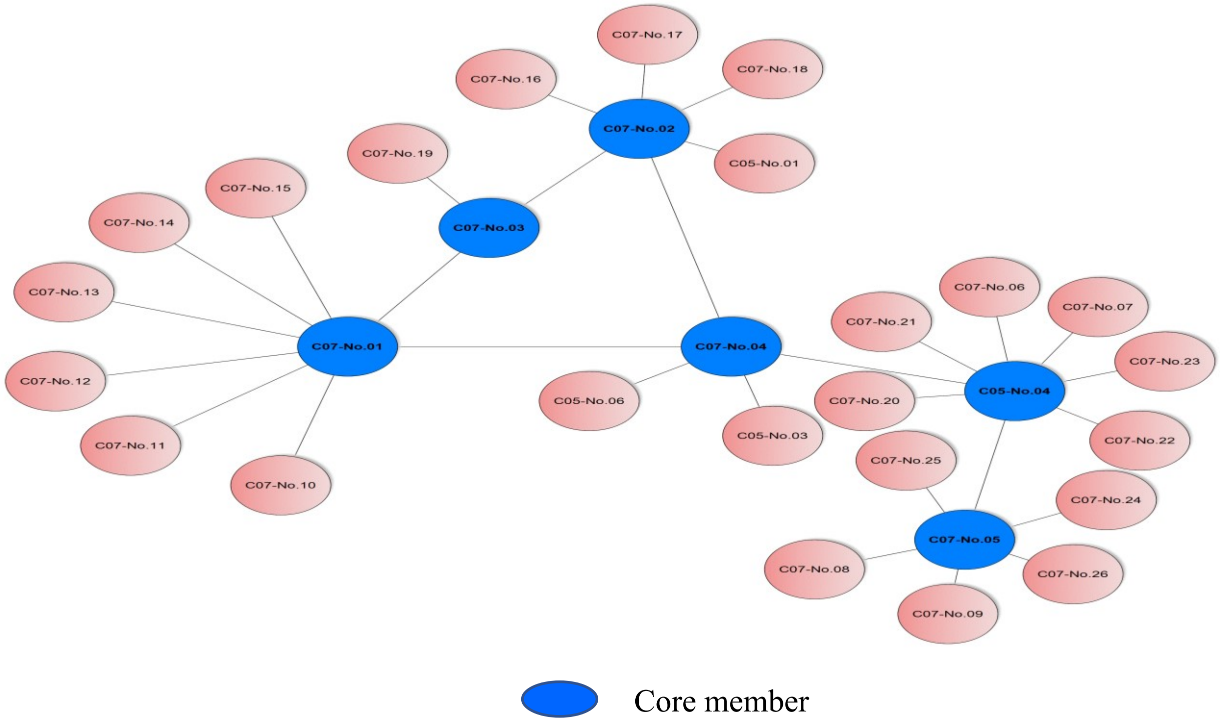


Figure 6.3. Structure of C07 network

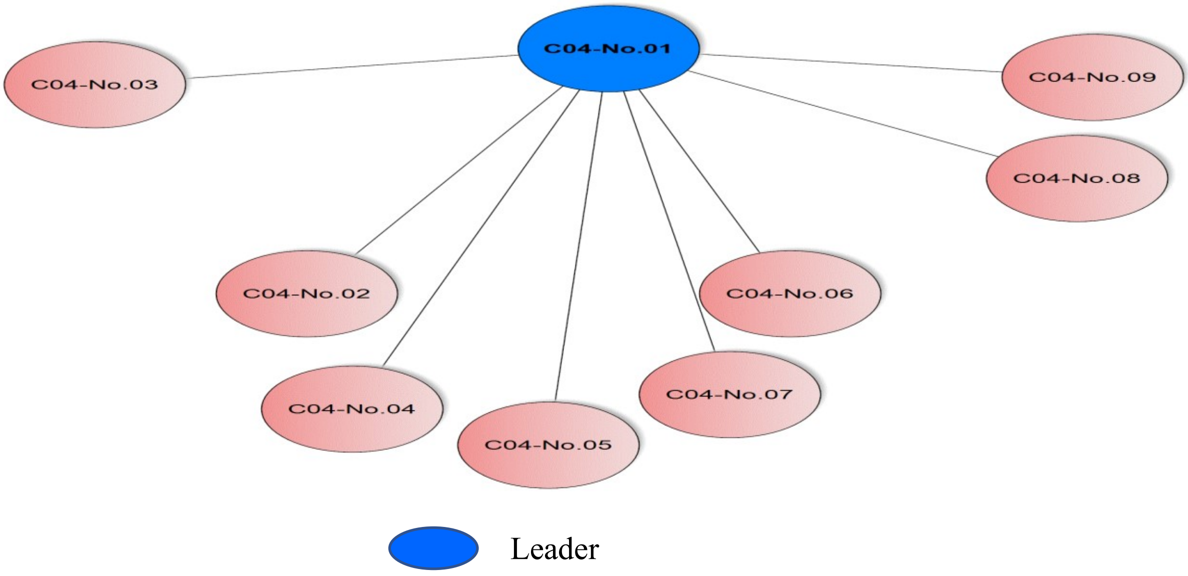


companies under the direction of the core member (C07-No.01) who communicated with them via email. At the time, C07-No.01 paid the shipping mules and other members through Liberty Reserve, a digital currency service shutdown by the US government in 2013, or banking services. As such, the online communication and digital money services enabled criminals to hide their real identities and money laundering activities from LEAs (Nurse and Bada 2018).

While face-to-face interaction seldom occurred in the sampled online purchase networks, trust remains a significant factor bridging co-offenders in offline and online crime networks (Kleemans and Bunt 1999; Leukfeldt, Lavorgna, and Kleemans 2017; Nurse and Bada 2018). Offline networks primarily operate on pre-existing social relationships (Kleemans and Bunt 1999). Accordingly, trust within online purchase networks could be constructed over a long period of time, as some core members have worked together several times before.

Additionally, trust could be built on the foundation of ranking systems existing in virtual hacking forums (Leukfeldt, Lavorgna, and Kleemans 2017). For example, in the forum *vietexpert.info*, the rating system was based on the number of times a user is "thanked" by other members. However, the number of "thanks" could be bought from admins at the price US$10 per 100 "thanks." As such, the ranking systems could be misused by untrustworthy members (Décary-Hétu and Dupont 2013).

Figure 6.4. Structure of core member network in C04 network



Comprising of nine core members, the C04 network had very high offline interaction. Constructed on the lines of a business model, such networks possess a clear division of labor to gain profits (Tropina 2012). The relationship between these core members was tight via the leader. As illustrated in Figure 6.4, under the guise of a legitimate company, the boss (C04-No.01) managed the employees face-to-face to establish a professional criminal network for exchanging stolen bank card data to gain money. As a central hub in a centralized network, C04-No.01 (BC[C04-No.01] = 28) was surrounded by other members (BC = 0), indicating that C04-No.01 controlled all information passing through the network. As the boss, C04-No.01 paid six employees monthly salaries ranging between VND 10,000,000–25,000,000 (equivalent to roughly US$500–1,250). Discussing the business model of the C04 network, investigator I03 from HTCP Department opined the following:

> The business model of this network was very professional to earn more profit and prevent detection by LEAs. The company was used as a cover for the fraudsters to implement cybercrime. The role of leadership was shown clearly in the network. The boss [C04-No.01] assigned specific missions to each follower. One culprit [C04-No.03] was in charge of buying stolen bank card data, while five other culprits specialized in selling card data for a profit. The two remaining members were responsible for receiving money via Western Union service. Each individual had specific roles that contributed to the success of computer fraud cases. (Interview #3)

Based on the operational profiles of the selected cases, almost all central actors in the five remaining networks, namely, C01, C03, C05, C07, and C08, were core members who initiated or coordinated the online purchases. It is unclear whether they held a leadership role. Similar to online hacker groups, they probably lacked an agreed leader responsible for directing and coordinating criminal operations (Nurse and Bada 2018). In this respect, the leadership role of core members was only reflected in the purchasing of bank card data from professional enablers and hiring of shipping mules to receive products from merchants. In a few situations, the core actors employed one another to order products.

Although the networks that use bank card data for online purchases are seldom hierarchical, hacking forum networks appear to operate under a strict hierarchy. Carding forum is a popular platform among cybercriminals, which enables the discussion and sharing of information and tools related to bank card data (Nurse and Bada 2018; Soudijn and Zegers 2012). The samples examined by this study reflected a clear ranking between the members of the criminal forums, including *vefamily.com* (case C03), *mattfeuter.cc* (case C04), and *vietexpert.info* (case C05). Figures 6.5 and 6.6 illustrate the model of *vefamily.com*, which can be regarded as the representative of Vietnamese hacking forums.

As per the examined criminal profiles, in 2008, P.X.N. initially established *vefamily.com* as the meeting point where fraudsters could exchange information regarding computer fraud and how to attack websites. In June 2010, P.X.N created an administrative board comprising of seven administrators ("admins") at the highest level of administration, two super moderators ("super mods") at the second level, and nine moderators ("mods") at the third level. The administrative board had the right to create content and delete the topics and sections of lower ranked participants. The nine "mods" were responsible for managing particular subforums, including Domain–Hosting–Server, Credit Card & Full Info, VietExpert Adult Zone, Sock & Proxies, Paypal–Mail/Pass, Gambling–Gameshow, and Box Report Logs (Figure 6.6). Operating from 2008 to 2011, *vefamily.com* attracted over 2,000 members with an approximate 500,000 reports. The content of *vefamily.com* was divided into subforums comprising of 58 sections in total.

Membership to *vefamily.com* was initially free. The forum had the characteristics of a "disorganized" model of organization, as it lacked a hierarchical command and a control structure (Wall 2015). However, as its membership grew, the forum's structure was reorganized, so that a new member could be introduced by the prestigious members to gain acceptance. Each new member had to pay a participation fee of US$25, as well as US$5–10

Figure 6.5. Structure of vefamily.com

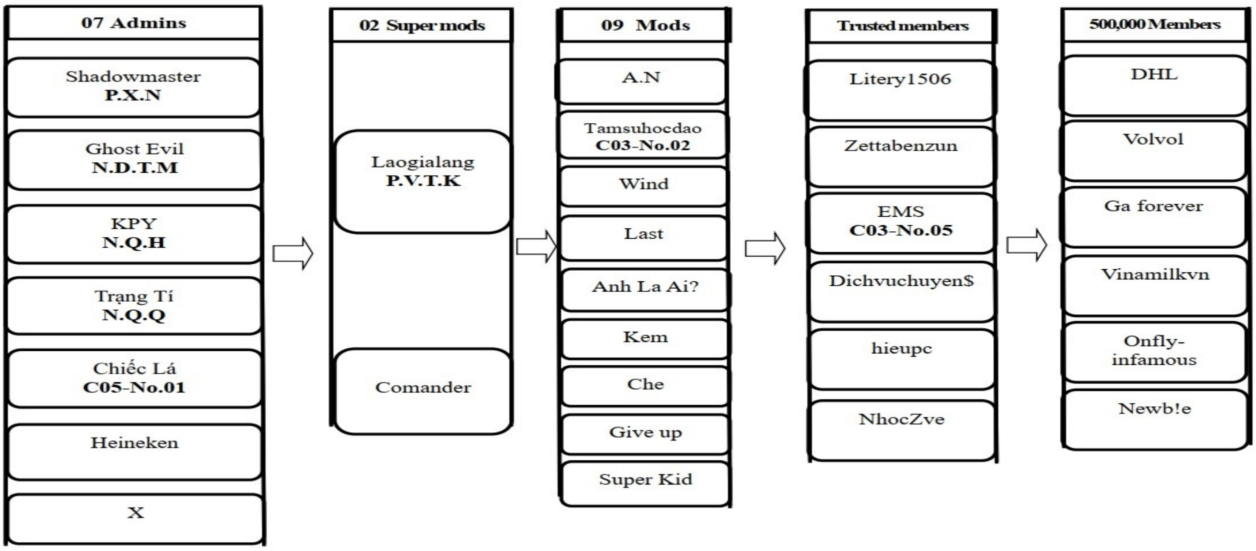
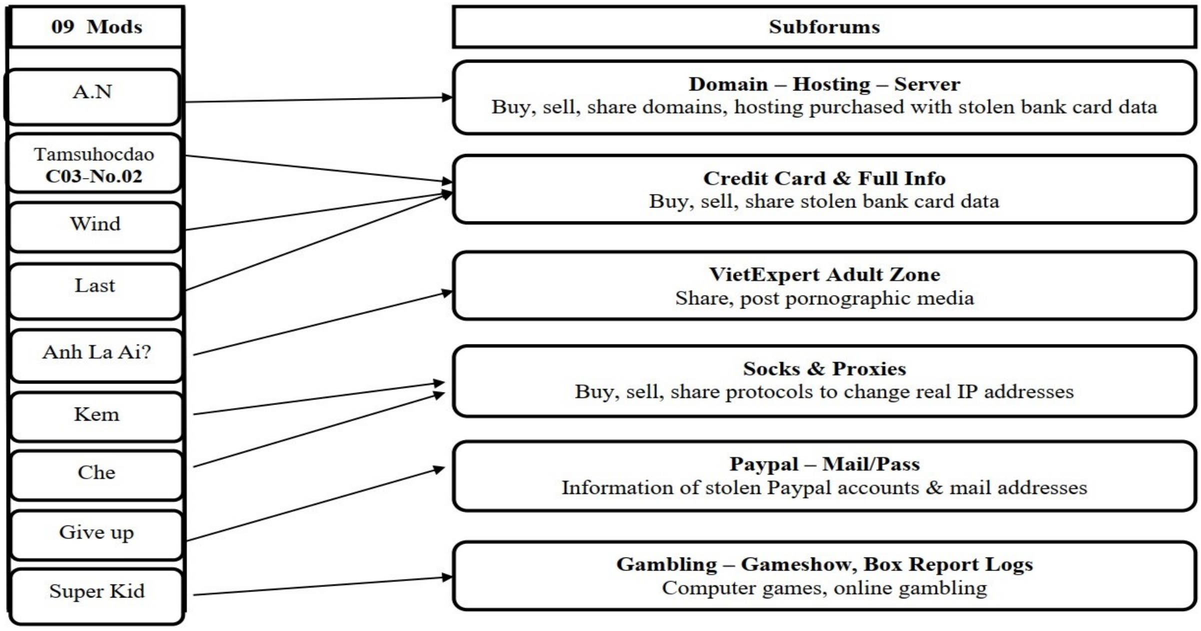


Figure 6.6. Responsibilities of nine vefamily.com mods


09 Mods
A.N
Tamsuhocdao
C03-No.02
Wind
Last
Anh La Ai?
Kem
Che
Give up
Super Kid
Subforums
Domain – Hosting – Server
Buy, sell, share domains, hosting purchased with stolen bank card data
Credit Card & Full Info
Buy, sell, share stolen bank card data
VietExpert Adult Zone
Share, post pornographic media
Socks & Proxies
Buy, sell, share protocols to change real IP addresses
Paypal – Mail/Pass
Information of stolen Paypal accounts & mail addresses
Gambling – Gameshow, Box Report Logs
Computer games, online gambling

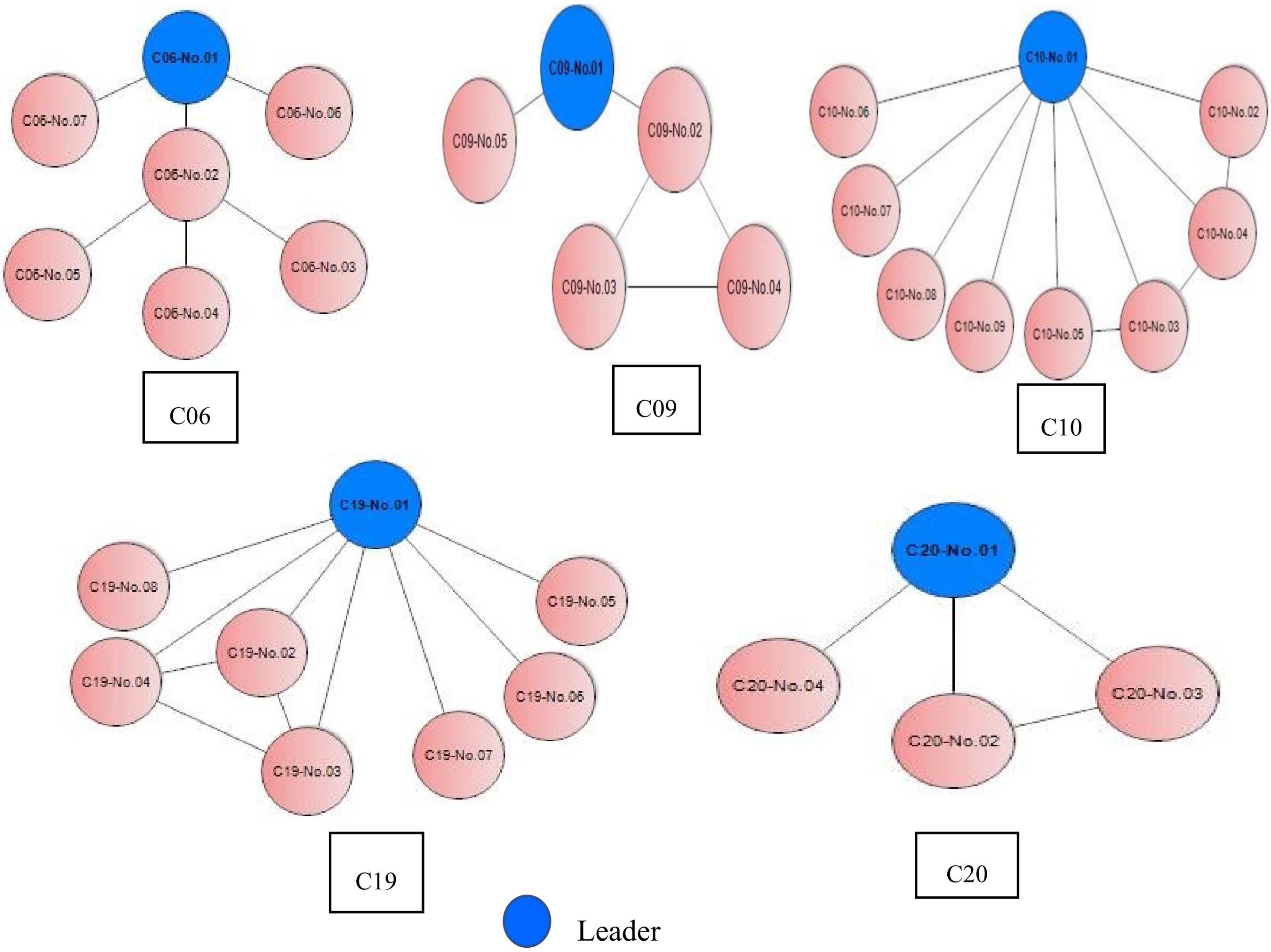
in monthly fees via Liberty Reserve. If a member violated forum rules, administrative boards had the right to implement online punishments such as reducing the membership level or deleting the account. The strict regulations facilitated the creation of trust between members and prevented the detection of forum by LEAs (Corritore, Kracher, and Wiedenbeck 2003; Lusthaus 2012; Nurse and Bada 2018).

6.2.2. Networks using stolen bank card data to make fake cards

In contrast to online purchase networks, networks using stolen bank data to make fake cards were often tighter and had fewer members. These networks have a maximum of 12 vertices, which is much lower than online purchase networks. However, the average CC values of these networks are often higher than those of online purchase networks. This indicates that the members within these networks generally shared closer communication with one another in comparison to online purchase networks.

As Figure 6.7 shows, the five fake card networks, C06, C09, C10, C19, and C20 had central actors with clear leadership roles. In the C10, C19, and C20 networks, the most central actor was the group leader. However, the most central actor was not necessarily the one with the greatest leadership potential. For example, in the C06 network, the most central actor, C06-No.02 (BC = 12, CC = 0.125), operated under one leader, C06-No.01 (BC = 9, CC = 0.111). Noticeably, the leader (C06-No.01) is a Chinese citizen who received stolen bank card data and

Figure 6.7. Structures of C06, C09, C10, C19, and C20 networks

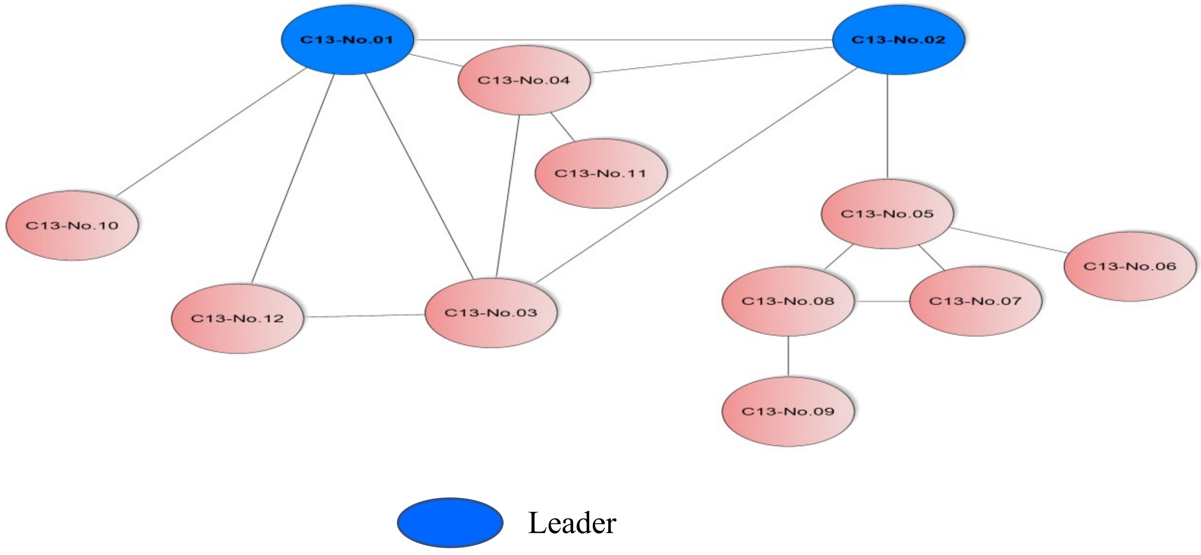


tools for making fake cards from two Chinese professional facilitators (C06-No.06 and C06-No.07) before entering Vietnam. C06-No.01 then cooperated with a Vietnamese recruiter (C06-No.02) to develop a network of fraudsters by recruiting three other Vietnamese money mules. Similarly, in another case (C09), one Chinese leader, C09-No.01 (DC = 2, BC = 3, CC = 0.167), cooperated with a Chinese professional enabler and directed network C09 via a Vietnamese culprit, C09-No.02 (BC = 4, CC = 0.200), who attracted more connections (DC = 3). This shows that the greatest leadership potential does not necessarily belong to the most central node. As detective I06 of C09 from Haiduong police station stated, "although the key offender was not involved anytime, anywhere, in any transaction, his contribution still played a steering role in the fraud group operation" (Interview #6).

Unlike these Chinese offenders, who first colluded with Chinese or Taiwanese foreign accomplices, Korean fraudsters colluded directly with Vietnamese counterparts in establishing their syndicate. As Figure 6.8 shows, in the C13 network, two leaders (C13-No.01 and C13-No.02) discussed about establishing a fraudulent network. The Vietnamese culprit, C13-No.02, was in charge of recruiting money mules who owned POS terminals. C13-No.02 then asked another culprit (C13-No.05) to borrow POS terminals from a small business manager (C13-No.06) and two company directors (C13-No.08 and C13-No.09). Meanwhile, the Korean culprit (C13-No.01) returned to Korea to find a source for stolen bank card data and the tools required to make fake bank cards.

In all six cases involving the making of fake cards, the professional enablers were foreign and lived outside Vietnam. They contacted core members via the Internet using Tencent

Figure 6.8. Structure of C13 network



QQ and WeChat messaging software, a popular instant messaging and chat service developed in China. Within the Chinese cybercriminal community, Tencent QQ is favored to carryout private communication concerning the black market for stolen bank cards (Yip 2011). This modus operandi facilitates the creation of a "hidden network" for sharing information and avoiding detection by police force. Indeed, the six cases lacked information concerning the arrest of professional facilitators.

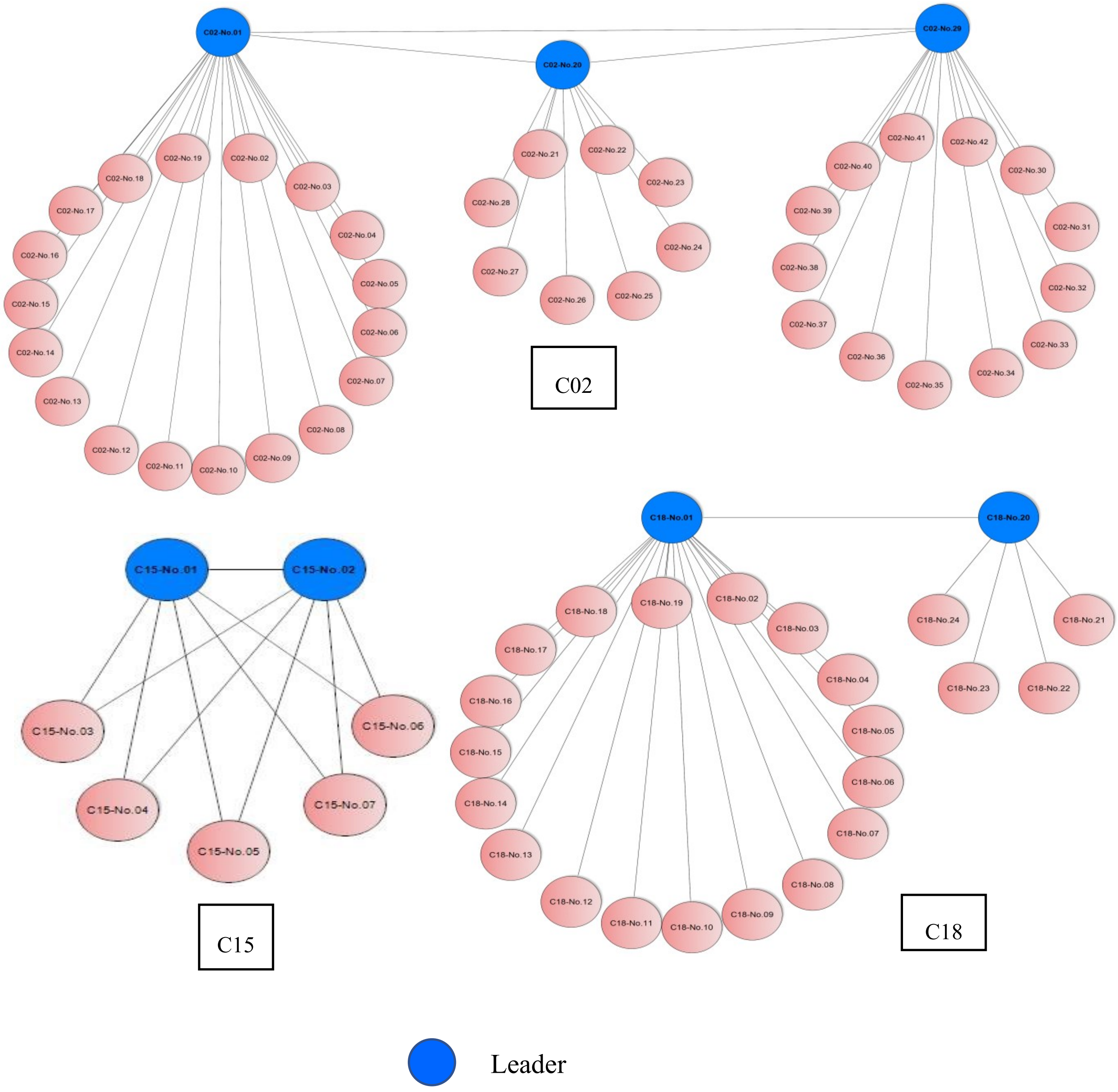
Meanwhile, the relationships between core members, recruited enablers, and money mules were established and maintained via direct meetings. Such offline relationship created a mutual trust between members, guaranteeing the success of their illegal activities (Kleemans and Bunt 1999; Leukfeldt, Lavorgna, and Kleemans 2017). However, they also made it easier to track them. For example, in the C13 network, the core actors (C13-No.01, C13-No.02, C13-No.03, and C13-No.04) were close friends. The core actor (C13-No.02) asked a recruited enabler (C13-No.05) to find POS terminals. The enabler (C13-No.05) then borrowed POS terminals from their other friends. Based on operational documents, the starting point of the investigation was the series of suspicious transactions implemented via the POS terminals of the money mules. The Hanoi HTCP subsequently cracked down the C13 network based on the real social relationships that existed between the members.

6.2.3. Networks of phone scams

The examined phone scam networks exhibited a clear division of labor and leadership involving two indispensable groups of money mules and callers. Each group had a different structure. The merging of the two groups produced an entire network of phone scams. In all the eight phone scam cases, the Vietnamese police forces were unable to identify the entire network. They were able to identify only one of the two groups: callers or money mules.

Figure 6.9 illustrates the structure of caller groups. These three networks comprised of Chinese, Taiwanese, and Korean culprits, who made scam calls from Vietnam to citizens in their home countries. The group of fraudulent callers can be divided into subgroups, with the whole network centralized around the leaders of each subgroup. The average BC of the two Chinese and Taiwanese caller groups is very high with many members, V(C02) = 42, BC(C02) = 30.976; and V(C18) = 24, BC(C18) = 13.542. In contrast, the Korean network had fewer members with a low betweenness centrality, V(C15) = 7, BC(C15) = 1.429. Similarly, all of the connections between the three foreign caller networks are achieved via several actors holding leadership positions.

Figure 6.9. Structures of caller networks



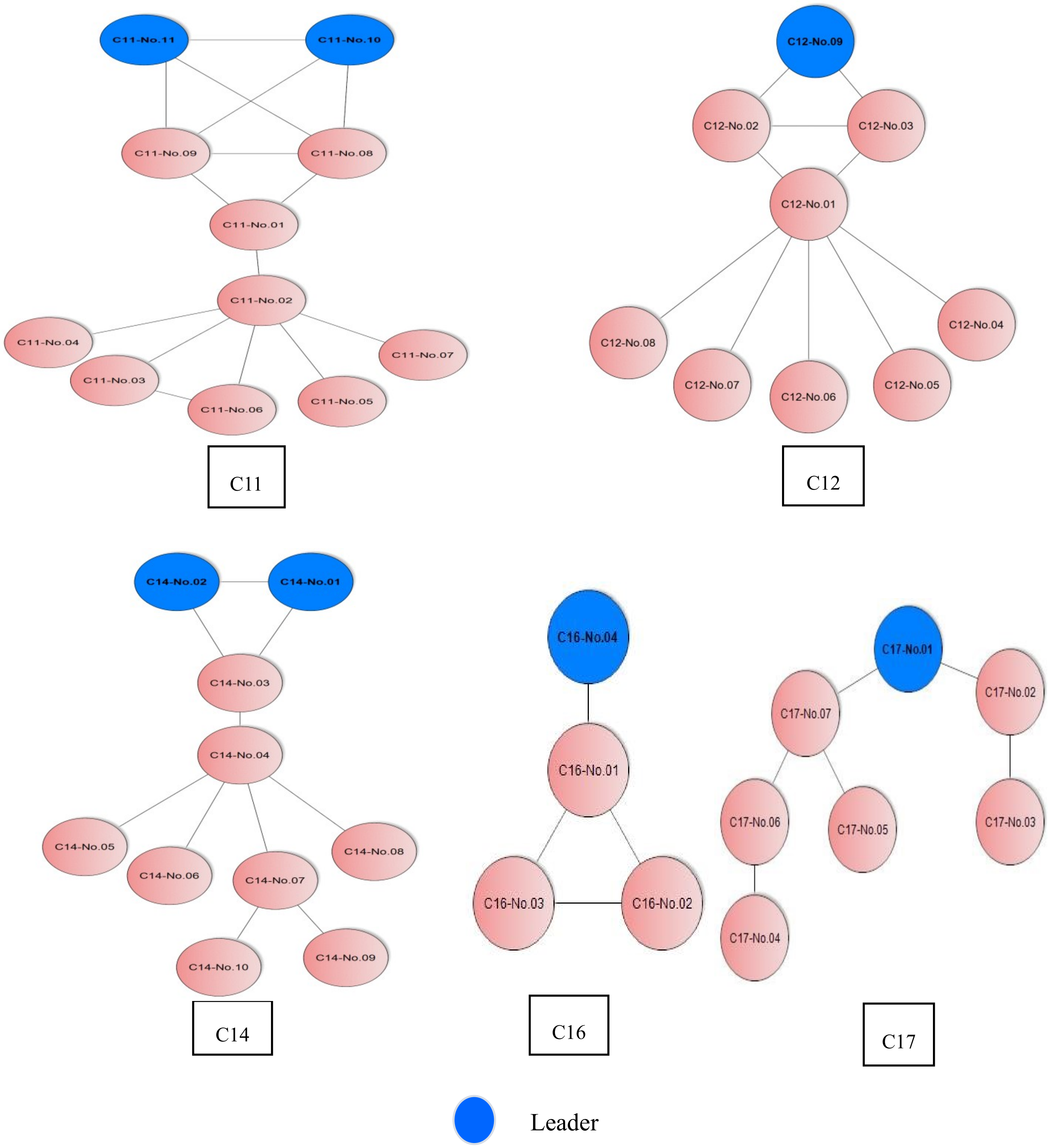
For example, the C02 network comprised of 42 fraudulent callers divided into three subgroups. Like traditional crime, physical presence and power are essential to maintain the criminal activities of these groups (Kleemans and Bunt 1999; Nurse and Bada 2018). The members of each subgroup worked and lived together at an isolated location under the management of a leader. There might have been direct social interaction between the members of each caller subgroup in one place. However, the leaders, C02-No.01 (BC = 567), C02-No.20 (BC = 292), and C02-No.29 (BC = 442), maintained connections among members (BC = 0) in order to implement fraudulent calls. Adopting a company model, the followers in the C02 network were recruited from Mainland China and Taiwan. After entering Vietnam, the core leader collected their passports in order to control their activities. Members received their passports and salaries upon leaving Vietnam. The operation of Korean caller group was less professional than the Chinese and Taiwanese networks, wherein, only a small group with few members implemented fraudulent calls. As investigator I09 of C15 shared, "Two Korean offenders hired five other Korean callers to establish a transnational fraud network in Vietnam. There were only seven core members working together at a hotel under the management of two leaders" (Interview #9).

Scholars suggest that money mules constitute the main bottleneck of criminal networks (Tropina 2012). C02, C15, and C18 involved another group known as money mules, who lived in Mainland China, Taiwan, and Korea. While Vietnamese police were unable to identify the foreign money mule networks, the country's LEAs were successful in bringing some Vietnamese money mule networks to justice. Figure 6.10 illustrates the structure of money mule groups. These groups were responsible for opening bank accounts and receiving the money illegally obtained from Vietnamese victims. The graph metrics of all five money mule networks indicate that the interactions between the members of these networks were typically better than those of the caller networks.

Chinese or Taiwanese culprits directed all five money mule networks via Vietnamese recruiters. According to investigator I04, "It is a marked concern for us to investigate instances of transnational fraud where most core criminals are foreigners because international cooperation in policing from both sides lacks frequent updates and effective collaboration" (Interview #4). For example, in C14, money mules were deployed by two Vietnamese recruiters (C14-No.03 and C14-No.04). Meanwhile, two Taiwanese culprits (C14-No.01 and C14-No.02), who served as principal architects, avoided detection, while directly orchestrating the operation of the money mule's activities.

The recruitment process began with Chinese or Taiwanese leaders employing enablers responsible for finding money mules. In all five of the sampled money mule groups, the leaders lived in Mainland China or Taiwan. They contacted enablers online using tools like WeChat and Facebook, often using these Internet communication methods to direct the recruiters responsible for finding Vietnamese money mules. The network of money mules thus, developed from real relationships between recruiters and money mules. This demonstrates that small cybercriminal networks centered on friends and relatives are essential elements of money mule networks (Broadhurst et al. 2014).

Figure 6.10. Structures of money mule networks

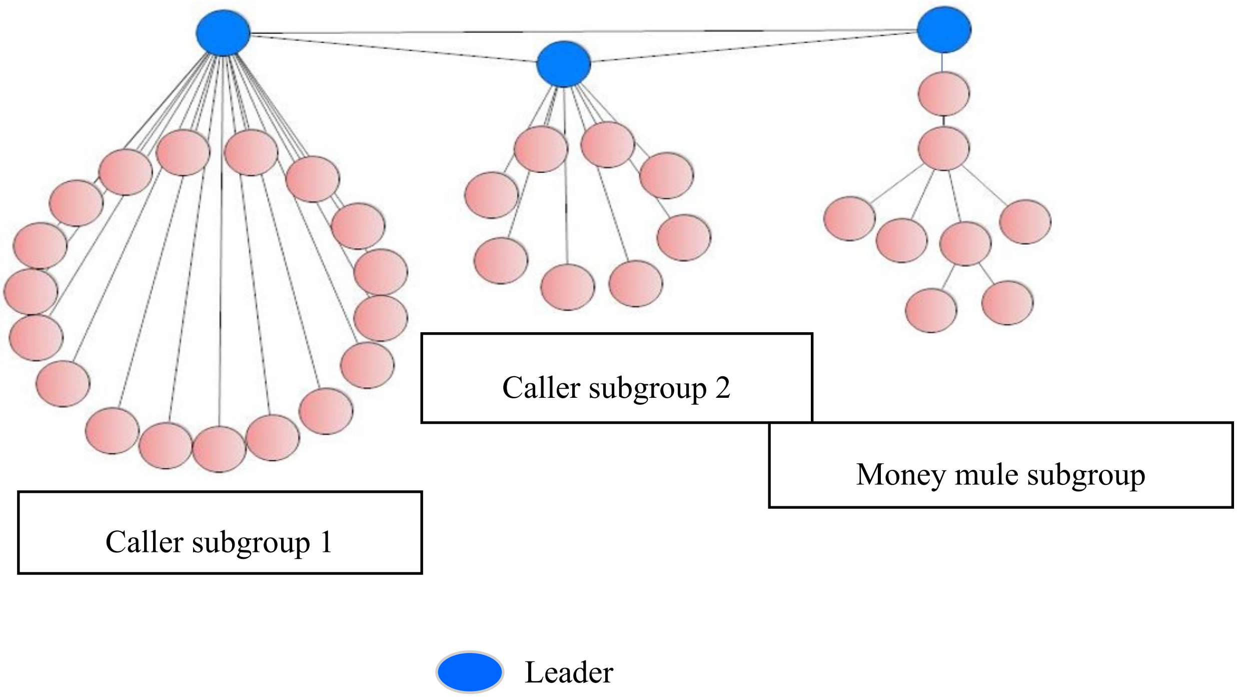


For example, the four recruiters in C11 (C11-No.01, C11-No.02, C11-No.08, and C11-No.09) were co-workers. The relationship between the recruiter (C11-No.02) and money mules could be one of friendship, family relation, or romance. Similarly, in other cases of money mule groups, Vietnamese recruiters developed a network of money mules based on genuine social or kin relationships. As in traditional offline criminal networks, existing social relationships probably serve as a foundation for criminal associations (Kleemans and Bunt 1999).

While the most central actor of caller groups was the boss, money mule networks often centered around recruiters. As the intermediaries of the entire network, recruiters played a vital role in connecting money mules to bosses. Moreover, within the scope of the operative investigation's process, these recruiters helped LEAs identify core leaders; however, it was difficult to arrest these leaders. According to investigator I11 of the Vinhphuc provincial police station, "To stir the grass and startle the snake, when LEAs had just arrested them [recruiters] in the initial operation, their big bosses [core leaders] escaped without a trace. We are unhappy because we cannot catch up with these big fishes!" (Interview ≠11). In all the five money mule networks, the Vietnamese police only succeeded in arresting money mules and a few recruiters, with the leaders evading justice.

As Figure 6.11 shows, although the sample cases did not reflect the entire phone scam network, combining the money mule (C11, C12, C14, C16, C17) and caller (C02, C15, C18) groups provided a comprehensive picture of decentralized phone scam networks. Based on the examined criminal profiles, the whole network of phone scams was often managed by a subgroup of leaders, with each leader responsible for managing one subset. Only the leaders knew the operational details of the whole network. Money mules only knew the real identities of the recruiters, who were under the guidance of leaders who communicated them via online

Figure 6.11. Structure of the whole phone scam network



communication methods. Fraudulent callers only knew the identifies of those with whom they lived and worked together in one place. While discussing phone scam networks, investigator I12 of the HTCP Department shared the following:

> The capacity to eradicate the whole network of phone scams is limited, as followers often only know the direct leader or the direct recruiter. Additionally, phone scam networks operate transnationally. In cases involving Chinese victims, Chinese caller groups move to Vietnam and other countries to implement fraudulent VoIP calls. In cases involving Vietnamese victims, Vietnamese caller groups also operate outside Vietnamese territory. Therefore, LEAs need to set up an international relationship with foreign partners. (Interview #12)

In all eight phone scam networks, Vietnamese police forces managed to halt the illegal activities of only one out of two groups. With respect to the foreign caller groups (C02, C15, and C18), after the Vietnamese police arrested offenders and discovered that all criminals and victims were foreign, they handed the cases over to their counterparts in the relevant countries.

6.3. Discussion

6.3.1. The structure of cybercrime networks implementing transnational computer fraud

The analysis of the two main types of TCF showed that each network probably comprises of many subgroups who are connected to each other by the central actors. In general, the members of these networks are motivated by financial gain. All current TCF cases do not reflect the dynamics of Choo and Smith's Type III and (Broadhurst et al. 2014) Type 4, with members lacking apparent ideological, political, or ethical motivations. Almost all of the four positions recommended by Leukfeldt, Lavorgna, and Kleemans (2017) appear in TCF networks. The shipping mules in online purchase networks, who support core members by receiving and transferring carded products from merchants, can be regarded as money mules in Leukfeldt, Lavorgna, and Kleemans' (2017) model. There are defined and specialized roles of members inside these TCF networks; however, the professional level of these TCF cases has not reached the degree recommended by Chabinsky (2010). Many roles clarified by Chabinsky (2010) do not exist within the sample cases; besides, most criminals here were not highly-skilled in technology, as analyzed by the previous chapter.

As in the case of McGuire's (2012) Type II group, offenders often combine both online and offline activities to obtain financial benefits in the bank card fraud and phone scam networks. The modus operandi of TCF was analyzed in detail in Chapter V. Fraudsters may conduct various scripts to defraud transnational victims. These scripts can occur both online and offline. However, each type of TCF networks has a different organizational structure. The tight extent of structure of TCF networks can depend on the degree of online and offline activities.

In bank card fraud cases, offenders use stolen bank card information to make online purchases or fake cards. Cases of fraudulent online purchases have a higher degree of online activity than those involving the making of counterfeit cards. The whole network of online purchases comprises of numerous subnetworks, with enablers and shipping mules concentrated around one core fraudster. In McGuire's (2012) typology, each subnetwork has the organizational structure of a hub group. However, the whole online purchase network is structured in accordance to the model of clustered hybrids or extended hybrids. Core actors cooperate in exchanging bank card data, hacking tools, and shipping mules. The whole network comprises of a group of core members surrounded by many auxiliaries, whose sole purpose being the obtaining of money illegally.

However, the leadership role of core actors within the online purchase networks is seldom clear. First, the leadership position often takes the form of a flat structure, in which, one actor hires other core members to order products and shipping mules to transfer illegal products. There is a lack of a clear hierarchical command and control within the structure of online purchase networks, a characteristic of "distributed" or "disorganized" networks, in which, members collude with one another via "assemblage" (Wall 2015). Second, the leadership position can change seamlessly. While a subnetwork can comprise of a single actor as the core member, the other subnetworks can involve that actor who provides other members with illegal services, such as consuming carded products or supplying stolen bank card data, by becoming the enabler. It is to say that just one member can hold many positions. Based on criminal policy, for example in Vietnam, member positions can be evaluated as mitigating or aggregating factors, making it essential that LEAs identify each member's position within a computer fraud network very carefully.

Relationships within online purchase networks are typically loose, with offline interaction seldom occurring in these networks. Like the physical locations of traditional offenders, virtual forums become "offender convergence settings," wherein computer fraudsters can exchange information and hacking tools, as well as establishing a relationship with others in developing fraud networks (Soudijn and Zegers 2012). Network members often use forums, email, and chat rooms to communicate. Core actors distribute financial benefits via digital money transfer services. However, in the sample cases, the C04 network was organized like a business model with a close structure, the boss leading other employees to earn profits by purchasing stolen card data. As such, cybercriminals can adapt their operations by applying the business models of legitimate companies (Tropina 2012).

According to McGuire's (2012) typology, hacking forums like *vefamily.com* and *vietexpert.info* get link to the online fraud exhibit features of a swarm or hierarchy group based on the development stage. In the first stage, online hacking forums have many of the characteristics of a swarm group, which fit with McGuire's (2012) Type I group. Cyber offenders and potential criminals are free to gather online to exchange information, buy and sell stolen bank card data, and share hacking tools. Such characteristics make these hacking forums similar to decentralized Chinese sites like open public message forums, Tencent QQ, and Baidu Tieba (Yip 2011). However, when hacking forums hold a broad membership, the organizational structure adapts to the new situation. Members can be granted, rewarded or punished by an administrative board by employing an unambiguous ranking. At this stage, hacking forums here bear hierarchical features that are often described as the characteristics of traditional criminal groups (Soudijn and Zegers 2012; Yip 2011).

Networks making fake cards have a higher degree of offline activities and a more apparent leadership structure than online purchase networks. Offline meetings and real relationships between members result in a tighter network structure in comparison to online purchase networks. With respect to McGuire's (2012) typology, networks making fake cards appear to fit the hubs or cluster hybrid structures, as smaller groups tend to involve somewhat closer social relationships between members. There often is a central actor surrounded by other actors. The primary actor retains the position of a core member or recruited enabler.

In comparison to the bank card fraud networks, phone scam networks share more similarities with traditional criminals. Offenders conduct fraudulent calls to victims by applying technology to set up VoIP call systems, which enable fraudsters to call victims from other countries with fake telephone numbers. With respect to Choo and Smith's (2008) typology, bank card fraud networks are akin to traditional organized criminal groups who use technology to enhance their fraudulent activities.

Under a subgroup of leaders, each phone scam network consists of two main groups, namely, callers and money mules, who possess different structures. A caller group comprises of centralized subgroups, with members staying together in an isolated place. Caller groups have a unique business model. Each subgroup is led by a boss who maintains the connection with other subgroups in the whole phone scam network. Therefore, each separate caller subgroup possesses the organizational features of hub groups. The merging of all separate caller subgroups produces an entire caller group that bears the characteristics of clustered hybrids.

Both phone scam and fake card networks involve the recruitment of money mules via their offline relationships with recruiters. Similar to the cybercrime networks with a low degree of technology use described by Leukfeldt, Lavorgna, and Kleemans (2014), the recruitment of members is based on real-world social ties, rather than on virtual forums. In contrast, cybercrime networks analyzed by Soudijn and Zegers (2012) recruit money mules online via hacking forums. In TCF networks, online recruitment is common in fraudulent online purchase networks. Moreover, in phone scam networks, the first acquaintance between the leaders and the enablers responsible for recruiting money mules also occurs online.

The structure of money mule groups in phone scam networks differs from that of caller groups. Money mule groups also share some features of hub groups. Money mules often gather around recruiters, who serve to break the direct connection between money mules, bosses, and other core members. The money mules only know the identity of recruiters. In contrast, in the hub model of caller groups, the central point is held by bosses, who constitute the core members. In this scenario, there is a high possibility of caller group members knowing the identity of their bosses. The merging of two main groups of callers and money mules has resulted in the whole phone scam network having the structure of cluster hybrids.

6.3.2. A new typology of cybercrime networks based on the degree of leadership

As such, the nature of TCF networks' structure proves that cybercrime networks tend to be fluid and have dynamic structures. Certain characteristics of traditional criminal organizations such as real-world social ties or trust possibly still exist inside cybercrime networks; however, technological factors make them distinctive. This finding clearly shows the transformation of cybercrime networks. Besides, McGuire's (2012) typology does not fit well the cases of TCF when comparing the relationships between the modus operandi of crime and the organizational structures. For example, in the first type recommended by McGuire, cybercrime networks that operate mainly online include swarm and hub groups. However, the current research's findings have proved that online hacking forums can possess swarm structure at the newborn stage then reform into hierarchical networks at the mature stage. With the fluid and dynamic characteristics, cybercrime networks' structures can change based on the development period.

The identification of typologies is essential for understanding the nature of crime and providing implications for countermeasures (Le 2012, 2013, pp.3,4; UNODC 2002, p.33). Certain existing scholars have suggested specific typologies of cybercrime networks that can be based on members' specific roles (Chabinsky 2010; Leukfeldt, Lavorgna, and Kleemans 2017), modus operandi (Choo and Smith 2008), and relationships within criminal networks (McGuire 2012). Supplementing the knowledge of cybercrime networks' typologies, this study can divide networks into four types depending on the clear degree of leadership. This typology may aid the investigation of fraudulent networks by LEAs, particularly with regard to developing investigation hypotheses to find evidence and solve computer fraud cases. More specifically, clarifying whether a network is organized or disorganized can aid LEAs in constructing a matrix of the relationships between various members, including money mules, enablers, and core members.

The typology proposed by this study indicates that groups with a high degree of online activity are seldom organized tightly in comparison to groups with a lower degree of online activity (see Appendix 12). This study proposes a typology comprising of the following four types:

- Type I: Swarm networks operating freely without any leadership, such as Vietnamese hacking forums at the first stage of development. This type is similar to the "swarming model" suggested by Brenner (2002) and the "swarm group" identified by McGuire (2012). These swarm networks probably attract many members in a short space of time because there is no strict restriction on membership. Swarm networks may pose a significant challenge to LEAs, insofar as arresting one member may not prevent the operation of networks.

- Type II: Distributed networks with unclear leadership and high degree of online activity. Almost all of the sampled online purchase networks (C01, C03, C05, C07, C08) were distributed networks. Reflecting a flat structure, these networks have one or a few centered actors attracting many connections, but no agreed upon leader. Distributed networks have a relatively higher rate of centrality in comparison to the swarm networks.

- Type III: Single-directed networks are organized and led by one leader. Single-directed networks include one online purchase network (C04), which was constructed under the guise of a company, as well as almost all fake card networks (C06, C09, C10, C19, C20). This type of network typically comprises of small groups.

- Type IV: Group-directed networks are organized and managed by a core subgroup of leaders. This network type includes all phone scam networks, one fake card network (C13), and Vietnamese hacking forums at the mature stage.

> Group-directed networks constitute large groups, wherein a member cannot manage an activity by oneself. The core subgroup of leaders operate with their being an equal distribution of management or operate in a hierarchical structure.

The lack of clear leadership among high-online networks proves that the distinctive nature of these cybercrime networks differs from offline criminal organizations. While traditional criminal organizations like Mafias are structured under a hierarchical command in a control form (Brenner 2002; Nurse and Bada 2018; Tropina 2012; Wall 2015), these cybercrime networks operate in a flat framework with a large number of members. Members of these online cybercrime networks may never meet physically and are possibly distributed across different locations (Wall 2015). Such characteristics have implications on LEAs with regard to the prevention and investigation of cybercrime, for networks with high degree of online activity are by their very nature impossible to be eradicated (Wall 2015). Thus, counter-cybercrime strategies should focus more upon prevention methods that mitigate the effects of cybercrime on victims.

6.4. Conclusion

While there is a marked lack of empirical research on specific cybercrime networks, this study identified the structure of cybercrime networks implementing TCF. The findings developed a more comprehensive understanding of how cybercriminal networks operate. In doing so, it showed that TCF networks can operate online and offline depending on their modus operandi. Central actors can keep the role of core members or recruited enablers inside criminal networks. Networks that make fake bank cards typically possess a stable structure of hub groups or clustered hybrids. The organizational structures of the remaining networks are likely to change as networks develop. This study suggested a new typology of cybercrime networks based on the degree of leadership comprising of four types: *swarm networks, distributed networks, single-directed networks,* and *group-directed networks*. Swarm networks and distributed networks do not have a clear leadership structure and possess a high degree of online activity. In contrast, single-directed and group-directed networks operate with a clearer command structure. While the single-directed model involves one leader controlling small groups, the group-directed model emerges within big networks. These findings have significant implications and recommendations for counter-crime strategies that will be provided in the next chapter.

CHAPTER VII: RECOMMENDATIONS FOR COUNTER-CRIME STRATEGIES

7.1. Introduction

The study aims to better understand the nature of cybercrime networks by focusing on the modus operandi and structure of Vietnamese TCF networks. The research is significant for theory, policy, and practice. The knowledge about TCF networks constitutes a foundation for recommending counter-crime strategies involving international cooperation, prevention, and investigation strategies. These recommendations are expected to be beneficial for LEAs, especially Vietnamese police forces to combat TCF as well as other cybercrimes. Therefore, these counter-crime strategies should be considered within the background of cybercrime and cybercrime regulation in Vietnam presented in Chapter III. Moreover, the reasons for cybercrime in Vietnam analyzed in Chapter IV also help the researcher suggest recommendations more comprehensively. Furthermore, Chapters V and VI that clarified the modus operandi and structure of TCF networks have brought about important recommendations for counter-crime strategies. By implications, the research proved the vital role of international cooperation and prevention methods of mitigating the effects of cybercrime on victims. Accordingly, the findings of Chapter V provide a beneficial guide for situational crime prevention. In case a crime has occurred, investigation strategies should be used to clarify the case and bring offenders to justice. The findings on the nature of TCF networks examined by Chapters V and VI urge specific actions for these investigation strategies.

This chapter consists of five sections. Following the introduction, the second section discusses the suggestions for international cooperation policy against cybercrime. Then, the third section presents the applications of situational crime prevention from the research's findings. Subsequently, the fourth section focuses on exploiting vulnerabilities within TCF networks for investigation strategies before the chapter concludes significant contents.

7.2. The role of international cooperation in combating cybercrime

The transnationality of computer fraud networks proves that international cooperation is crucial to counter-cybercrime strategies. Chinese, Taiwanese, and Korean fraudsters migrate to Vietnam, then establish transnational phone scam networks. Vietnam could be regarded as an operational base for them to make fraudulent calls back to their countries through VoIP calling systems. In such cases, fraudsters use the ICT infrastructure of Vietnam to conduct transnational scam calls. Vietnam does not receive any harm in these cases. All fraudsters and victims are foreign. If Vietnamese LEAs are unable or unwilling to cooperate with foreign counterparts, foreign LEAs will be much difficult to arrest and prosecute phone scammers.

Besides, in phone scams involving Vietnamese victims, fraudulent calls originate outside Vietnam under the direction of Chinese or Taiwanese leaders. Without the support of foreign LEAs, it seems impossible to bring core members of these networks to justice. In the sample cases, Vietnamese LEAs were successful in arresting money mule groups but failed to trace caller groups and leaders. In such cases, there was a lack of information about international cooperation between Vietnamese police and counterparts. It is clear that the disruption of the whole network requires the willingness of all relevant countries, including victims' countries and operational bases' countries. The fight against transnational phone scams surely will meet more obstacles if scammers move their operational bases to countries that lack cooperation with victims' countries.

In cases of bank card data fraud, most individual victims are foreigners. Vietnamese hackers do not need to cross geographic boundaries to defraud foreign victims. Due to cyberspace and ICT, Vietnamese cybercriminals can easily obtain and turn foreigners' bank card data into financial benefits. The physical distance between cybercriminals and victims disappears in cyberspace (Scholte 2005). Cybercriminals may avoid countries with strong cyber legislation and choose developing countries to commit transnational cybercrime. As a result, many developing countries can be regarded as hubs, or even "safe havens" for cybercrime (Gercke 2012, p.78). Vietnam is listed as one of the emerging cybercrime centers along with other countries, including India, Brazil, and North Korea (CSIS and McAfee 2018). Therefore, the international community's consensus is vital for eradicating TCF and other cybercrimes.

However, the lack of mutual understanding is one of the main factors affecting cross-border cooperation against cybercrime (United Nations 2019; UNODC 2013). This issue can result from a conflict of interests or unwillingness to cooperate among countries. As presented in Chapters V and VI, in three cases C02, C05, C18, all phone scammers and victims were foreign. C02, C18 included Chinese, Taiwanese offenders and victims; while C05 involved Korean suspects and victims. Vietnam's territory was used by foreign fraudsters to defraud foreign victims via VoIP calls. Logically, there was an argument for an appropriate approach to jurisdiction between related parties. These examples can prove that international cooperation can meet obstacles as the topic of transnational crime may be politicized and lead to tensions between countries (Caparini and Marenin 2006; Council on Foreign Relations 2013; Finlay 2012).

In fact, the cases C02 and C18 had a strong tension about jurisdiction between Vietnam, Mainland China, and Taiwan. Under the "territoriality principle," these two cases could be processed within the jurisdiction of Vietnam, where main criminal activities happened. The "protective principle" and "effects principle" could also be applied as victims were Chinese. At last, Vietnam decided to transfer Chinese criminals over to Chinese counterparts while Taiwanese criminals were handled to Taiwanese counterparts. Vietnam officially recognizes the "one China" policy with only the People's Republic of China; Vietnam-Taiwan relations are maintained at an unofficial level. Furthermore, Vietnam was not harmed in these cases as all criminals and victims were foreign. After a close dialogue between related partners, the last decision was based on the "national principle" in which Chinese and Taiwanese criminals were transferred to the respective counterparts. Although this approach causes an ongoing dispute, especially as the LEAs of Mainland China would like to solve the cases under their jurisdiction, it possibly is useful for the application in future cases. Further research should be implemented to clarify and evaluate the issue in detail.

As explained in Chapter III, international cooperation is one of the primary contents of Vietnamese cybersecurity policies. At the governmental level, the Vietnamese Government has signed many bilateral and multilateral instruments (Vietnam Ministry of Foreign Affairs 2017). Under the Government's direction, the Ministry of Public Security has established international cooperation with many counterparts (HTCP Department 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017). The contents of international cooperation can be various: the exchange of information and experiences in combating cybercrime; mutual legal assistance; education and research; finance, equipment, and tools of fighting cybercrime (Nghia and Binh 2014). Furthering international cooperation is essential for effective counter-cybercrime strategies.

As one characteristic of swarm or distributed networks, cybercriminals and victims can be scattered worldwide (Brenner 2002; Wall 2015). The analysis of TCF modus operandi, however, proves that cybercriminals and victims concerning Vietnamese cases can be centered around several "hotspot" countries. While phone scams and fake card cases are relevant to some Asian countries (Mainland China, Taiwan, and Korea), online purchase cases involve foreign culprits and victims from North America (the US) and Europe (such as the UK). As LEA's resources are limited, international cooperation against cybercrime should be more targeted. The identification of "hotspot" countries contributes to the greatest value of international cooperation activities (Lusthaus 2020, p.3).

Deeper relationships should be built between Vietnamese cyber police forces and LEAs of the "hotspot" countries. These relationships should exist in both individual cases and macro-level programs. Constructing enduring relationships is significant (Lusthaus 2020, p.3). Besides the present communication channels such as the INTERPOL 24/7 network, the G8 24/7 network, the Vietnamese Ministry of Public Security should consider establishing direct contact points with the "hotspot" countries. Using liaison officers can be one of the most effective ways of building enduring relationships (Lusthaus 2020, p.3). The presence of liaison officers can improve investigation partnerships and enhance trusted relationships between Vietnamese LEAs and counterparts.

Furthermore, after one decade of foundation, Vietnamese HTCP have still faced challenges concerning technical snags, financial problems, and human resources (HTCP Department 2017). These challenges are regarded as one factor affecting cybercrime prevention and investigation negatively, as analyzed in Chapter IV. When cyber police resources are limited, they may logically prioritize cases involving domestic victims rather than foreign ones. Therefore, countries with a strong history of counter-cybercrime strategies should support Vietnam to improve law enforcement capacity via training programs. Besides the advantage of sharing experiences, training programs can contribute to building more enduring relationships between Vietnamese cyber police and counterparts.

To sum up, the transnational characteristics of cybercrime show that international cooperation should be a crucial content of counter-cybercrime policies. However, the effectiveness of international cooperation can be impacted by the lack of mutual understanding between related partners. Therefore, Vietnamese LEAs should overcome the obstacles concerning conflicts of interests or unwillingness of cooperation. Mutual understanding among countries is a requirement for eradicating transnational cybercrime and bringing cybercriminals to justice. The clarification of "hotspot" countries and enduring relationships can enable LEAs to effectively conduct cooperation policies against cybercrime. The next section will provide recommendations for prevention strategies.

7.3. Prevention strategies

Research findings presented in Chapter V have important implications for prevention measures. The power of crime script analysis is the ability to examine crime as a process, and second, design situational prevention at each stage of the crime (Dehghanniri and Borrion 2019). Moreover, under RAT, potential recommendations for situational prevention can be summarized via the crime triangle suggested by Clarke and Eck (2016). The problem triangle includes three elements (offenders, targets/victims, and places) under the supervision of "controllers." Furthermore, Chapter IV has argued that under the expansion of ICT leading to more meetings of like offenders and suitable targets, it is imperative to use capable guardians to prevent cybercrime. Guardians or "controllers" possibly become an effective "shield" against cybercrime. As explained in Chapter III, cyber police play a central role in implementing the cybersecurity policy in Vietnam. Besides, the fight against cybercrime requires the joint liability of all organizations and individuals. Therefore, adapted from Clarke and Eck's (2016) suggestion, specific "controllers" can consist of cyber police, all individuals, and organizations in the Vietnamese context.

Research findings presented in Chapter V show that cybercriminals can conduct various methods to defraud victims. The modus operandi of TCF can be illustrated via three main stages (preparation, activity, and post-activity) in which fraudsters conduct many scripted actions to obtain money from victims' bank cards. Under the crime triangle, "controllers" should supervise behaviors relating to offenders, targets/victims, and places to reduce and prevent the chance of crime occurrence. Further research should be conducted to analyze the cost-effectiveness of particular prevention strategies; however, this study's findings can bring about the following prevention methods against bank card data fraud (see Table 7.1). The gaps inside the table mean that the analysis cannot bring about sufficient information for preventive measures.

Table 7.1. Potential prevention points for bank card data fraud

Script stages	Offender	Target/victim	Place
1. Preparation * Source bank card data		*Cardholders:* Be wary of suspicious devices attached to ATMs; be cautious about using bank card data for online payment (especially on e-commerce websites managed by small companies). *Ecommerce companies:* Enhance security for e-commerce websites (detect and fix errors like SQL Injection).	*Banks:* Enhance security for ATMs (avoid putting ATMs in deserted areas, use CCTV cameras for surveillance). *Cyber police:* Shut down hacking forums; impede the normal functionality of hacking forums.
* Recruit money mules and other members	*Cyber police:* Raise citizens' awareness to prevent the recruitment of members; use undercover money mules. *Banks:* Be cautious about managing POS terminals.		

* Prepare tools			*Cyber police:* Shut down hacking forums; impede the normal functionality of hacking forums.
2. Activity * Online purchases		*Cardholders:* Register for receiving bank alerts; act fast to inform banks and card organizations about unauthorized transactions. *E-commerce companies:* Increase defenses against suspicious orders (detect signals of fraudulent transactions).	
* Counterfeit cards		*Cardholders:* Register for receiving bank alerts; act fast to inform banks and card organizations about unauthorized transactions. *Banks:* Enhance security for ATMs; consider limiting transaction time (avoid midnight); apply technical solutions for detecting suspicious transactions.	
3. Post-activity * Flee	*Cyber police:* Prevent fraudsters (especially members of making fake cards) from fleeing immediately.		

Table 7.1 presents all possible intervention points. Some mentioned methods can be straightforward. For example, cardholders should be cautious when withdrawing cash at ATMs or using bank cards for online payment. This strategy seems obvious, and maybe it seldom needs a comprehensive study to make such a recommendation. However, the findings of this study have explained detailed reasons for these obvious suggestions. Moreover, this study also clarifies TCF networks' other vulnerabilities that LEAs can exploit. As explained in Chapter III, crime prevention strategies can be divided into broad and narrow levels. This chapter has focused on some particular points concerning the direct duty of LEAs at the narrow level.

More particularly, hacking forums are one of the vulnerabilities of TCF networks. As analyzed in Chapter V and VI, hacking forums are virtual places or "convergence settings," wherein fraudsters can exchange information and hacking tools, as well as establishing a relationship with others in developing fraud networks (Holt and Lampke 2010; Holt 2013;

Leukfeldt 2014; Soudijn and Zegers 2012). Therefore, cyber police should close down[45] these virtual forums. The closure would impair criminal networks' abilities (Ayling 2009). However, the elimination of hacking forums is not simple (Soudijn and Zegers 2012). Hacking forums' servers are often placed in other countries or moved about regularly (Soudijn and Zegers 2012). The closure of hacking forums often requires international cooperation between LEAs. Whereas the collaboration can meet obstacles if the requested countries are unable or unwilling to conduct the coordination (Al Hait 2014; Maillart 2019), or regulations are inadequate or incompatible in one of these countries (Clough 2014; Maillart 2019; Singh and Singh 2007).

In practice, as presented in Chapters IV, V, and VI, Vietnamese HTCP managed to cooperate with counterparts to disable some infamous carding forums such as *vefamily, mattfeuter, vietexpert,* and *hkvfamily.* All these forums were shut down after 2010. For example, the closure of *vefamily* carding forum resulted from the unprecedented collaboration between three countries: Vietnam, the US, and the UK. It lasted from August 2009 to May 2013. As analyzed in Chapters III, IV, before 2010, the behavior of uploading and sharing bank card information was not regulated strictly under the Vietnamese legislation. Since 2010, the Vietnamese Penal Code has updated such behaviors as crimes; therefore, Vietnamese LEAs have a legal foundation to combat hacking forums. Cracking down these forums destroyed the places where demand and supply could meet. This action can prevent further computer fraud. The success of Vietnamese cyber police proves that despite being difficult, the elimination of hacking forums is not an impossible mission.

Another solution is to impede the normal functionality of hacking forums. Blocking[46] access to these websites can be implemented (McNamee and Coordinator 2010). Logically, the admins of websites can move website contents to new servers and addresses; however, the blocking solution can impact members' normal entry (McNamee and Coordinator 2010). This solution possibly is suitable for being applied in the Vietnamese context. Cyber police play a central role, while all organizations and individuals must have a joint liability in ensuring cybersecurity. Cyber police can coordinate with Internet service providers to conduct the blocking solution in preventing cybercrime.

[45] Close-down (or deletion, elimination) of illegal forums involves removing them from the Internet; users cannot access these websites anymore (McNamee and Coordinator 2010).

[46] Blocking is the method of leaving illegal forums exist but making access more difficult (McNamee and Coordinator 2010).

Besides the blocking solution, LEAs can exploit the trust factor to interfere with the operation of forums. Trust is a significant element to maintain the relationship between members within a criminal network (Leukfeldt, Lavorgna, and Kleemans 2017; Lusthaus and Varese 2017; von Lampe 2003, p.11; von Lampe and Ole Johansen 2004). Therefore, mistrust can reduce the value of carding forums. Soudijn and Zegers (2012) proposed two ways of impeding the trust among cybercriminals, namely using a sybil attack and a slander attack. Both ways use various identities to interfere with the status system of hacking forums. The sybil attack tries to turn a low-status member into a high-status one. Whereas, in the slander attack, LEAs can target members having a trustworthy status. Undercover hackers can support LEAs to conduct these attacks. However, one potential limitation of this strategy is that it is difficult to know when mistrust is sufficient to disrupt the forums (Soudijn and Zegers 2012).

The recruitment of money mules can be another weak spot of TCF networks. Money mules are often regarded as indispensable members inside cybercriminal networks (Hao et al. 2015; Leukfeldt, Lavorgna, and Kleemans 2017; Peretti 2008; Soudijn and Zegers 2012). They are responsible for receiving, transferring illegal money or products to core members. Many of them do not recognize the criminal purpose of their activities. Hence, raising citizens' awareness can be an effective strategy to prevent the recruitment of money mules. Education can be implemented in various forms, from mass media, social media, posters, or publicity campaigns. The movement "*All citizens participate in the national security protection*" [Vietnamese: Toàn dân bảo vệ an ninh Tổ quốc] should be exploited to raise citizens' awareness against cybercrime in Vietnam. While cyber police resources are limited, the involvement of all agencies, organizations, and individuals can increase education campaigns' effectiveness.

Furthermore, undercover money mules can be recruited by LEAs to react to the advertisements for receiving and shipping products/money. Undercover money mules, of course, do not implement the instructions of core criminals. The strategy can increase the cost or risks that fraudsters cope with when committing TCF. As analyzed in Chapter IV, likely offenders can be motivated to reach their decision to commit cybercrime when estimating the benefits and risks of illegal behaviors. If they recognize that risks are much more than benefits, they will not commit the crime (Cohen and Felson 1979; Miró 2014). Consequently, using undercover money mules can lead to reducing criminals' inclination.

For preventing phone scams, some specific strategies can be applied at each crime stage (see Table 7.2). Under situational crime prevention, these strategies aim to increase risks and reduce opportunities of crime. Research findings presented in Chapter V prove that phone scammers implement scripted behaviors at each stage of crime ("preparation," "activity," and "post-activity"). "Controllers" should focus on affecting three elements (offenders, targets/victims, and places) during these stages to prevent phone scams.

Table 7.2. Potential prevention points for phone scams

Script stages	Offender	Target/victim	Place
1. Preparation * Recruit member	*Cyber police:* Raise citizens' awareness to prevent the recruitment of members. *Banks:* Be cautious about opening bank accounts for customers (criminal money mules often use fake identity cards).		
* Prepare tools and locations	*Cyber police:* Cooperate with local officials about management on residence registration.		*Cyber police:* Cooperate with local officials to detect suspicious locations (isolated places where many foreigners stay without official registrations); encourage citizens to report suspicious places to police.
2. Activity * Make fraudulent calls to victims	*Service providers:* Apply technical solutions to detect scam calls.	*Cyber police:* Raise citizens' awareness to prevent victimization. *Individuals:* Be cautious about suspicious calls (contents related to LEAs, crime, finance issues). *Banks:* Inform customers about fraud cases; notice customers' unusual behaviors (worried, anxious) (they possibly are victims).	
* Receive illegal money	*Banks:* Notice customers' unusual behaviors (they possibly are money mules); use filters to highlight unusual patterns of transactions.		
3. Post-activity * Flee	*Cyber police:* Prevent fraudsters from fleeing.		

All potential prevention opportunities for phone scams are presented in the above table. The prevention strategies require the joint liability of all individuals, banks, and service providers. In this study, the focus is on certain strategies for LEAs. Accordingly, cyber police should pay attention to raising citizens' awareness and detecting suspicious locations.

Education is a preferred method to prevent phone scams. Like bank card data fraud networks, phone scam gangs need to recruit members. This recruitment process should be disrupted by LEAs. Many money mules are unaware of the criminal truth of their activities. Furthermore, the victims of phone scams are defrauded via a series of scripted fraudulent calls. As analyzed in Chapter V, fraudulent calls are often faked to originate from LEAs or trustworthy subjects. All these calls aim to threaten or lure victims into transferring money. Individuals have become victims of crime following these fraudulent calls. Therefore, raising citizens' awareness is essential for preventing phone scams. Like prevention strategies against bank card data fraud, specific forms of education are various. Practically, Vietnamese cyber police can use mixed-form strategies. Further research should be conducted to evaluate the cost-effectiveness of these education forms.

Operational bases can be evaluated as another weakness of phone scam networks. Chapter V has proved that scam callers could live and work together at one specific location for several months without official registration. They often choose isolated houses or apartments in uncrowded neighborhoods. Additionally, scammers enhance security at these locations. All these characteristics can help LEAs deter suspicious locations that can be used for operational bases of phone scams. This strategy needs close collaboration between cyber police and local officials regarding management on residence registration. Moreover, citizens should be encouraged to report suspicious foreign groups and locations to the police.

As such, cyber police can be based on situational crime prevention to conduct a range of different strategies to reduce and deter TCF. Prevention strategies are expected to diminish the opportunities for TCF by using "controllers" to impact three factors: offenders, targets/victims, and places. Consequently, TCF does not occur, or the negative effect on victims reduces. Crime prevention is one of "the two sides of the same coin" combating cybercrime. The other side focuses on investigation strategies which will be presented as follows.

7.4. Investigation strategies

Criminal investigation is considered the process of generating and testing hypotheses to find the truth of a criminal case (Ask 2006, p.3; Greenwood et al. 1977; Nghia and Binh 2014;

Sunde 2020; Thuat 1998). The success of crime investigation constructs public confidence and strengthens citizens' respect for LEAs (UNODC 2006, p.1). However, due to the nature of cybercrime, investigating and prosecuting cybercrime meet many obstacles (Brown 2015). As explained in Chapter III, the rate of successful cybercrime disruption is very low, like the iceberg of hidden cybercrime. The findings of this study can lead to practical techniques that LEAs can apply to disrupt TCF networks.

Two decades ago, Brenner (2002) and Williams (2001a) highlighted that online crime and organizations would never reach the same level because cybercrimes often were conducted by individuals rather than organizations. However, there has been increasing evidence that the time of "lone wolf" hackers has passed (Tropina 2012). Indeed, global criminal networks have emerged as a powerful form of criminal models in the current era (Scholte 2005). Currently, only a few hackers operate solely, whereas most rely on group or organization affiliations (Goodman 2010; Ranger 2016). Moreover, technology can enable criminal networks to commit transnational cybercrime easily. While criminals are quick to adopt ICTs, LEAs seem to move relatively slowly (Goodman 2010). Traditional counter-crime strategies based on physical evidence and offline relationships of suspects may be ineffective when applied to cybercrime disruption (Goodman 2010). From understanding the nature of cybercrime networks, LEAs should design suitable countermeasures to investigate cybercrime networks.

The knowledge of the modus operandi and structure of TCF networks may help LEAs develop hypotheses to find the truth of criminal cases. Besides similarities, each type of TCF has distinguishable characteristics that can be impacted by technological factors. Regarding modus operandi, there is a strict correlation between the degree of the technology used and the interaction between suspects and victims. In terms of organizational structure, networks with a higher degree of online activity are often constructed loosely in comparison with networks with a lower degree of online activity. Furthermore, this study clarified specific scripts of crime stages, suspects' roles and relationships, criminal motivations, and other information about TCF networks. Such findings contribute to the answers to main investigation questions: how, why, where, why, and by whom cybercrime was implemented. As such, these findings can aid investigators in generating and testing hypotheses when collecting information about TCF as well as other cybercrimes.

While there is a lack of knowledge of central actors within cybercrime networks, this study clarified central actors within TCF networks. Under the SNA perspective, central actors are the vulnerable points of criminal networks (Morselli 2010; Sparrow 1991, p.264; van der Hulst 2009). In counter-crime strategies, one of the most efficient approaches is to identify central actors and target them for investigation and arrest (Sparrow 1991, pp.263-264). In networks of bank card data fraud and caller groups of phone scam networks, central actors often are the core members or even leaders of criminal networks. They are responsible for directing other members, distributing missions and benefits, or conducting the main stages of crime. Therefore, arresting them will possibly lead to the disruption of the whole network.

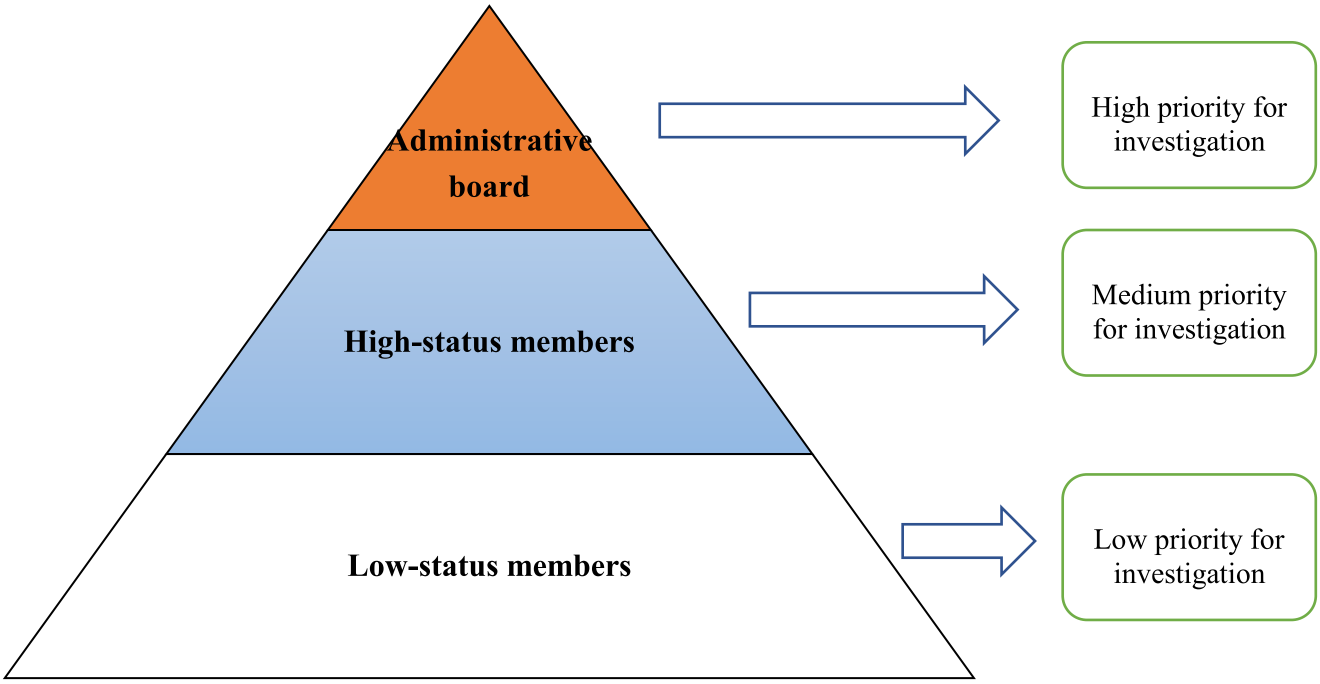
Whereas in money mule groups of phone scam networks, central actors often are the recruiters of money mules. They play the role of brokers or middle-men connecting money mules to bosses. Criminal bosses stand in the dark and direct money mule groups via the recruiters. The capture of the recruiters cannot crack down the whole phone scam networks. Criminal bosses and other core members still exist, and they immediately find other enablers who support them to recruit other money mules.

Money mule groups are evaluated as the bottleneck of criminal networks (Tropina 2012). They interrupt the financial investigation from LEAs to core members (Soudijn and Zegers 2012; Leukfeldt, Kleemans, and Stol 2017; Leukfeldt, Lavorgna, and Kleemans 2017). Therefore, arresting the recruiters cannot immediately disrupt the whole criminal network; however, LEAs are still able to investigate the hidden bosses and caller groups based on their relationships. Indeed, the investigation is complicated as the relationships between recruiters and bosses are often online. Moreover, bosses reside outside the country of recruiters and money mules. In such cases, international cooperation is essential for disrupting the whole network.

Hacking forums also should be targeted for cybercrime investigation. The disruption of hacking forums is vital for preventing cybercrime, as analyzed in the above section. Moreover, hacking forums are beneficial for investigating cybercrime as they are virtual meeting places of demand and supply (Leukfeldt 2014; Soudijn and Zegers 2012). Computer fraudsters expand criminal relationships on these carding forums. LEAs should infiltrate the hacking forums to investigate cybercriminals and their relationships.

However, it seems impossible to investigate all members of hacking forums. The number of members can reach thousands or more while cyber police resources are limited. Cyber police should prioritize their work. The priority of crime investigation should depend on the seriousness of deviant behaviors. The hierarchical structure of carding forums can be used to arrange the seriousness into three levels (see Figure 7.1). The most serious level consists of

Figure 7.1. Priority strategy for investigation, based on the structure of hacking forums


Administrative board
High-status members
Low-status members
High priority for investigation
Medium priority for investigation
Low priority for investigation

the administrative board. Arresting this group can lead to the disruption of the whole hacking forums. Even it can cause a snowball effect in which other hacking communities can be impacted. The second includes prestigious or high-status members. They are often involved directly or indirectly in many criminal behaviors. The third group comprise normal members who can be potential criminals or commit minor crimes unprofessionally.

The variations in structures within cybercrime networks cause challenges to cyber police to counter cybercrime. As discussed in Chapter VI, the structures are not the same for all the cybercrime networks; this is even for a specific cybercrime like TCF. The organizational structure of TCF networks can vary further as the networks develop. Based on the particular categories of modus operandi and development stages, TCF networks may fit various structural forms from swarm to hierarchical patterns. Hence, LEAs need to precisely identify how one cybercrime network is structured at one specific time, and then use countermeasures suitably.

This study proposes a typology of cybercrime networks based on the clear degree of leadership. The new typology includes four categories: *swarm networks, distributed networks, single-directed networks,* and *group-directed networks.* LEAs can use this typology for developing investigative hypotheses. Based on initial investigative information, LEAs can claim what kind of networks one cybercriminal group belongs to, the degree of organizational structure, central actors, the number of leaders, and the degree of relationships between members. Afterward, LEAs can choose suitable disruption strategies.

The novel typology indicates that groups with a high degree of online activity are hardly organized tightly when compared to groups with a lower degree of online activity. The flat framework of high-online networks results in obstacles in investigating and eradicating the whole network (Wall 2015). There is no clear leadership within these groups. Members can be distributed across the world and only communicate with each other online. As a result, counter-cybercrime strategies should focus more on prevention methods that reduce cybercrime consequences on victims.

However, it is not hopeless to investigate and eradicate high-online networks. This study's findings proved that unlike traditional criminal organizations such as Mafias, trust inside cybercrime networks is often not developed through offline relationships such as kinship or ethnicity. Therefore, loyalty within cybercrime networks is low (Yip et al. 2013). Cyber police can recruit undercover agents more easily. Undercover hackers can assist LEAs to infiltrate carding forums and collect information about cybercrime networks.

For single-directed networks, arresting one key leader possibly causes the disruption of the whole network (Lindquist and Zenou 2019). Whereas, for group-directed networks, LEAs should focus upon arresting the group of leaders (Borgatti 2006). In group-directed networks, when LEAs do not arrest the whole group of leaders, the unoccupied position can be replaced by another leader. These networks can adapt, transform into a new organizational form. In some situations, remaining leaders can quit the old network and establish a new one. For example, the culprit C05-No.01 was a technical administrator of *vefamily.com* forum. After *vefamily.com* was cracked down and some leaders were arrested in 2010, C05-No.01 copied its source code to design another carding forum, namely *vietexpert.info*. Therefore, arresting the whole group of leaders is necessary to disrupt these criminal networks. The eradication of group-directed networks often requires a long time and more resources in comparison with single-directed networks.

7.5. Conclusion

The fight against cybercrime is difficult but not an impossible mission. The capability of suppressing cybercriminals depends much on counter-crime strategies. The present study has significant recommendations for counter-crime strategies. Understanding cybercrime’s nature is a beneficial way of designing and applying countermeasures. First, international cooperation should be targeted and enduring with the clarification of “hotspot” countries. Second, situational prevention measures can be conducted to reduce crime opportunities. Third, various investigation strategies can be adopted to crack down cybercriminal networks. Understanding the nature of each type of criminal networks is essential for designing effective counter-crime strategies. The value of SNA is highlighted when central actors can be identified to disrupt criminal networks. In some cases, arresting central actors can cause the disintegration of the whole cybercriminal network. In other cases, although the attack on central actors possibly does not lead to the disruption of the whole network, it can assist LEAs to expand the investigation to leaders and other core members. Additionally, education, hacking forums, and trust should be exploited to prevent and investigate TCF and cybercrime. Further studies should be conducted to examine the cost-effectiveness of each strategy.

CHAPTER VIII: CONCLUSION

8.1. Introduction

This study utilized the criminal network perspective to examine TCF networks particularly in Vietnam, contributing to a more comprehensive knowledge of cybercrime networks in general. In respect of practical aspects, this research's findings provide not only better understanding of the modus operandi and structure of cybercrime but also a more effective response to cybercrime, especially TCF. Research findings about the nature of TCF networks constitute a foundation for suggesting counter-cybercrime measures, adding to the techniques of cybercrime control. In this chapter, following the introduction, the second section summarizes the significant findings in the relationship to two main research questions. Subsequently, the contributions of the research are discussed in the third section. Along with theoretical and methodological contributions, this section also focuses on practical contributions to cybercrime suppression. Then, the final section acknowledges the limitations and future research in this area.

8.2. Summary of findings

Under the circumstance of a dearth of empirical research on specific cybercrimes in the Asian context, this research analyzed TCF networks as one specific type of cybercrime networks in Vietnam. It aimed to gain objective insights into the modus operandi and structure of TCF networks. The criminal network perspective has assisted the researcher in analyzing the nature of cybercrime via interactions of suspects inside criminal organizational systems. The clarification of Vietnamese TCF case studies brought about a more comprehensive understanding of cybercrime networks in general. The significant findings proved the essential transformation of the ideas on cybercrime networks. The primary research questions have been addressed below:

8.2.1. How is transnational computer fraud implemented in the Vietnamese context?

Vietnam is both host to and victim of transnational cybercrime, especially TCF, as evidenced by the unfavorable statistics of cybercrime-related cases originating from and directed at Vietnam. Given this serious situation, perceptions surrounding cybercrime and TCF in Vietnam are increasingly significant. Against this backdrop, one main part of this study clarified methods employed by fraudsters in the Vietnamese context. Data from criminal profiles and in-depth interviews with investigators were combined, and the results showed that

Vietnam could become an operational base for both domestic and foreign criminals to implement TCF. This type of fraud, which includes crimes with only minor technological elements and those involving almost entirely technological factors, represents the intersection of fraud, transnationality, and technology. The whole process of TCF, including bank card data fraud and phone scams, was examined under crime script analysis. Accordingly, TCF's modus operandi in Vietnam possesses both similar and distinctive characteristics compared with computer fraud in other regions.

Like computer fraud clarified by other scholars such as Hardeveld et al. (2016), Meijerink (2013), Peretti (2008), Lee (2020), both types of TCF in Vietnam follow some same main steps from the pre-crime to the post-crime stage. Core fraudsters must recruit members and prepare tools to establish a transnational criminal network. Then, cybercriminals must find a way of cashing out and transferring money into benefits for core fraudsters before fleeing. This framework of committing the crime is likely popular for all types of computer fraud, in which cybercriminals cooperate on defrauding victims. However, each type of TCF in Vietnam has distinguishable characteristics.

In cases of bank card data fraud, domestic fraudsters from Vietnam can defraud foreign victims without crossing geographical boundaries. Besides, several fraudsters from China, Taiwan, and Korea migrate to Vietnam, then establish a small fraudulent network. As transient criminals, these foreign fraudsters often operate in one place for a short time, then flee immediately after obtaining the money. Phishing, which is the main method of obtaining bank card information by European and North American fraudsters (Leukfeldt, Kleemans, and Stol 2017; Peretti 2008), did not exist in the Vietnamese sample cases. In Vietnam, fraudsters can obtain bank card data via skimming technique at ATMs, SQL injection hacking, or most buying it from other hackers on hacking forums. After collecting bank card data, Vietnamese core fraudsters often use it to order products on American e-commerce websites, subsequently direct foreign shipping mules to receive and ship products from the US to Vietnam. Alternatively, bank card data can be used to clone cards to withdraw cash at ATMs or implement fake transactions via POS terminals. In contrast to networks of online purchases, networks making fake cards are often directed by foreigners (mainly Chinese).

Contributing to the literature gap on phone scams in Asia, this study analyzed the whole process of phone scams in Vietnam. This study examined the specific scripts conducted by two types of important actors: fraudulent callers and money mules under the management of foreign leaders. Migration is an important factor of phone scams (Lee 2020), as callers must cross borders to set up fraudulent caller groups. In phone scams targeting foreign victims, Vietnam can be regarded as an attractive spot for foreign fraudsters to enter and establish operational bases of transnational scam calls. Whereas, in phone scams concerning Vietnamese victims, calls originate outside Vietnam, from Mainland China or Taiwan. From operational bases outside the country of victims, caller groups conduct fraudulent calls with planned scripts via VoIP calling systems. Money mule groups located in victims' countries are responsible for receiving and transferring illegal money to criminal bosses. Like networks of making fake cards, and the Korean cases clarified by Lee (2020), Shin (2018), Chinese or Taiwanese criminals often are the architects of phone scam networks.

There is a high correlation between the degree of technology used and the interaction between culprits and individual victims. Bank card data fraud with a higher degree of technology does not require any interaction between fraudsters and victims. In contrast, phone scams are conducted with close interaction between them via VoIP calling systems. Therefore, there is no face-to-face interaction between criminals and individual victims within Vietnamese TCF cases. This finding fits with the characteristics of phishing cases in The Netherlands studied by Leukfeldt, Kleemans, and Stol (2017). As such, due to the Internet and ICTs, cybercrime can be transnational easily and conducted without direct interaction between suspects and victims. This essential transformation of cybercrime can lead to more serious consequences but more obstacles to eliminate cybercrime.

In short, by analyzing TCF into chronological stages, one important part of this thesis clarified the methods employed by TCF networks in the Vietnamese context. From providing insights into TCF's modus operandi in the Vietnamese context, the study continued to explore how TCF networks are structured, contributing to more understanding of cybercrime networks in general. Fraudsters must find an effective way to cooperate on obtaining illegal money from transnational victims. This question has been solved, as presented in the next part.

8.2.2. How are cybercrime networks structured to conduct transnational computer fraud?

The SNA approach helped the researcher identify the characteristics of the organizational structure and central actors inside TCF networks. The structure of TCF networks has many different factors compared to the nature of cybercrime networks clarified by existing research. This study's findings proved that each TCF network, especially networks of online purchases and networks of phone scams, may comprise many subgroups connecting by central actors. There is no evidence of TCF groups operating with political, ideological, or ethical motivations in the sample cases, as suggested by Choo and Smith (2008), Broadhurst et al. (2014). Members are willing to participate in TCF networks as they are motivated by financial benefits; hence, cybercriminals' relationships are often horizontal.

Computer fraudster networks often mix both online and offline activities to get financial benefits, as Type II group of cybercrimes suggested by McGuire (2012). However, the degree of online and offline activities is different, and the organizational structures of each type are dissimilar. Networks of making counterfeit bank cards have a stable structure of hub groups or clustered hybrids. The structures of the remaining networks of TCF are likely to vary based on each stage of development. For instance, in online purchase networks, each core member establishes a loose hub group. When core members cooperate to create a bigger criminal group, the new network takes on a clustered hybrid or even an extended hybrid structure. Online purchase networks lack a hierarchical command and control that is still viewed as an element of power networks (Cressey 1969; Williams 2001b). Underground forums exhibit the features of a swarm or hierarchy group in each period of development, with the hierarchical structure appearing in the mature period in virtual forums. Clustered hybrid structures of phone scam networks are constructed with the cooperation of two kinds of hub groups, namely, callers and money mules. While members of caller groups work together under a company model directed by a boss, money mules are recruited offline by enablers, thereby hiding the connection between money mules and other members.

By examining TCF networks as one specific type of cybercrime networks, the study proved that central actors could be core members or recruited enablers inside cybercrime networks. Each type of cybercrime networks can have a different structure. Moreover, on the whole, cybercrime networks tend to be fluid and possess dynamic organizational structures rather than fixed ones. The tight extent of cybercrime networks' structure can depend on the degree of online and offline activities. Especially, cybercrime networks with a high degree of online activities often operate loosely and consist of many members distributed across the world. Certain characteristics of traditional criminal organizations still can be recognized inside cybercrime networks; however, in general, there is a substantial transformation of the ideas on cybercrime. For example, cybercriminals can still adopt the business model and the hierarchical structure when their criminal networks achieve a highly-professional level of operation.

Additionally, trust that is based on offline social ties inside traditional criminal groups can be built on the foundation of ranking systems in hacking forums.

To sum up, the Internet and ICTs have transformed the nature of criminal activities. Technological factors impact much the characteristics of cybercrime networks in terms of both modus operandi and structure. There is a correlation between the extent of the technology used and the interaction between culprits and individual victims. Criminal networks with a higher degree of online activity are often constructed more loosely than networks with a lower degree of online activity. In Vietnam, cyberspace is regulated as a special territory under the principle of national sovereignty. Therefore, the findings of this study prefer viewing cybercrime as "new wine in new bottles." The characteristics of "new wine" and "new bottles" of cybercrime require the transformation of counter-crime strategies to prevent and investigate cybercrime effectively.

8.3. Contributions of research

8.3.1. Theoretical contributions

The modus operandi and structure of cybercrime networks have become a focus area within criminology and policymaking worldwide (Bossler and Berenblum 2019; Leukfeldt, Kleemans, et al. 2017; Leukfeldt, Lavorgna, et al. 2017; Ngo and Jaishankar 2017). While studies on cybercrime have concentrated in the North American and European contexts, there is a dearth of research that analyzes the modus operandi and the structure of specific cybercrimes, especially in Asia. The chapter V of this empirical study identified the specific TCF methods conducted by cybercriminal groups to defraud victims in Vietnam. Two types of TCF, including bank card data fraud and phone scams, were examined to clarify distinguishable characteristics of TCF's modus operandi in the Vietnamese context. Accordingly, there are major differences concerning the modus operandi of two types of TCF in Vietnam like transnational factors, technological factors, suspect-victim interactions, and the roles of Vietnamese and foreign suspects.

From exploring TCF's modus operandi, Chapter VI continued to identify the structure of TCF networks by examining these Vietnamese TCF case studies. The findings have contributed to a more comprehensive understanding of cybercrime networks. While central actors who are vulnerable and strategic positions inside cybercrime networks have been overlooked in existing studies, this research proved that central actors could be core members or recruited enablers. Moreover, focusing on the transformation of cybercrime, the study proved that the Internet and ICTs substantially impact the nature of cybercrime networks. Even though certain characteristics of traditional criminal organizations still are likely to exist within cybercrime networks, technological factors make them distinctive. In general, cybercrime networks tend to become fluid, and their organizational structures often are dynamic. Especially, cybercrime networks having a high-online degree often operate in a flat framework with many members. They can meet only online and be distributed across various locations, which differs from traditional criminal organizations like Mafias operating under a hierarchical command-and-control structure (Brenner 2002; Nurse and Bada 2018; Tropina 2012; Wall 2015).

Constructing criminal networks' models is an effective way to examine their nature and design counter-crime strategies (Le 2012, 2013, pp.3,4; UNODC 2002, p.33). From examining the structure of TCF networks, this study suggested a novel typology of cybercrime networks with four types depending on the clear leadership degree. Type I includes *swarm networks* operating freely without any leadership. Type II consists of *distributed networks* with unclear leadership and a high degree of online activity. Type III involves *single-directed networks* that are directed by one leader. Type IV comprises *group-directed networks* that are organized and led by a core subgroup of leaders. This typology indicates that networks with a high level of online activity are often structured loosely compared to networks with a lower degree of online activity. The transformation of cybercrime networks affects LEAs' responses to cybercrime.

8.3.2. Practical contributions

Contributing to the techniques of cybercrime reduction, the knowledge of cybercrime's characteristics helps LEAs design counter-cybercrime strategies effectively. As one valuable part of the current research, the findings explored by Chapters V and VI had some policy and practical implications concerning international cooperation, prevention, and investigation strategies against cybercrime. Accordingly, particular recommendations were suggested to increase the efficiency of the fight against cybercrime in Chapter VII. Therefore, the findings of this research might result in impacts on policy and practical decisions in combating cybercrime.

First, as one important content of counter-cybercrime policies, international cooperation should be targeted and enduring with the clarification of "hotspot" countries. This suggestion results from the transnational characteristics of cybercrime. Second, situational crime prevention can be used to impede cybercrime by reducing crime opportunities. This recommendation mainly derives from the answers to Question 1 presented in Chapter V and the combination of RAT and crime script analysis. Third, LEAs can exploit vulnerabilities, especially central actors inside cybercrime networks, to investigate and disrupt cybercrime. This proposition comes from the answers to both Questions 1 and 2 shown in Chapters V and VI. LEAs can consider applying these recommendations in practice. Moreover, this research can also assist all individuals and organizations in preventing themselves from becoming victims of computer fraud.

This empirical study's findings can be among the first step of evaluating the cost-effectiveness of counter-cybercrime strategies. The transnational characteristics of cybercrime prove that international cooperation plays a crucial role in cybercrime control. Besides, cybercrime networks possess vulnerabilities that LEAs can exploit to prevent and investigate cybercrime. Targeting central actors is an effective approach for disruption policies against TCF. This approach can be applied to other specific types of cybercrime. However, LEAs should consider carefully whether arresting central actors can lead to disrupting the whole criminal network. Moreover, the novel typology of cybercrime networks based on the leadership degree is beneficial for building investigation hypotheses against cybercrime. Additionally, LEAs can exploit education, virtual forums, and trust to increase countermeasures' effectiveness. For countermeasures against cybercrime, this study presented important strategies; however, further research should be conducted to investigate their cost-effectiveness.

8.3.3. Methodological contributions

One of the most significant contributions of this research is related to methodology. In this study, the criminal network perspective was utilized for implementing research on cybercrime. Existing studies on cybercrime networks often adopted the substantive approach that interprets networks as a distinct model of organization. This study is among the first ones utilizing the instrumental one that views networks as a set of nodes (actors) and ties (relationships). The SNA approach was used by combining both qualitative and quantitative techniques to obtain fruitful findings of TCF networks. For further research, SNA can be used to identify the nature of various cybercrimes in other contexts.

Besides SNA, the present study used the crime script analysis and RAT to explore the nature of cybercrime in the Vietnamese context. This mixture can be used to understand other cybercrimes’ networks. The clear advantage of this mixture is that the researcher could have a systematic blueprint to identify nodes with their roles and ties during sequential crime stages (Duijn and Klerks 2014; Sparrow 1991). Accordingly, a framework of research on cybercrime networks can be suggested. First, data collected from investigation files and interviews with police investigators provide rich and reliable information. Subsequently, crime script analysis can be applied to explore the modus operandi of crime before SNA is used to identify the structure of cybercrime networks.

8.4. Research limitations and future research

Although the study has contributed much to the extant literature on cybercrime networks, it is not free of limitations. First, the data were obtained through investigation files, which can be impacted by police officials' opinions and the limited capabilities of LEAs. Moreover, there was a missing data issue due to the international dimension of the networks as many foreign suspects and victims could not be identified. Limited information on some aspects of the TCF crime scripts and structure, such as recruitment of fraudulent callers, sourcing of lists of potential victims' phone numbers, and fleeing, should be clarified. Transnational dimensions should be investigated more comprehensively to understand the nature of cybercrime. In future research, it may be beneficial to interview computer fraudsters to clarify and refine these crime scripts and their relationships.

Besides, this study's findings might not be generalizable to other types of computer fraud or to other countries, as only two types of TCF—bank card data fraud and phone scams—were analyzed in the Vietnamese context. Therefore, while this research facilitates a comprehensive awareness of cybercrime networks, future studies should consider various sources, research methods, and related contexts. Future research should focus on other specific cybercrime networks as each type can have a different structure.

Furthermore, the findings of this study have policy and practical implications for counter-cybercrime strategies: international cooperation, prevention and investigation measures. Concerning the strategies' content, there is an urgent need to examine the cost-effectiveness of each strategy. Especially as international cooperation plays a crucial role in combating cybercrime, it should be investigated more. Future research should clarify international cooperation between Vietnamese cyber police and counterparts, aiming to examine the success and obstacles of international cooperation against cybercrime.

REFERENCES

Abadinsky, H. (2007). Organized crime (8th ed.). Belmont, CA: Thomson/Wadsworth.

Agee, J. (2009). Developing qualitative research questions: A reflective process. International Journal of Qualitative Studies in Education, 22(4), 431–447. https://doi.org/10.1080/09518390902736512

Ahmed, M., Sharif, L., Kabir, M., & Al-maimani, M. (2012). Human errors in information security. International Journal of Advanced Trends in Computer Science and Engineering, 1(3), 82–87. Retrieved from http://warse.org/pdfs/ijatcse01132012.pdf

Akers, R., & Sellers, C. S. (2004). Criminological theories: Introduction, evaluation, and application (4th ed.). Los Angeles: Roxbury Publishing.

Akers, R. L. (1973). Deviant behavior: A social learning approach. Belmont, CA: Wadsworth.

Al Hait, A. A. S. (2014). Jurisdiction in cybercrimes: A comparative study. Journal of Law Policy and Globalization, 22, 75–84. Retrieved from http://www.iiste.org/Journals/index.php/JLPG/article/viewFile/11050/11351

Albanese, J. (2000). The causes of organized crime: Do criminals organize around opportunities for crime or do criminal opportunities create new offenders? Journal of Contemporary Criminal Justice, 16(4), 409–423.

Albanese, J. S. (2010). Organized crime in our times (6th ed.). Burlington, MA: Anderson.

Allen, M. (2017a). Archival analysis. In The SAGE Encyclopedia of Communication Research Methods. https://doi.org/10.4135/9781483381411.n19

Allen, M. (2017b). Survey: Open-ended questions. In The SAGE Encyclopedia of Communication Research Methods. https://doi.org/10.4135/9781483381411.n608

Allen, M. (2017c). Vulnerable groups. In The SAGE Encyclopedia of Communication Research Methods. https://doi.org/10.4135/9781483381411.n673

Anh, N. N. (2011). Hoan thien che dinh hop tac quoc te trong To tung Hinh su dap ung yeu cau cai cach tu phap [Update regulations of international cooperation in criminal procedure under judicial reform]. Hanoi Procuratorate University. Retrieved from https://tks.edu.vn/thong-tin-khoa-hoc/chi-tiet/79/224

APCERT. (2019). APCERT Annual Report 2018. Retrieved from http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2018.pdf

APCERT. (2020). APCERT Annual Report 2019. Retrieved from https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2019.pdf

APCERT. (2021). APCERT Annual Report 2020. Retrieved from https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2020.pdf

Ask, K. (2006). Criminal investigation: Motivation, emotion and cognition in the processing of evidence. Göteborg University, Sweden.

Atkinson, R., & Flint, J. (2001). Accessing hidden and hard-to-reach populations: Snowball research strategies. Social Research Update, (33). Retrieved from https://sru.soc.surrey.ac.uk/SRU33.PDF

Ayling, J. (2009). Criminal organizations and resilience. International Journal of Law, Crime and Justice, 37, 182–196. https://doi.org/10.1016/j.ijlcj.2009.10.003

Babbie, E., & Mouton, J. (2001). The practice of social research. Cape Town: South Africa Oxford University Press.

Beavon, D. J. K., Brantingham, P. L., & Brantingham, P. J. (1994). The influence of street networks on the patterning of property offenses. In Clarke (Ed.), Crime Prevention Studies (pp. 115–148). Monsey, N.Y: Criminal Justice Press.

Bennett, R. R. (1991). Routine activities: A cross-national assessment of a criminological perspective. Social Forces, 70(1), 147–163. https://doi.org/https://doi.org/10.1093/sf/70.1.147

Berg, B. L. (2007). Qualitative research methods for the social sciences. London: Pearson.

Bichler, G., Christie-Merrall, J., & Sechrest, D. (2011). Examining juvenile delinquency within activity space: Building a context for offender travel patterns. Journal of Research in Crime and Delinquency, 48(3), 472–506.

Bichler, G., Malm, A., & Enriquez, J. (2014). Magnetic facilities: Identifying the convergence settings of juvenile delinquents. Crime & Delinquency, 60(7), 971–998. https://doi.org/https://doi.org/10.1177/0011128710382349

BKAV. (2016). Ma doc tan cong VNA xuat hien tai nhieu co quan, doanh nghiep [Malware attacking VNA exists at the systems of many agencies]. Retrieved June 15, 2019, from http://m.bkav.com.vn/en_GB/ho_tro_khach_hang/-/chi_tiet/400028/trang-tin-tuc?cur=8

BKAV. (2017). Tong ket an ninh mang nam 2017 va du bao xu huong 2018 [Cybersecurity summary 2017 and trend 2018]. Retrieved June 15, 2019, from https://www.bkav.com.vn/trong-ngoi-nha-bkav/-/chi_tiet/511114/tong-ket-an-ninh-mang-nam-2017-va-du-bao-xu-huong-2018

Black, P. (2013). Subcultural theories of crime. In The Encyclopedia of Criminology and Criminal Justice (pp. 1–3). https://doi.org/10.1002/9781118517383.wbeccj254

Blumer, H. (1969). Symbolic interactionism: Perspective and method. Englewood Cliffs: Prentice-Hall.

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

Borgatti, S. P. (2006). Identifying sets of key players in a social network. Computational & Mathematical Organization Theory, 12, 21–34. https://doi.org/10.1007/s10588-006-7084-x

Bossler, A. M., & Berenblum, T. (2019). Introduction: New directions in cybercrime research. Journal of Crime and Justice, 42(5), 495–499. https://doi.org/10.1080/0735648X.2019.1692426

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of Routine Activities Theory. International Journal of Cyber Criminology, 3(1), 400–420. Retrieved from http://cybercrimejournal.com/bosslerholtjan2009.htm

Botnet-tracker. (2017). Botnet statistics for the year of 2016. Retrieved June 18, 2019, from http://botnet-tracker.blogspot.com/2017/01/botnet-statistics-for-year-of-2016.html

Botnet-tracker. (2018). Botnet statistics for the year of 2017. Retrieved June 18, 2019, from https://botnet-tracker.blogspot.com/2018/02/botnet-statistics-for-year-of-2017.html

Boyatzis, R. E. (1998). Transforming qualitative information: Thematic analysis and code development. Thousand Oaks, CA: Sage.

Branigan, S. (2004). High-tech crimes revealed: cyberwar stories from the digital front. Addison-Wesley Professional.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.

Brenner, S. W. (2002). Organized cybercrime? How cyberspace may affect the structure of criminal relationships. North Carolina Journal of Law & Technology, 4(1), 1–50.

Brenner, S. W. (2007). History of computer crime. In K. De Leeuw & J. Bergstra (Eds.), The history of information security (pp. 705–721). https://doi.org/https://doi.org/10.1016/B978-044451608-4/50026-2

Broadhurst, R., & Chang, Y.-C. (2012). Cybercrime in Asia: Trends and challenges. In J. Liu, B. Hebenton, & S. Jou (Eds.), Handbook of Asian Criminology (pp. 49–63). https://doi.org/https://doi.org/10.1007/978-1-4614-5218-8_4

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. Retrieved from https://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf

Brown, C. S. D. (2015). Investigating and prosecuting cybercrime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55–119. https://doi.org/10.5281/zenodo.22387

Browning, C. R., Cagney, K. A., & Morris, K. (2014). Early Chicago School theory. In G. Bruinsma & D. Weisburd (Eds.), Encyclopedia of Criminology and Criminal Justice. https://doi.org/https://doi.org/10.1007/978-1-4614-5690-2_425

Bruinsma, G., & Bernasco, W. (2004). Criminal groups and transnational illegal markets. Crime, Law and Social Change, 41(1), 79–94.

BSA. (2018). Software management: Security imperative, business opportunity. Retrieved from https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf

Burt, R. S. (1992). Structural holes: The social structure of competition. Cambridge: Harvard University Press.

Calcara, G. (2019). Rethinking legal research on matters of international police cooperation: Issues, methods and raison d'être. Liverpool Law Review, 40(2), 95–111. https://doi.org/10.1007/s10991-019-09229-9

Calderoni, F. (2012). The structure of drug trafficking Mafias: the ‘Ndrangheta and cocaine. Crime, Law and Social Change, 58, 321–349. https://doi.org/10.1007/s10611-012-9387-9

Calderoni, F., & Piccardi, C. (2014). Uncovering the structure of criminal organizations by community analysis: The Infinito network. The Tenth International Conference on Signal-Image Technology and Internet-Based Systems (SITIS), 301–308.

Calderoni, F., & Superchi, E. (2019). The nature of organized crime leadership: Criminal leaders in meeting and wiretap networks. Crime, Law and Social Change, 72, 419–444. https://doi.org/10.1007/s10611-019-09829-6

Campana, P. (2016). Explaining criminal networks: Strategies and potential pitfalls. Methodological Innovations, 9, 1–10. https://doi.org/10.1177/2059799115622748

Campana, P., & Varese, F. (2012). Listening to the wire: Criteria and techniques for the quantitative analysis of phone intercepts. Trends in Organized Crime, 15(1), 13–30. https://doi.org/10.1007/s12117-011-9131-3

Campana, P., & Varese, F. (2013). Cooperation in criminal organizations: Kinship and violence as credible commitments. Rationality and Society, 25(3), 263–289. https://doi.org/10.1177/1043463113481202

Caparini, M., & Marenin, O. (2006). Borders and security governance: Managing borders in a globalized world. Retrieved from https://www.files.ethz.ch/isn/105336/fulltext.pdf

Carley, K. M., Lee, J.-S., & Krackhardt, D. (2001). Destabilizing networks. Connections, 24, 79–92. Retrieved from https://www.andrew.cmu.edu/user/krack/documents/pubs/2001/2001 Destabilizing Networks.pdf

Carrington, P. J. (2016). Crime and social network analysis. In J. Scott & P. J. Carrington (Eds.), The SAGE Handbook of Social Network Analysis (pp. 236–255). https://doi.org/https://dx.doi.org/10.4135/9781446294413

Chabinsky, S. R. (2010). The cyber threat: Who’s doing what to whom? Retrieved February 3, 2021, from FBi website: https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom

Chau, T. (2016). Tuyen an bang “Mattfeuter” chiem đoat 61 ty đong tu the tin dung [Sentence criminal syndicate “Mattfeuter” who appropriated 61 billion VND via credit cards].

Retrieved June 18, 2019, from https://www.tienphong.vn/phap-luat/tuyen-an-bang-mattfeuter-chiem-doat-61-ty-dong-tu-the-tin-dung-956671.tpo

Chinh, N. M. (2019, September 25). 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. Retrieved from 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#!

Choi, Kwan, Lee, J., & Chun, Y. (2017). Voice phishing fraud and its modus operandi. Security Journal, 30(2), 454–466. https://doi.org/10.1057/sj.2014.49

Choi, Kyung-shick. (2008). Computer crime victimization and integrated theory: An empirical assessment. International Journal of Cyber Criminology, 2(1), 308–333. Retrieved from https://www.cybercrimejournal.com/Choiijccjan2008.htm#_ftn1

Choo, K. R., & Smith, R. G. (2008). Criminal exploitation of online systems by organised crime groups. Asian Criminology, 3(1), 37–59. https://doi.org/10.1007/s11417-007-9035-y

Chowdappa, K. B., Lakshmi, S. S., & Kumar, P. N. V. S. P. (2014). Ethical hacking techniques with penetration testing. International Journal of Computer Science and Information Technologies, 5(3), 3389–3393. Retrieved from https://pdfs.semanticscholar.org/b33f/6d6769a72df4447d8fec556a28d85f59650d.pdf

Clark, R. S. (1982). The criminal justice system: An analytical approach. Boston, MA: Allyn & Bacon.

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. Retrieved from https://link.gale.com/apps/doc/A422445386/AONE?u=waseda&sid=AONE&xid=f83b8d9d. Accessed 13 Nov. 2020

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589

Cohen, L., Manion, L., & Morison, K. (2007). Research methods in education (6th ed.). London: Routledge.

Cooper, G., & Le, H. (2018). Vietnam' s new Cybersecurity Law: A headache in the making? Duane Morris, pp. 14–16. Retrieved from https://www.duanemorris.com/articles/static/cooper_le_cybersecurity_practitioner_0718.pdf

Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention. Crime Prevention Studies, 3, 151–196.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. International Journal of Human-Computer Studies, 58, 737–758. https://doi.org/10.1016/S1071-5819(03)00041-7

Council on Foreign Relations. (2013). The global regime for transnational crime. Retrieved January 14, 2021, from https://www.cfr.org/report/global-regime-transnational-crime

Couture, X., & Pardoe, A. (2017). Changing the story on scams. Retrieved from https://www.citizensadvice.org.uk/Global/CitizensAdvice/Consumer publications/Scams report - final.pdf

Cressey, D. R. (1969). Theft of the nation: The structure and operations of organized crime in America. New York: Harper and Row.

Creswell, J. W. (2007). Qualitative inquire & research design: Choosing among five approaches. Thousand Oaks: SAGE Publications.

Creswell, J. W. (2009). Research design: Qualitative, quantitative, and mixed methods approaches (3rd ed.). Thousand Oaks, CA: Sage Publications Inc.

Creswell, J. W., Clark, V. L. P., & Hanson, M. L. G. E. (2003). Advance mixed methods research designs. In A. Tashakkori & C. Teddlie (Eds.), Handbook of mixed methods in social & behavioral research (pp. 209–240). Thousand Oaks, CA: SAGE.

CSIS, & McAfee. (2018). Economic impact of cybercrime – No slowing down. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

Curry, G. D., & Decker, S. H. (2002). Confronting gangs: Crime and community (2nd ed.). Los Angeles, CA: Roxbury Pub Co.

Cybersecurity Ventures. (2017). 2017 cybercrime report. In Cybersecurity Ventures. Retrieved from https://internetassociation.org/wp-content/uploads/2019/09/IA_Measuring-The-US-Internet-Sector-2019.pdf

Dai, Q. T. (2015). Khong gian mang: Tuong lai va hanh dong [Cyberspace: Future and action]. Hanoi: Public Security Publishing House.

Davis, B. (2016). Hacking attack at Vietnam airports another chapter in South China Sea dispute. Retrieved June 19, 2019, from https://www.forbes.com/sites/davisbrett/2016/08/13/hacking-attack-at-vietnam-airports-another-chapter-in-south-china-sea-dispute/#4e3aa4816e35

de Bie, J. L., de Poot, C. J., & van der Leun, J. P. (2015). Shifting modus operandi of Jihadist foreign fighters from the Netherlands between 2000 and 2013: A crime script analysis. Terrorism and Political Violence, 27(3), 416–440. https://doi.org/10.1080/09546553.2015.1021038

Décary-Hétu, D., & Dupont, B. (2013). Reputation in a dark network of online criminals. Global Crime, 14(2–3), 175–196.

Décary-Hétu, David. (2014). Information exchange paths in IRC hacking chat rooms. In C. Morselli (Ed.), Crime and Networks (pp. 218–230). https://doi.org/10.4324/9781315885018-21

Decker, S. H. (1996). Collective and normative features of gang violence. Justice Quarterly, 13(2), 243–264. https://doi.org/https://doi.org/10.1080/07418829600092931

Dehghanniri, H., & Borrion, H. (2019). Crime scripting: A systematic review. European Journal of Criminology, 1–22. https://doi.org/10.1177/1477370819850943

Denzin, N., & Lincoln, Y. (1994). Handbook of qualitative research (N. Denzin & Y. Lincoln, Eds.). Thousand Oaks, CA, US: Sage Publications Inc.

Department of Cybersecurity and Counter High-tech Crime. (2018). Bao cao tong ket nam 2018 [Annual report 2018]. Hanoi.

Department of Movement of Protecting National Security. (2021). Nhin lai cong tac xay dung phong trao va viec to chuc Ngay hoi toan dan bao ve an ninh To quoc, giai doan 2015-2020 [Analysis of the movement and festival day All citizens participate in the national security protection]. Retrieved March 8, 2021, from http://phongtraoantq.gov.vn/NewsDetail.html?newsId=3122

Desnoyers, S. (2013). The challenges of cybercrime for international law enforcement. Utica College.

Dong, A. (2020, March 6). Truyen thong, an ninh mang va luat phap [Media, cybersecurity and law]. The Communist Party of Vietnam. Retrieved from https://nhandan.com.vn/binh-luan-phe-phan/truyen-thong-an-ninh-mang-va-luat-phap-579963/

Duijn, P. A. C., & Klerks, P. P. H. M. (2014). Social network analysis applied to criminal networks: Recent developments in Dutch law enforcement. In A. J. Masys (Ed.), Networks and Network Analysis for Defence and Security. Lecture Notes in Social Networks (pp. 121–159). https://doi.org/10.1007/978-3-319-04147-6_6

Dupont, B. (2014). Skills and trust: A tour inside the hard drives of computer hackers. In C. Morselli (Ed.), Crime and Networks (pp. 195–217). New York: Routledge.

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity theory approach. Crime Prevention Studies, 16, 7–39. Retrieved from https://www.academia.edu/17828081/Classifying_Common_Police_Problems_A_Routine_Activity_Theory_Approach

EUCPN. (2015). Cybercrime: A theoretical overview of the growing digital threat. In EUCPN Secretariat (eds.), EUCPN Theoretical Paper Series. Retrieved from https://eucpn.f2w.fedict.be/sites/default/files/content/download/files/theoretical_paper_cybercrime_.pdf

European Commission. (2012). Communication from the commission to the Council and the European Parliament - Tackling crime in our digital age: Establishing a European Cybercrime Center. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0140&from=EN

FBI. (2013). Leader in $200 Million International Stolen Data Ring Charged in New Jersey as Part of Worldwide Takedown. Retrieved October 21, 2020, from 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

Felson, M. (1998). Crime and everyday Life. Thousand Oaks, Calif.: Pine Forge Press.

Finckenauer, J. O. (2005). Problems of definition: What is organized crime? Trends in Organized Crime, 8(3), 63–83. https://doi.org/10.1007/s12117-005-1038-4

Finckenauer, J. O., & Waring, E. J. (1998). Russian Mafia in America: Immigration, culture, and crime. Boston: Northeastern University Press.

Finckenauer, J., & Voronin, Y. (2001). The threat of Russian organized crime. In US Department of Justice. Retrieved from https://www.hsdl.org/?view&did=471340

Finlay, B. (2012). Managing across boundaries. In C. Leuprecht, T. Hataley, & K. Nossa (Eds.), Evolving Transnational Threats and Border Security: A New Research Agenda (pp. 11–21). Ontario: Centre for International and Defence Policy, Queen's University.

Flitter, E. (2013, June 6). Global $200 million credit card hacking ring busted. Reuters. Retrieved from https://www.reuters.com/article/us-cybercrime-hacking-arrests/global-200-million-credit-card-hacking-ring-busted-idUSBRE95419G20130605

Forexbonuses. (n.d.). The world's most cashless countries. Retrieved June 24, 2019, from http://www.forexbonuses.org/cashless-countries/

Franzese, A., & Seigler, C. (2020). Symbolic interactionism. In Encyclopedia of Personality and Individual Differences (pp. 5342–5346). https://doi.org/10.1007/978-3-319-24612-3_2125

Freeman, L. C. (1978). Centrality in social networks conceptual clarification. Social Networks, 1(3), 215–239. https://doi.org/10.1016/0378-8733(78)90021-7

Freeman, L. C. (2004). The development of social network analysis: A study in the sociology of science. Canada: Empirical Press Vancouver.

Freilich, J. D., & Newman, G. R. (2017). Situational crime prevention. In Oxford Research Encyclopedia of Criminology and Criminal Justice. https://doi.org/10.1093/acrefore/9780190264079.013.3

Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime legislation EV6.pdf

Gibson, W. (1984). Neuromancer. New York: Ace Books.

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. British Dental Journal, 204, 291–295. https://doi.org/10.1038/bdj.2008.192

Giommoni, L., Aziani, A., & Berlusconi, G. (2017). How do illicit drugs move across countries? A network analysis of the heroin supply to Europe. Journal of Drug Issues, 47(2), 217–240. https://doi.org/https://doi.org/10.1177/0022042616682426

Given, L. M. (2008). Historical research. In The SAGE Encyclopedia of Qualitative Research Methods. https://doi.org/10.4135/9781412963909.n199

Glenny, M. (2018, December 6). The cyber Mafia is growing and bringing a new level of organization to digital and internet crime. Roland Berger. Retrieved from https://www.rolandberger.com/en/Insights/Publications/Cybercrime-is-becoming-the-mafia's-newest-racket.html

Goel, A. (2016). The great cyber game in South China Sea. Retrieved June 19, 2019, from https://cyware.com/news/the-great-cyber-game-in-south-china-sea-883f7f39?PageSpeed=noscript

Gogolin, G. (2010). The digital crime tsunami. Digital Investigation, 7(1–2), 3–8. https://doi.org/10.1016/j.diin.2010.07.001

Goodman, M. (2010). International dimensions of cybercrime. In S. Ghosh & E. Turrini (Eds.), Cybercrimes: A multidisciplinary analysis (pp. 311–339). https://doi.org/10.1007/978-3-642-13547-7

Google, & Temasek. (2018). e-Conomy SEA 2018: Southeast Asia's Internet economy hits an inflection point. Retrieved from https://www.thinkwithgoogle.com/_qs/documents/6730/Report_e-Conomy_SEA_2018_by_Google_Temasek_v.pdf

Gorard, S. (2020). Research design: Creating robust approaches for social sciences. https://doi.org/: https://dx.doi.org/10.4135/9781526431486

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? Social & Legal Studies, 10(2), 243–249. https://doi.org/10.1177/a017405

Granja, F. M., & Rafael, G. D. (2017). The preservation of digital evidence and its admissibility in the court. International Journal of Electronic Security and Digital Forensics, 9(1), 1–18. https://doi.org/10.1504/IJESDF.2017.081749

Gray, D. E. (2014). Doing research in the real world (Third). London: SAGE.

Greenwood, P. W., Chaiken, J. M., & Petersilia, J. (1977). The criminal investigation process. Lexington, MA: Heath.

Guille, L. (2010). Police and judicial cooperation in Europe: Bilateral versus multilateral cooperation. In F. Lemieux (Ed.), International Police Cooperation: Emerging Issues, Theory and Practice (pp. 25–41). Portland: Willan.

Hai, M. (2020). Mat tien trong tai khoan vi truy cap vao đuong link la [Lose money in bank accounts because of accessing fraudulent links]. Retrieved August 8, 2021, from Public Security News website: https://cand.com.vn/Phap-luat/Mat-tien-trong-tai-khoan-vi-truy-cap-vao-duong-link-la-i580643/

Hagan, F. (2010). Research methods in criminal justice and criminology (8th ed.). London: Prentice Hall.

Handcock, M. S., & Gile, K. J. (2011). Comment: On the concept of snowball sampling. Sociological Methodology, 41(1), 367–371. https://doi.org/10.1111/j.1467-9531.2011.01243.x

Hao, S., Borgolte, K., Nikiforakis, N., Stringhini, G., Egele, M., Eubanks, M., … Vigna, G. (2015). Drops for stuff: An analysis of reshipping mule scams. UC Santa Barbara, 1081–1092. https://doi.org/10.1145/2810103.2813620

Hirschi, T. (1969). Causes of delinquency. Berkeley: University of California Press.

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

Hobbs, D. (2002). Going down the global: The local context of organised crime. The Howard Journal of Criminal Justice, 37(4). https://doi.org/https://doi.org/10.1111/1468-2311.00109

Hogue, R. (2017). What is domain squatting and what can you do about it? Retrieved March 3, 2021, from https://www.godaddy.com/garage/what-is-domain-squatting-and-what-can-you-do-about-it/

Hollinger, R. C., & Lanza-Kaduce, L. (1988). The process of criminalization: The case of computer crime laws. Criminology, 26(1), 101–126. https://doi.org/https://doi.org/10.1111/j.1745-9125.1988.tb00834.x

Holt, Thomas J. (2013). Exploring the social organisation and structure of stolen data markets. Global Crime, 14(2–3), 155–174. https://doi.org/10.1080/17440572.2013.787925

Holt, Thomas J. (2020). Subcultural theories of crime. In The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 513–526). https://doi.org/10.1007/978-3-319-78440-3_19

Holt, Thomas J, & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. Criminal Justice Studies, 23(1), 33–50. https://doi.org/10.1080/14786011003634415

Hooton, C. (2019). Measuring the U.S. Internet sector 2019. Retrieved from https://internetassociation.org/wp-content/uploads/2019/09/IA_Measuring-The-US-Internet-Sector-2019.pdf

HSN Consultants. (2019). The Nilson report. Retrieved from https://nilsonreport.com/upload/content_promo/The_Nilson_Report_Issue_1164.pdf

HTCP Department. (2010). Bao cao tong ket nam 2010 [Annual report 2010]. Hanoi.

HTCP Department. (2011). Bao cao tong ket nam 2011 [Annual report 2011]. Hanoi.

HTCP Department. (2012). Bao cao tong ket nam 2012 [Annual report 2012]. Hanoi.

HTCP Department. (2013). Bao cao tong ket nam 2013 [Annual report 2013]. Hanoi.

HTCP Department. (2014). Bao cao tong ket nam 2014 [Annual report 2014]. Hanoi.

HTCP Department. (2015). Bao cao tong ket nam 2015 [Annual report 2015]. Hanoi.

HTCP Department. (2016). Bao cao tong ket nam 2016 [Annual report 2016]. Hanoi.

HTCP Department. (2017). Bao cao tong ket nam 2017 [Annual report 2017]. Hanoi.

Huebner, M., Vach, W., & Cessie, S. (2016). A systematic approach to initial data analysis is good research practice. The Journal of Thoracic and Cardiovascular Surgery, 1(151), 25–27. https://doi.org/10.1016/j.jtcvs.2015.09.085

Hung, G. (2018). 160 trieu tai khoan Zing ID bi lo, ngo ngang cach dat mat khau cua nguoi Viet [160 million Zing ID accounts leaked, surprised at passwords of Vietnamese users]. Retrieved June 19, 2019, from https://dantri.com.vn/suc-manh-so/160-trieu-tai-khoan-zing-id-lo-lot-mat-khau-de-chiem-rat-nhieu-20180502063917763.htm

Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. Crime, Law and Social Change, 62(1), 1–20. https://doi.org/10.1007/s10611-014-9520-z

Hutchings, Alice, & Holt, T. J. (2015). A crime script analysis of the online stolen data market. British Journal of Criminology, 55(3), 596–614. https://doi.org/10.1093/bjc/azu106

ICTNews. (2018). Mua khong dung loai phan mem diet virus, may tinh nguoi dung khong duoc bao ve hieu qua [Buying unsuitable antivirus software makes computers not to be protected effectively]. Retrieved June 18, 2019, from https://ictnews.vn/cntt/bao-mat/mua-khong-dung-loai-phan-mem-diet-virus-may-tinh-nguoi-dung-khong-duoc-bao-ve-hieu-qua-168415.ict

IMPERVA. (2008). SQL Injection 2.0. Retrieved from https://pdfs.semanticscholar.org/9e33/338f42d2d97349063cf24db36a74936f0613.pdf

International Association of Crime Analysts. (2018). Social network analysis for law enforcement. Retrieved from https://crimegunintelcenters.org/wp-content/uploads/2018/07/iacawp_2018_02_social_network_analysis.pdf

Internet World Stats. (2020). World Internet usage and population statistics. Retrieved June 6, 2020, from https://internetworldstats.com/stats.htm#links

INTERPOL. (2017). Global cybercrime strategy (summary). Retrieved from https://www.interpol.int/en/content/download/5586/file/Summary_CYBER_Strategy_2017_01_EN LR.pdf

INTERPOL. (n.d.). How INTERPOL supports Italy to tackle international crime. Retrieved January 14, 2021, from https://www.interpol.int/en/Who-we-are/Member-countries/Europe/ITALY

ISACA. (2019a). State of cybersecurity 2019, part 1: Current trends in workforce development. Retrieved from https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpsc191

ISACA. (2019b). State of cybersecurity 2019 part 2: Current trends in attacks, awareness and governance. Retrieved from https://www.isaca.org/Pages/DocumentDownloadRegistration.aspx?file=http%253a%252f%252fwww.isaca.org%252fKnowledge-

Center%252fResearch%252fDocuments%252fcyber%252fstate-of-cybersecurity-2019-part-2_res_eng_0619.pdf&ReturnUrl=%252fPages%252fFileDownload.asp

ISO. (2018). ISO/IEC 27000:2018. Retrieved March 2, 2021, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

ITU. (2018). Global Cybersecurity Index (GCI) 2017. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

ITU. (2019). Global Cybersecurity Index (GCI) 2018. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

ITU. (2021). Global Cybersecurity Index 2020: Measuring commitment to cybersecurity. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Jewkes, Y., & Yar, M. (2009). Handbook of Internet crime. https://doi.org/10.4324/9781843929338.ch3

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a definition of mixed methods research. Journal of Mixed Methods Research, 1(2), 112–133. https://doi.org/10.1177/1558689806298224

Kaspersky. (n.d.). What is a DDoS attack? DDoS meaning. Retrieved March 2, 2021, from https://www.kaspersky.com/resource-center/threats/ddos-attacks

Kaspersky. (2017). Kaspersky security bulletin: Overall statistics for 2017. Retrieved from https://media.kaspersky.com/jp/pdf/pr/Kaspersky_KSB2017_Statistics-PR-1045.pdf

Kaspersky. (2018). Kaspersky security bulletin 2018 statistics. Retrieved from https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/

Kigerl, A. (2011). Routine activity theory and the determinants of high cybercrime countries. Social Science Computer Review, 30(4), 470–486. https://doi.org/10.1177/0894439311422689

Kleemans, E. R., & Bunt, H. G. van de. (1999). The social embeddedness of organized crime. Transnational Organized Crime, 5(1), 19–36.

Klein, M. W. (1971). Street gangs and street workers. Englewood Cliffs: Prentice-Hall.

Klein, M. W., & Maxson, C. L. (2006). Street gang patterns and policies. Oxford: Oxford University Press.

Kshetri, N. (2010). The global cybercrime industry: Economic, institutional and strategic perspectives. Springer Berlin Heidelberg.

Kvale, S. (1996). InterViews: An introduction to qualitative research interviewing. Thousand Oaks, CA: SAGE.

Lam, N. V. (2020, June 2). Hop tac va dau tranh ve an ninh mang trong quan he quoc te: Co hoi, thach thuc va de xuat chinh sach doi voi Viet Nam [Cooperation and fight about cyberspace in international relations: Opportunities, challenges, and policies to Vietnam]. Vietnam Communist Party's Central Committee. Retrieved from https://www.tapchicongsan.org.vn/web/guest/the-gioi-van-de-su-kien/-/2018/816711/hop-tac-va-dau-tranh-ve-an-ninh-mang-trong-quan-he-quoc-te- co-hoi%2C-thach-thuc-va-de-xuat-chinh-sach-doi-voi-viet-nam.aspx

Lam, T. (2020, August 10). 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

Lavorgna, A. (2016). Exploring the cyber-organised crime narrative: The hunt for a new bogeyman? In P. C. van Duyne, M. Scheinost, G. A. Antonopoulos, J. Harvey, & K. von Lampe (Eds.), Narratives on Organised Crime in Europe: Criminals, Corrupters & Policy (pp. 193–219). Oisterveijk: Wolf Legal Publishers.

Lavorgna, A., & Sergi, A. (2016). Serious, therefore organized? A critique of the emerging "'cyber-organized crime'" rhetoric in the United Kingdom. International Journal of Cyber Criminology, 10(2), 170–187.

Le, V. (2012). Organized crime typologies: Structure, activities and conditions. International Journal of Criminology and Sociology, 1, 121–131.

Le, V. (2013). Understanding the operational structure of Southeast Asian drug trafficking groups in Australia. Queensland University of Technology.

Lee, C. S. (2020). A crime script analysis of transnational identity fraud: migrant offenders' use of technology in South Korea. Crime, Law and Social Change, 74(2), 201–218. https://doi.org/10.1007/s10611-020-09885-3

Leukfeldt, E., Kleemans, E., & Stol, W. P. (2017). A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. Crime, Law and Social Change, 67, 21–37. https://doi.org/10.1007/s10611-016-9662-2

Leukfeldt, E. R. (2014). Cybercrime and social ties: Phishing in Amsterdam. Trends in Organized Crime, 17(4), 231–249. https://doi.org/10.1007/s12117-014-9229-5

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. European Journal on Criminal Policy and Research, 23, 287–300. https://doi.org/10.1007/s10610-016-9332-z

Li, X. (2017). A review of motivations of illegal cyber activities. Criminology & Social Integration Journal, 25(1), 110–126. Retrieved from https://hrcak.srce.hr/file/266976

Lindquist, M. J., & Zenou, Y. (2019). Crime and networks: Ten policy lessons. Oxford Review of Economic Policy, 35(4), 746–771. https://doi.org/10.1093/oxrep/grz020

Luong, H. T. (2017). Transnational narcotics trafficking and law enforcement: A Vietnam perspective. RMIT.

Luong, H. T., Duc Phan, H., Chu, D. Van, 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

Lusthaus, J. (2012). Trust in the world of cybercrime. Global Crime, 13(2), 71–94. https://doi.org/10.1080/17440572.2012.674183

Lusthaus, J. (2020). Cybercrime in Southeast Asia: Combating a global threat locally. Retrieved from https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-05/Cybercrime in Southeast Asia.pdf?naTsKQp2jtSPYsWpSo4YmE1sVBNv_exJ

Lusthaus, J., & Varese, F. (2017). Offline and local: The hidden face of cybercrime. Policing: A Journal of Policing and Practice, 1–11. https://doi.org/10.1093/police/pax042

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

Malm, A., & Bichler, G. (2011a). Networks of collaborating criminals: Assessing the structural vulnerability of drug markets. Journal of Research in Crime and Delinquency, 48(2), 271–297. https://doi.org/10.1177/0022427810391535

Malm, A., & Bichler, G. (2011b). Networks of collaborating criminals: Assessing the structural vulnerability of drug markets. Journal of Research in Crime and Delinquency, 48(2), 271–297. https://doi.org/10.1177/0022427810391535

Malm, A. E., & Bichler, G. (2015). Why networks? In G. Bichler & A. E. Malm (Eds.), Disrupting Criminal Networks: Network Analysis in Crime Prevention edited by (pp. 1–8). Boulder, CO: Lynne Rienner Publishers, Inc.

Malm, Aili E, Kinney, J. B., & Polland, N. R. (2008). Social network and distance correlates of criminal associates involved in illicit drug production. Security Journal, 21, 77–94. https://doi.org/10.1057/palgrave.sj.8350069

Maltz, M. D. (1976). On defining “organized crime”: The development of a definition and a typology. Crime & Delinquency, 22(3), 338–346.

Mancuso, M. (2014). Not all madams have a central role: Analysis of a Nigerian sex trafficking network. Trends in Organized Crime, 17, 66–88. https://doi.org/10.1007/s12117-013-9199-z

Manyika, J., & Roxburgh, C. (2011). The great transformer: The impact of the Internet on economic growth and prosperity. In McKinsey Global Institute. Retrieved from http://www.iei.liu.se/facksprak/engelska/civilingenjorsutbildning/then18/kursmaterialarkiv/lesson-twelve/1.333650/The_great_transformer_Impact_of_Internet_on_economic_growth.pdf

Marcelline, F., & Charlie, P. (2009). E-crime prevention: An investigation of the preparation of e-commerce professionals. Journal of Internet Commerce, 8(1), 2–22.

Marsden, P. V., & Lin, N. (1982). Social structure and network analysis (1st ed.). Beverley Hills, CA: SAGE Publications, Inc.

Martinson, K., & O’Brien, C. (2015). Conducting case studies. In Handbook of Practical Program Evaluation (pp. 177–196). https://doi.org/10.1002/9781119171386.ch8

Mathers, N., Fox, N., & Hunn, A. (2007). Surveys and questionnaires. Retrieved from https://www.rds-yh.nihr.ac.uk/wp-content/uploads/2013/05/12_Surveys_and_Questionnaires_Revision_2009.pdf

McGloin, J. M. (2005). Policy and intervention considerations of a network analysis of street gangs. Criminology & Public Policy, 4(3), 607–635. https://doi.org/10.1111/j.1745-9133.2005.00306.x

McGloin, J. M., & Kirk, D. S. (2010). An overview of social network analysis. Journal of Criminal Justice Education, 21(2), 169–181. https://doi.org/10.1080/10511251003693694

McGuire, M. (2012). Organised crime in the digital age. London: John Grieve Centre for Policing and Security.

McIllwain, J. S. (1999). Organized crime: a social network approach. Crime, Law and Social Change, 32(4), 301–323.

McLeod, S. (2012). Experimental method. Retrieved March 6, 2021, from Simply Psychology website: https://www.simplypsychology.org/experimental-method.html

McNamee, J., & Coordinator, A. (2010). Internet blocking: Crimes should be punished and not hidden. Retrieved from https://www.edri.org/files/blocking_booklet.pdf

Mehrotra, K. (2019, November 22). On global cybercrime, India votes in favour of Russia-led resolution. The Indian Express. Retrieved from https://indianexpress.com/article/india/on-global-cybercrime-india-votes-in-favour-of-russia-led-resolution-6130980/

Meijerink, T. J. (2013). Carding: Crime prevention analysis. University of Twente.

Microsoft. (2015). Microsoft security intelligence, report volume 20 (July-December 2015). Retrieved from https://go.microsoft.com/fwlink/p/?linkid=2036113

Microsoft. (2016). Microsoft security intelligence report, volume 21 (January-June 2016). Retrieved from https://go.microsoft.com/fwlink/p/?linkid=2036108

Milkovich, D. (2020). 25 cyber security terms that everyone who uses a computer should know. Retrieved March 2, 2021, from https://www.cybintsolutions.com/20-cyber-security-terms-that-you-should-know/

Ministry of Public Security. (2020). Nguoi dan can nang cao canh giac truoc nhung cuoc dien thoai cua nguoi la tu xung la can bo cua cac co quan tu phap, tien hanh to tung [Citizens should be on the alert against strange calls pretending from justice officials]. Retrieved October 20, 2020, from http://bocongan.gov.vn/canh-bao-toi-pham/nguoi-dan-can-nang-cao-canh-giac-truoc-nhung-cuoc-dien-thoai-cua-nguoi-la-tu-xung-la-can-bo-cua-cac-co-quan-tu-phap-tien-hanh-to-tung-d104-t28835.html

Miró, F. (2014). Routine activity theory. In J. Mitchell Miller (Ed.), The Encyclopedia of Theoretical Criminology. https://doi.org/10.1002/9781118517390/wbetc198

Morselli, C. (2009). Inside criminal networks (C. Morselli, Ed.). New York: Spinger.

Morselli, C. (2010). Assessing vulnerable and strategic positions in a criminal network. Journal of Contemporary Criminal Justice, 26(4), 382–392. https://doi.org/10.1177/1043986210377105

Morselli, C., & Savoie-Gargiso, I. (2014). Coercion, control, and cooperation in a prostitution ring. The ANNALS of the American Academy of Political and Social Science, 653(1), 247–265. https://doi.org/10.1177/0002716214521995

Muratore, M. G. (2014). Victimization. In Encyclopedia of Quality of Life and Well-Being Research. https://doi.org/10.1007/978-94-007-0753-5_3156

Myers, M. (2009). Qualitative research in business and management. California: Sage Publications Inc.

Natarajan, M. (2006). Understanding the structure of a large heroin distribution network: A quantitative analysis of qualitative data. Journal of Quantitative Criminology, 22, 171–192. https://doi.org/10.1007/s10940-006-9007-x

Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using Routine Activities Theory to predict cyberbullying experiences. Sociological Spectrum, 32(1), 81–94. https://doi.org/10.1080/02732173.2012.628560

Newton, M. (2003). The encyclopedia of high-tech crime and crime-fighting. New York: Facts On File.

Nexusguard. (2017). DDoS threats report 2017 Q4. Retrieved from https://www.nexusguard.com/threat-report-q4-2017

Nexusguard. (2018a). DDoS threats report 2018 Q1. Retrieved from https://www.nexusguard.com/threat-report-q1-2018

Nexusguard. (2018b). DDoS threats report 2018 Q2. Retrieved from https://www.nexusguard.com/threat-report-q2-2018

Nexusguard. (2018c). DDoS threats report 2018 Q3. Retrieved from https://www.nexusguard.com/threat-report-q3-2018

Nexusguard. (2018d). DDoS threats report 2018 Q4. Retrieved from https://www.nexusguard.com/threat-report-q4-2018

Nghia, N. Q., & Binh, P. H. (2014). Nhung van de co ban ve phong, chong toi pham su dung cong nghe cao [Basic knowledge about combating high-tech crime]. Hanoi: The People's Police Academy.

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. https://doi.org/10.5281/zenodo.495762

Nguyen, T. (2016). Bo truong Truong Minh Tuan len tieng vu hacker tan cong san bay Viet Nam [Minister Truong Minh Tuan gives official speech about cyber-attacks on Vietnam airports]. Retrieved June 10, 2019, from http://thanhtra.com.vn/phap-luat/an-ninh-trat-tu/bo-truong-truong-minh-tuan-len-tieng-vu-hacker-tan-cong-san-bay-viet-nam_t114c1144n107052

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

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

Nguyen, T. Van. (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

Nurse, J. R. C., & Bada, M. (2018). The group element of cybercrime: Types, dynamics, and criminal operations. In A. Attrill-Smith, C. Fullwood, M. Keep, & D. J. Kuss (Eds.), The Oxford Handbook of Cyberpsychology (pp. 691–716). https://doi.org/10.1093/oxfordhb/9780198812746.013.36

O'Malley, J., & Marsden, P. V. (2008). The analysis of social networks. Health Services & Outcomes Research Methodology, 8(4), 222–269. https://doi.org/10.1007/s10742-008-0041-z

O'Neill, M. E. (2000). Old crimes in new bottles: Sanctioning cybercrime. George Mason Law Review, 9(2), 237–288. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/gmlr9&div=16&g_sent=1&casa_token=jdzWTewZt7IAAAAA:4e9YQcZv1qpcIGN4kyDgZubAUXdWp3KSmq3RZLWSC0ZdQmPQlltTj43VvEmrRPuhp6NVTrCVfg&collection=journals

Omotubora, A. (2019). Old wine in new bottles? Critical and comparative perspectives on identity crimes under the Nigerian Cybercrime Act 2015. African Journal of International and Comparative Law, 27(4), 609–628. Retrieved from https://www.euppublishing.com/doi/full/10.3366/ajicl.2019.0293

Otte, E., & Rousseau, R. (2002). Social network analysis: A powerful strategy, also for the information. Journal of Information Science, 28(6), 441–453. https://doi.org/https://doi.org/10.1177/016555150202800601

Padilla, F. M. (1992). The gang as an American enterprise. New Brunswick, NJ: Rutgers University Press.

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. Administration and Policy in Mental Health and Mental Health Services Research, 42, 533–544. https://doi.org/https://doi.org/10.1007/s10488-013-0528-y

Paoli, L. (2002). The paradoxes of organized crime. Crime, Law and Social Change, 37(1), 51–97. Retrieved from https://link.springer.com/article/10.1023/A:1013355122531

Paoli, L. (2004). Italian organised crime: Mafia associations and criminal enterprises. Global Crime, 6(1), 19–31. https://doi.org/10.1080/1744057042000297954

Papachristos, A. V. (2011). The coming of a networked criminology? In J. MacDonald (Ed.), Measuring Crime & Criminality (pp. 101–140). New Brunswick, NJ: Routledge.

Papachristos, A. V., Hureau, D. M., & Braga, A. A. (2013). Conflict and the corner: The impact of intergroup conflict and geographic turf on gang violence. American Sociological Review, 78(3), 417-447.

Pascale, C.-M. (2010). Symbolic interaction. In Cartographies of Knowledge: Exploring Qualitative Epistemologies (pp. 77–104). California: SAGE Publications, Inc.

Payne, B. K. (2020). Defining cybercrime. In T. J Holt & A. M. Bossler (Eds.), The Palgrave handbook of international cybercrime and cyberdeviance (pp. 3–25). https://doi.org/10.1007/978-3-319-90307-1_1-1

PCA. (2016). PCA press release: The South China Sea Arbitration (The Republic of the Philippines v. The People's Republic of China). Retrieved from https://pca-cpa.org/en/news/pca-press-release-the-south-china-sea-arbitration-the-republic-of-the-philippines-v-the-peoples-republic-of-china/

Peretti, K. (2008). Data breaches: What the underground world of carding reveals, 25 Santa Clara High Tech. Santa Clara High Technology Law Journal, 25(2), 375–413. Retrieved from http://digitalcommons.law.scu.edu/chtljhttp://digitalcommons.law.scu.edu/chtlj/vol25/iss2/4

Perez, E., & Shortell, D. (2019, March 1). North Korean-backed bank hacking on the rise, US officials say. CNN. Retrieved from https://edition.cnn.com/2019/03/01/politics/north-korea-cyberattacks-cash-bank-heists/index.html

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

Potter, G. W. (1993). Criminal organizations: Vice, racketeering, and politics in an American city. Prospect Heights, IL: Waveland Pr Inc.

Powell, W. W. (1990). Neither market nor hierarchy: Network forms of organization. Research in Organizational Behavior, 12, 295–336. Retrieved from http://www.uvm.edu/pdodds/files/papers/others/1990/powell1990a.pdf

Pratt, T. C., Holtfreter, K., & Reisig, M. (2010). Routine online activities and Internet fraud targeting: Extending the generality of Routine Activity Theory. Journal of Research in Crime and Delinquency, 47(3), 267–297. https://doi.org/10.1177/0022427810365903

Preminger, B. (2019). 23 million stolen credit cards for sale on the dark web in the first half of 2019. Retrieved June 7, 2020, from https://blog.cybersixgill.com/23million_stolen_cc_blog#

PwC. (2018). Global economic crime and fraud survey 2018: Pulling fraud out of the shadows Vietnam perspectives. Retrieved from https://www.pwc.com/vn/en/publications/2018/pwc-gecs-2018-vietnam-en.pdf

Qin, J., Xu, J. J., Hu, D., Sageman, M., & Chen, H. (2005). Analyzing terrorist networks: A case study of the global Salafi Jihad network. Intelligence and Security Informatics. ISI 2005. Lecture Notes in Computer Science. https://doi.org/10.1007/11427995_24

Quang, D. N. (1999). Giao trinh toi pham hoc [Criminology]. Hanoi: Vietnam National University Press.

Quangbinh Provincial Police Station. (2021). Trien khai chuong trinh cong tac xay dung phong trao toan dan bao ve an ninh To quoc [Deploy the program of constructing the Movement "All citizens participate in the national security protection"]. Retrieved March 8, 2021, from https://conganquangbinh.gov.vn/trien-khai-chuong-trinh-cong-tac-xay-dung-phong-trao-toan-dan-bao-ve-an-ninh-to-quoc/

Quyen, H. T. (2020, November 16). Bao ve chu quyen quoc gia tren khong gian mang trong thoi dai cong nghe so [Protect national sovereignty in cyberspace in the digital age]. Ho Chi Minh National Academy of Politics. Retrieved from https://hcma.vn/vanban/Pages/van-ban-quan-ly.aspx?ItemId=30799&CateID=0

Ranger, S. (2016, July 5). Cybercrime kingpins are winning the online security arms race. ZDNet. Retrieved from https://www.zdnet.com/article/cybercrime-kingpins-are-winning-the-online-security-arms-race/

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. Journal of Research in Crime and Delinquency, 50(2), 216–238. https://doi.org/10.1177/0022427811425539

Richardson, R. (2008). 2008 CSI computer crime & security survey. Retrieved from http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall10/CSIsurvey2008.pdf

Robson, C., & McCartan, K. (2016). Real world research: a resource for users of social research methods in applied settings (4th ed.; C. Robson & K. McCartan, Eds.). London: Wiley.

Rubin, H. J., & Rubin, I. S. (2012). Qualitative interviewing: The art of hearing data (3rd ed.). Thousand Oaks, CA: SAGE Publications, Ltd.

Rush, H., Smith, C., Kraemer, E., & Tang, P. (2009). Crime online: Cybercrime and illegal innovation.

Sageman, M. (2004). Understanding terror networks. Philadelphia: University of Pennsylvania Press.

Sands, G. (2016). What to know about the worldwide hacker group "Anonymous." ABCnews. Retrieved from https://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302

SaveNET. (2018). Luat an ninh mang: Nhung dieu can biet [Law on cybersecurity: Basic knowledge]. Retrieved from https://vanhocnghethuat.files.wordpress.com/2019/01/savenet-camnangluatanninhmang-nhungdieucanbiet.pdf

Scholte, J. A. (2005). Globalization: A critical introduction (2nd ed.). Retrieved from http://aditi.du.ac.in/uploads/econtent/Globalization-Second-Edition-A-Critical-Introduction-.pdf

Scott, J. (2000). Social Network Analysis: A Handbook. London: SAGE.

Sellers, C. S., & Winfree, L. T. (2010). Akers, Ronald L.: Social Learning Theory. In Encyclopedia of Criminological Theory. https://doi.org/10.4135/9781412959193.n6

Silverman, D. (2013). Doing qualitative research (4th ed.; D. Silverman, Ed.). Lodon: SAGE Publications, Ltd.

Silverman, D. (2020). Introducing qualitative research. In D. Silverman (Ed.), Qualitative research (5th ed.). London: SAGE.

Singh, M., & Singh, S. (2007). Cyber crime convention and trans border criminality. Masaryk University Journal of Law and Technology, 1(1), 53–66.

Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cybercrime and virtual offender convergence settings. Trends in Organized Crime, 15(2–3), 111–129. https://doi.org/10.1007/s12117-012-9159-z

Sparrow, M. K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. Social Networks, 13(3), 251–274. https://doi.org/10.1016/0378-8733(91)90008-H

Spreen, M. (1992). Rare populations, hidden populations, and link-tracing designs: What and why? Bulletin of Sociological Methodology, 36(1), 34–58. https://doi.org/10.1177/075910639203600103

Standler, R. B. (2002). Computer crime. Retrieved June 18, 2019, from http://www.rbs2.com/ccrime.htm

Stolton, S. (2020). UN backing of controversial cybercrime treaty raises suspicions. Retrieved April 20, 2021, from EURACTIV website: https://www.euractiv.com/section/digital/news/un-backing-of-controversial-cybercrime-treaty-raises-suspicions/

Sunde, N. (2020). Structured hypothesis development in criminal investigation: A method aimed at providing a broad and objective starting point for a criminal investigation. The Police Journal: Theory, Practice and Principles. https://doi.org/10.1177/0032258X20982328

Sutherland, E. H. (1939). Principles of criminology (3rd ed.). Chicago: J.B. Lippincott Co.

Sutherland, E. H. (1947). Principles of criminology (4th ed.). Chicago: J.B. Lippincott Co.

Symantec. (2018). ISTR Internet security threat report volume 23. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

Taylor, C. S. (1990). Dangerous society. East Lansing, MI: Michigan State University Press.

Taylor, R. E., Fritsch, E. J., & Liederbach, J. (2014). Digital crime and digital terrorism (3rd ed.). New York: Pearson.

The 1999 Penal Code (No. 15/1999/QH10), 1999 December 21. Retrieved from https://thuvienphapluat.vn/van-ban/Trach-nhiem-hinh-su/Bo-Luat-hinh-su-1999-15-1999-QH10-46056.aspx

The 1999 Penal Code (amended in 2009) (No. 37/2009/QH12), 2009 June 19. Retrieved from https://thuvienphapluat.vn/van-ban/Trach-nhiem-hinh-su/Bo-luat-hinh-su-2009-sua-doi-37-2009-QH12-90648.aspx

The 2003 Criminal Procedure Code (No. 19/2003/QH11), 2003 November 26. Retrieved from https://thuvienphapluat.vn/van-ban/Trach-nhiem-hinh-su/Bo-luat-To-tung-Hinh-su-2003-19-2003-QH11-51701.aspx

The 2015 Criminal Procedure Code (No. 101/2015/QH13), 2015 November 27. Retrieved from https://thuvienphapluat.vn/van-ban/Trach-nhiem-hinh-su/Bo-luat-to-tung-hinh-su-2015-296884.aspx

The 2015 Penal Code (amended in 2017) (No. 12/2017/QH14), 2017 June 20. Retrieved from https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Luat-sua-doi-Bo-luat-Hinh-su-2017-354053.aspx

The Budapest Convention on Cybercrime (CETS No.185), 2001 November 23. Retrieved from https://www.coe.int/en/web/cybercrime/the-budapest-convention.

The Council of Europe. (2021). Chart of signatures and ratifications of Treaty 185. Retrieved January 16, 2021, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=fDCxuST0

The Crown Prosecution Service. (2019). Cybercrime - prosecution guidance. Retrieved March 6, 2021, from https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

The European Cybercrime Center. (2014). The Internet organised crime threat assessment (iOCTA) 2014. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014%0D

The Internet Society. (2017). Paths to our digital future. Retrieved from https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

The Japan Sociological Society. Code of Ethics. (2005). Retrieved from https://jss-sociology.org/about/ethicalcodes/

The Law on Cyber Security (No. 24/2018/QH14), 2018 June 12. Retrieved from https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-an-ninh-mang-2018-351416.aspx

The Law on Mutual Legal Assistance (No. 08/2007/QH12), 2007 November 21. Retrieved from https://thuvienphapluat.vn/van-ban/Thu-tuc-To-tung/Luat-tuong-tro-tu-phap-2007-08-2007-QH12-59655.aspx

The National Fraud Center. (2000). The growing global threat of economic and cyber crime. Retrieved from https://www.utica.edu/academic/institutes/ecii/publications/media/global_threat_crime.pdf

The UN Convention against Transnational Organized Crime. (2000). Retrieved from https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

The United Nations. (n.d.). Cybercrime. Retrieved December 29, 2020, from https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

The World Bank. (2019). Unemployment, total (% of total labor force) (modeled ILO estimate). Retrieved June 22, 2019, from https://data.worldbank.org/indicator/SL.UEM.TOTL.ZS?end=2018&locations=VN&start=2008

Thuat, N. H. (1998). Ly luan va phuong phap luan cua khoa hoc dieu tra hinh su [Theory and methodology of criminal investigation science]. Hanoi: The People's Police Academy.

Tropina, T. (2012). The evolving structure of online criminality. EUCRIM, 4, 158–165. Retrieved from http://www.corteidh.or.cr/tablas/r15111.pdf

Trung, B. (2019). Viet Nam tham du Doi thoai Quoc phong Seoul [Vietnam attends Seoul Defense Dialogue]. Retrieved from https://www.qdnd.vn/doi-ngoai/doi-ngoai-quoc-phong/viet-nam-tham-du-doi-thoai-quoc-phong-seoul-590340

Ulmer, J. T., & Wilson, M. S. (2003). The potential contributions of quantitative research to symbolic interactionism. Symbolic Interaction, 26(4), 531–552. https://doi.org/10.1525/si.2003.26.4.531

UN Economic and Social Council. (2002). UN Economic and Social Council Resolution 2002/13: Action to Promote Effective Crime Prevention. Retrieved from https://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/resolution_2002-13.pdf

United Nations. (2004). United Nations Convention against transnational organized crime and the protocols thereto. Retrieved from https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf

United Nations. (2019). Countering the use of information and communications technologies for criminal purposes. Retrieved from https://www.unodc.org/documents/Cybercrime/SG_report/V1908182_E.pdf

UNODC. (2002). Results of a pilot survey of forty selected organized criminal groups in sixteen countries. In United Nations Office on Drugs and Crime. Retrieved from http://publications.lib.chalmers.se/records/fulltext/245180/245180.pdf%0Ahttps://hdl.handle.net/20.500.12380/245180%0Ahttp://dx.doi.org/10.1016/j.jsames.2011.03.003%0Ahttps://doi.org/10.1016/j.gr.2017.08.001%0Ahttp://dx.doi.org/10.1016/j.precamres.2014.12

UNODC. (2006). Crime investigation. Retrieved from https://www.un.org/ruleoflaw/files/3_Crime_Investigation.pdf

UNODC. (2010). The globalisation of crime: A transnational organized crime threat assessment. In United Nations. https://doi.org/10.2307/20637835

UNODC. (2013). Comprehensive study on cybercrime - Draft. Retrieved from http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

van der Hulst, R. C. (2009). Introduction to social network analysis as an investigative tool. Trends in Organized Crime, 12, 101–121. https://doi.org/10.1007/s12117-008-9057-6

van Wilsem, J. (2013). “Bought it, but never got it” assessing risk factors for online consumer fraud victimization. European Sociological Review, 29(2), 168–178. https://doi.org/10.1093/esr/jcr053

Varese, F. (2006). The structure of criminal connections: The Russian-Italian mafia network. Oxford Legal Studies Research Paper, 21, 1–71.

VECITA. (2017). Thuong mai dien tu Viet Nam 2017 [E-commerce in Vietnam 2017]. Retrieved from http://www.idea.gov.vn/file/335ad166-71c3-48dc-9bf8-f1b13323843a

Vergelis, M., Shcherbakova, T., & Sidorina, T. (2019). Spam and phishing in 2018. Retrieved June 22, 2019, from https://securelist.com/spam-and-phishing-in-2018/89701/

Viet, T. T. (2008). Khai niem phong ngua toi pham duoi goc do toi pham hoc [Defining crime prevention under the perspective of crimonology]. The VNU Journal of Science, 24, 185–199. Retrieved from https://tks.edu.vn/thong-tin-khoa-hoc/chi-tiet/80/15

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]. Retrieved March 8, 2020, from https://lanhsuvietnam.gov.vn/Lists/BaiViet/Bài viết/DispForm.aspx?List=dc7c7d75-6a32-4215-afeb-47d4bee70eee&ID=414

VISA. (2014). Skimming is a scam. Retrieved from https://www.visa.co.jp/dam/VCOM/download/merchants/skimming-is-a-scam.pdf

VNISA. (2014). Bao cao nam 2013 [Annual Report 2013].

VNISA. (2015). Bao cao nam 2014 [Annual Report 2014].

VNISA. (2016a). Bao cao nam 2015 [Annual Report 2015].

VNISA. (2016b). Thong cao bao chi ve vu hacker tan cong vao he thong Vietnam Airlines [Press release about cyberattacks on the systems of Vietnam Airlines]. Retrieved June 18, 2019, from https://vnisa.org.vn/tin-tuc/an-ninh-mang/thong-cao-bao-chi-ve-vu-hacker-tan-cong-vao-he-thong-vietnam-airlines.html

VNISA. (2017). Bao cao nam 2016 [Annual Report 2016].

VNISA. (2018). Bao cao nam 2017 [Annual Report 2017].

VNISA. (2019). Bao cao nam 2018 [Annual Report 2018].

von Lampe, K. (2003). Criminally exploitable ties: A network approach to organized crime. In E. C. Viano, J. Magallanes, & L. Bidel (Eds.), Transnational Organized Crime: Myth, Power and Profit (pp. 9–22). Durham, NC: Carolina Academic Press.

von Lampe, K., & Ole Johansen, P. (2004). Organized crime and trust: On the conceptualization and empirical relevance of trust in the context of criminal networks. Global Crime, 6(2), 159–184. https://doi.org/10.1080/17440570500096734

Wall, D. (1999). Cybercrimes: New wine, no bottles? In P. Davies, P. Francis, & V. Jupp (Eds.), Invisible Crime (pp. 105–139). https://doi.org/10.1007/978-1-349-27641-7_5

Wall, D. S. (2015). Dis-organised crime: Towards a distributed model of the organization of cybercrime. The European Review of Organised Crime, 2(2), 71–90. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2677113

Waseda University. (2015). Academic research ethics guide: A guide to responsible conduct in research. Retrieved from https://www.waseda.jp/inst/ore/assets/uploads/2015/03/2015_Academic_Research_Ethics_Guide-1.pdf

We Are Social & Hootsuite. (2018). Digital in 2018. Retrieved from https://wearesocial.com/blog/2018/01/global-digital-report-2018

Weir, G. R. S., Toolan, F., & Smeed, D. (2011). The threats of social networking: Old wine in new bottles? Information Security Technical Report, 16(2), 38–43. https://doi.org/10.1016/j.istr.2011.09.008

Weisel, D. L. (2002). The evolution of street gangs: An examination of form and variation. In W. L. Reed & S. H. Decker (Eds.), Responding to Gangs: Evaluation and Research (pp. 25–65). Washington D.C.: National Institute of Justice.

Wikström, P.-O. H. (2009). Routine activity theories. In Oxford Bibliographies. https://doi.org/10.1093/OBO/9780195396607-0010

Williams, M. L. (2016). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. British Journal of Criminology, 56(1), 21–48. https://doi.org/10.1093/bjc/azv011

Williams, P. (2001a). Organized crime and cybercrime: Synergies, trends, and responses. Global Issues, 6(2), 22–26. Retrieved from https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=191389

Williams, P. (2001b). Transnational criminal networks. In J. Arquilla & D. Ronfeldt (Eds.), Networks and netwars: The Future of terror, crime, and militancy (pp. 61–97). Retrieved from https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch3.pdf

Williams, P. (2002). Organized crime and cybercrime: Implications for business. Retrieved from https://www.yumpu.com/en/document/read/29578286/organized-crime-and-cyber-crime-implications-for-business-cert

Wortley, R., & Mazerolle, L. (2008). Environmental criminology and crime analysis (R. Wortley & L. Mazerolle, Eds.). https://doi.org/10.1057/cpcs.2008.22

Yang, B. S., Keller, F. B., & Zheng, L. (2019). Descriptive methods in social network analysis. In Social Network Analysis: Methods and Examples (pp. 54–85). https://doi.org/10.4135/9781071802847

Yar, M. (2005). The novelty of "cybercrime": An assessment in light of routine activity theory. European Journal of Criminology, 2(4), 407–427. https://doi.org/10.1177/147737080556056

Yar, M. (2012). E-Crime 2.0: the criminological landscape of new social media. Information & Communications Technology Law, 21(3), 207–219.

Yeli, H. (2017). A three-perspective theory of cyber sovereignty. PRISM, 7(2), 109–115.

Yem, N. X. (2001). Toi pham hoc hien dai va phong ngua toi pham [Modern criminology and crime prevention]. Hanoi: Public Security Publishing House.

Yin, R. K. (2003). Case study research: Design and methods. In SAGE Publications, Inc. (Vol. 5). Retrieved from https://www.tandfonline.com/doi/full/10.1300/J145v03n03_07

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed). Thousand Oaks, California: SAGE Publications, Inc.

Yip, M. (2011). An investigation into Chinese cybercrime and the applicability of social network analysis. Retrieved from https://eprints.soton.ac.uk/272351/2/yip_poster_2011.pdf

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. Policing and Society, 23(4), 516–539. https://doi.org/https://doi.org/10.1080/10439463.2013.780227

Zhang, M. (2010). Social network analysis: History, concepts, and research. In B. Furht (Ed.), Handbook of Social Network Technologies and Applications (pp. 3–21). https://doi.org/10.1007/978-1-4419-7142-5_1

Zimba, A., Wang, Z., & Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. ICT Express, 4(1), 14–18. https://doi.org/10.1016/j.icte.2017.12.007

APPENDIX

Appendix 1. Criminal legislation on computer fraud in Vietnam

(The 1999 Penal Code, amended in 2009; and the 2015 Penal Code, amended in 2017)

Article 226b – The 1999 Penal Code, amended in 2009. Using computer networks, telecommunications networks, Internet or digital devices to appropriate property

1. Any person who uses computer networks, telecommunications networks, the Internet or digital devices to commit any of the following acts shall face a fine of between 10,000,000 VND and 100,000,000 VND or be sentenced to between 01 year and 05 years of imprisonment:

a. Using information on bank accounts or bank cards of agencies, organizations and individuals to obtain or produce fake bank cards to obtain property of card holders or pay for goods and services;

b. Illegally accessing the accounts of agencies, organizations and individuals to obtain property;

c. Committing fraud in ecommerce, currency trading, credit mobilization, share trading and payment online to appropriate property of agencies, organizations and individuals;

d. Other acts to appropriate property of agencies, organizations and individuals.

2. Committing the crime in any of the following cases, culprits shall be sentenced to between 03 and 07 years of imprisonment:

a. In an organized way;

b. Committing the crime more than once;

c. In a professional way;

d. Obtaining property valued between 50,000,000 VND and under 200,000,000 VND;

dd. Causing serious consequences;

e. Dangerous recidivism.

3. Committing the crime in any of the following cases, culprits shall be sentenced to between 07 and 15 years of imprisonment:

a. Obtaining property valued between 200,000,000 VND and under 500,000,000 VND;

b. Causing very serious consequences.

4. Committing the crime in any of the following cases, culprits shall be sentenced to between 12 years and 20 years of imprisonment or life imprisonment:

a. Obtaining property valued at 500,000,000 VND or more;

b. Causing extremely serious consequences.

5. Offenders might also be imposed a fine of between 5,000,000 VND and 100,000,000 VND, have a part or the whole of their property confiscated, be prohibited from holding certain positions or doing certain professions or jobs for between 01 year and 05 years.

Article 290 – the 2015 Penal Code, amended in 2017. Using computer networks, telecommunications networks, or digital devices to appropriate property

1. Any person who uses computer networks, telecommunications networks, or digital devices to commit any of the following acts, except for the cases in Article 173 and 174 hereof, shall face a penalty of up to 03 years' community sentence or be sentenced to between 06 months and 03 years' imprisonment:

a. Using information on bank accounts or cards of agencies, organizations, individuals to appropriate property of bank account owners, card holders, or pay for products, services;

b. Producing, storing, trading, using counterfeit bank cards to appropriate property of account owners, card holders or pay for products, services;

c. Illegally accessing the accounts of agencies, organizations, individuals to obtain property;

d. Committing fraud in ecommerce, digital payment, currency trading, capital mobilization, multi-level marketing, or share trading online to obtain property;

dd. Illegally installing or providing telecommunications or Internet services to appropriate property;

2. Committing the crime in any of the following cases, culprits shall be sentenced to between 02 years and 07 years' imprisonment:

a. In an organized way;

b. Committing the crime more than once;

c. In a professional way;

d. The number of fake cards is from 50 to under 200 cards;

dd. The property’s value is from 50,000,000 VND to under 200,000,000 VND;

e. Causing the damage from 50,000,000 VND to under 300,000,000 VND;

g. Dangerous recidivism.

3. Committing the crime in any of the following cases, culprit shall be sentenced to between 07 years and 15 years' imprisonment:

a. The property’ value is from 200,000,000 VND to under 500,000,000 VND;

b. Causing the damage from 300,000,000 VND to under 500,000,000 VND;

c. The number of fake cards is from 200 to under 500.

4. Committing the crime in any of the following cases, culprits shall be sentenced to between 12 years and 20 years' imprisonment:

a. The property’ value is from 500,000,000 VND;

b. Causing the damage from 500,000,000 VND;

c. The number of fake cards is from 500.

5. Offenders might also be imposed a fine of between 20,000,000 VND and 100,000,000 VND or prohibited from holding certain positions or doing certain professions or jobs for from 01 years to 05 years or have a part or all of their property confiscated.

Appendix 2. 20 selected case studies

Case study 01 (C01)

Using stolen bank card information to appropriate property by N.D.T & accomplices

Operation H211 – HTCP Department (2010)

Main content: From 2005 to 2010, N.D.T & accomplices bought stolen credit card data from international criminals and sold them for others. Stolen credit card data belonged to foreigners. Vietnamese fraudsters used stolen credit card information to buy products online from US ecommerce websites. Foreign shipping mules were recruited online to receive the packages and shipped them to Vietnam.

Clarified financial consequences: US$141,000.

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	N.D.T	C01-No.01	Male	25	Vietnamese	Unstable	No	Core member
2	L.T.T	C01-No.02	Male	27	Vietnamese	Unstable	No	Core member
3	H.T.D	C01-No.03	Male	23	Vietnamese	Unstable	No	
4	L.D.Q	C01-No.04	Male	21	Vietnamese	Unstable	No	
5	L.V.A	C01-No.05	Male	24	Vietnamese	Bank officer	No	
6	N.M.T	C01-No.06	Male	19	Vietnamese	Unstable	No	
7	D.H.Q	C01-No.07	Male	19	Vietnamese	Unstable	No	
8	T.D.T	C01-No.08	Male	23	Vietnamese	Unstable	No	
9	H.T.T	C01-No.09	Male	22	Vietnamese	Unstable	No	
10	L.T.Q	C01-No.10	Male	21	Vietnamese	Unstable	No	
11	M.H.V	C01-No.11	Male	27	Vietnamese	Unstable	No	
12	B.H.M	C01-No.12	Male	22	Vietnamese	Unstable	No	
13	N.T.T	C01-No.13	Male	23	Vietnamese	Unstable	No	
14	T.N.H	C01-No.14	Male	26	Vietnamese	Unstable	No	
15	L.D.D	C01-No.15	Male	22	Vietnamese	Unstable	No	
16	V.H.H	C01-No.16	Male	34	Vietnamese	Logistics officer	No	

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
17	V.Q.T	C01-No.17	Male	35	Vietnamese	Logistics officer	No	
18	D.Q.H	C01-No.18	Male	22	Vietnamese	Unstable	No	Core member
19	Shipping mule 01 of N.D.T	C01-No.19	?	?	?	?	?	Unidentified suspect
20	Shipping mule 02 of N.D.T	C01-No.20	?	?	?	?	?	Unidentified suspect
21	Shipping mule 03 of N.D.T	C01-No.21	?	?	?	?	?	Unidentified suspect
22	CC provider 01 of N.D.T	C01-No.22	?	?	?	?	?	Unidentified suspect
23	CC provider 02 of N.D.T	C01-No.23	?	?	?	?	?	Unidentified suspect
24	CC provider of Thuan 3	C01-No.24	?	?	?	?	?	Unidentified suspect
25	Shipping mule 01 of L.T.T	C01-No.25	?	?	?	?	?	Unidentified suspect
26	Shipping mule 02 of L.T.T	C01-No.26	?	?	?	?	?	Unidentified suspect
27	Shipping mule 03 of L.T.T	C01-No.27	?	?	?	?	?	Unidentified suspect
28	CC provider of L.T.T	C01-No.28	?	?	?	?	?	Unidentified suspect
29	Shipping mule 01 of H.T.D	C01-No.29	?	?	?	?	?	Unidentified suspect
30	CC provider 01 of H.T.D	C01-No.30	?	?	?	?	?	Unidentified suspect
31	CC provider of D.Q.H	C01-No.31	?	?	?	?	?	Unidentified suspect
32	Shipping mule 01 of D.Q.H	C01-No.32	?	?	?	?	?	Unidentified suspect
33	Shipping mule 02 of D.Q.H	C01-No.33	?	?	?	?	?	Unidentified suspect
34	Shipping mule 03 of D.Q.H	C01-No.34	?	?	?	?	?	Unidentified suspect
35	Shipping mule 02 of H.T.D	C01-No.35	?	?	?	?	?	Unidentified suspect
36	Shipping mule 03 of H.T.D	C01-No.36	?	?	?	?	?	Unidentified suspect
37	CC provider 02 of H.T.D	C01-No.37	?	?	?	?	?	Unidentified suspect

Case study 02 (C02)

Caller groups of phone scams operated by 42 Chinese and Taiwanese criminals

Operation HĐL1 – Haiphong Provincial Police (2014)

Main content: From October 2013 to October 2014, 42 Chinese and Taiwanese criminals entered Vietnam, then implemented fraudulent calls to Chinese citizens through VoIP systems. They were divided into three groups operating at different locations. Fraudulent callers used VoIP calls to contact Chinese victims, pretend to be authorities, and threaten victims about suspicious financial activity. After the victims were convinced, fraudsters requested victims to transfer money from their bank accounts to the money mules' accounts. Then, illegal money could be transferred via various bank accounts and lastly withdrawn by core fraudsters in Mainland China, Taiwan. In these cases, all criminals and victims were Chinese and Taiwanese. The locations of transferring and withdrawing illegal money were in Mainland China and Taiwan. Fraudulent callers used Vietnam's territory to conduct fraudulent VoIP calls. Vietnamese LEAs cooperated with counterparts of Mainland China, Taiwan to deport foreign fraudsters back to their country.

Clarified financial consequences: US$31,900.

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	G.J.M	C02-No.01	Male	39	Taiwanese	IT technician	No	Leader
2	C.W.Y	C02-No.02	Male	32	Taiwanese	Unstable	No	
3	C.W.M	C02-No.03	Male	34	Taiwanese	Chef	No	
4	C.C.T	C02-No.04	Male	18	Taiwanese	Worker	No	
5	L.X.Y	C02-No.05	Female	19	Taiwanese	Unstable	No	
6	L.C.W	C02-No.06	Male	29	Taiwanese	Unstable	No	
7	L.T.W	C02-No.07	Male	24	Taiwanese	Car mechanic	No	
8	C.R.S	C02-No.08	Male	26	Taiwanese	Unstable	No	
9	P.W.H	C02-No.09	Male	21	Taiwanese	Unstable	No	

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
10	L.Y.C	C02-No.10	Male	33	Taiwanese	Unstable	No	
11	T.P.C	C02-No.11	Male	21	Taiwanese	Student	No	
12	Y.H.T.Y	C02-No.12	Male	31	Taiwanese	Unstable	No	
13	T.C.C	C02-No.13	Male	23	Taiwanese	Unstable	No	
14	W.C.T	C02-No.14	Male	20	Taiwanese	Unstable	No	
15	C.H.C	C02-No.15	Male	44	Taiwanese	Unstable	No	
16	C.S.J	C02-No.16	Female	24	Taiwanese	Babysitter	No	
17	Z.G.F	C02-No.17	Male	18	Chinese	Unstable	No	
18	X.L.M	C02-No.18	Female	27	Chinese	Unstable	No	
19	Z.S.H	C02-No.19	Male	21	Chinese	Restaurant Waiter	No	
20	T.Y.S	C02-No.20	Male	31	Taiwanese	Unstable	No	Leader
21	T.H.Y	C02-No.21	Male	34	Taiwanese	Unstable	No	
22	L.T.W	C02-No.22	Male	29	Taiwanese	Construction Worker	No	
23	C.K.C	C02-No.23	Male	39	Taiwanese	Unstable	No	
24	P.H.H	C02-No.24	Male	36	Taiwanese	Worker	No	
25	K.J.H	C02-No.25	Female	30	Chinese	Business	No	
26	N.C.L	C02-No.26	Female	28	Chinese	Unstable	No	
27	L.H.Y	C02-No.27	Female	28	Chinese	Unstable	No	
28	F.H.W	C02-No.28	Female	28	Chinese	Unstable	No	
29	C.Y.C	C02-No.29	Male	24	Taiwanese	Unstable	No	Leader
30	Y.S.T	C02-No.30	Male	22	Taiwanese	Unstable	No	
31	C.S.F	C02-No.31	Male	24	Taiwanese	Unstable	No	

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
32	C.P	C02-No.32	Male	21	Chinese	Unstable	No	
33	Z.P.H	C02-No.33	Male	36	Chinese	Farmer	No	
34	W.B	C02-No.34	Male	24	Chinese	Worker	No	
35	H.X.H	C02-No.35	Male	23	Chinese	Hotel Receptionist	No	
36	L.R.P	C02-No.36	Female	39	Chinese	Unstable	No	
37	L.M.J	C02-No.37	Female	33	Chinese	Worker	No	
38	J.M.H	C02-No.38	Female	36	Chinese	Unstable	No	
39	L.L.F	C02-No.39	Female	40	Chinese	Unstable	No	
40	C.C.H	C02-No.40	Male	25	Chinese	Unstable	No	
41	W.F.Z	C02-No.41	Female	36	Chinese	Unstable	No	
42	L.H.Y	C02-No.42	Female	32	Chinese	Unstable	No	

Case study 03 (C03)

Using stolen bank card information to appropriate property by V.H.L and accomplices

Operation 129T – High-tech Crime Police Department (2011)

Main content: From 2008 to 2010, V.H.L & accomplices joined the website *vefamily.com* (with about 2,000 members) to buy and sell stolen credit card data. They also attacked foreign websites to obtain credit card information. They used stolen credit card data to buy products via US ecommerce websites. Foreign shipping mules were recruited online to receive and ship the illegal products from America to Vietnam. The total number of pieces of stolen bank card information was about 49,000.

Clarified financial consequences: US$1.2 million

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	V.H.L	C03-No.01	Male	22	Vietnamese	Techer	No	Core member
2	P.X.T	C03-No.02	Male	28	Vietnamese	Unstable	No	Core member
3	L.N.K	C03-No.03	Male	19	Vietnamese	Student	No	Core member
4	N.N.H	C03-No.04	Male	20	Vietnamese	Director of Logistics Company	No	
5	P.Q.H	C03-No.05	Male	24	Vietnamese	Student	No	Core member
6	T.V.T	C03-No.06	Male	24	Vietnamese	Student	No	Core member
7	L.D	C03-No.07	Male	24	Vietnamese	Student	No	Core member
8	L.H.H	C03-No.08	Male	20	Vietnamese	Unstable	No	Core member
9	T.N.L	C03-No.09	Male	26	Vietnamese	Unstable	No	
10	N.X.C	C03-No.10	Male	27	Vietnamese	Unstable	No	Core member
11	L.H.Q	C03-No.11	Male	24	Vietnamese	Unstable	No	Core member
12	H.Q.V	C03-No.12	Male	23	Vietnamese	Unstable	No	
13	N.M.T	C03-No.13	Male	19	Vietnamese	Student	No	
14	V.B	C03-No.20	?	?	?	?	?	Unidentified suspect
15	B.N	C03-No.21	?	?	?	?	?	Unidentified suspect
16	K.A	C03-No.22	?	?	?	?	?	Unidentified suspect
17	G.T	C03-No.23	?	?	?	?	?	Unidentified suspect
18	F	C03-No.24	?	?	?	?	?	Unidentified suspect
19	D.P.1	C03-No.25	?	?	?	?	?	Unidentified suspect
20	D.P 2	C03-No.26	?	?	?	?	?	Unidentified suspect
21	nhomaidang…	C03-No.27	?	?	?	?	?	Unidentified suspect

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
22	tuv…	C03-No.28	?	?	?	?	?	Unidentified suspect
23	black…	C03-No.29	?	?	?	?	?	Unidentified suspect
24	shadow…	C03-No.30	?	?	?	?	?	Unidentified suspect
25	Shipping mule 01 of P.Q.H	C03-No.31	?	?	?	?	?	Unidentified suspect
26	Shipping mule 02 of P.Q.H	C03-No.32	?	?	?	?	?	Unidentified suspect
27	Shipping mule 03 of P.Q.H	C03-No.33	?	?	?	?	?	Unidentified suspect
28	T.S	C03-No.34	?	?	?	?	?	Unidentified suspect
29	V.G	C03-No.35	?	?	?	?	?	Unidentified suspect
30	mast…	C03-No.36	?	?	?	?	?	Unidentified suspect
31	hait..	C03-No.37	?	?	?	?	?	Unidentified suspect
32	aloho8x…	C03-No.38	?	?	?	?	?	Unidentified suspect
33	Shipping mule 01 of L.D	C03-No.39	?	?	?	?	?	Unidentified suspect
34	Shipping mule 02 of L.D	C03-No.40	?	?	?	?	?	Unidentified suspect
35	C.T	C03-No.41	?	?	?	?	?	Unidentified suspect
36	one…	C03-No.42	?	?	?	?	?	Unidentified suspect
37	Binh…	C03-No.43	?	?	?	?	?	Unidentified suspect
38	Shipping mule 01 of L.H.H	C03-No.44	?	?	?	?	?	Unidentified suspect
39	Shipping mule 02 of L.H.H	C03-No.45	?	?	?	?	?	Unidentified suspect
40	D.N	C03-No.46	?	?	?	?	?	Unidentified suspect
41	CC provider 01 of N.X.C	C03-No.47	?	?	?	?	?	Unidentified suspect
42	CC provider 02 of N.X.C	C03-No.48	?	?	?	?	?	Unidentified suspect
43	Shipping mule 01 of N.X.C	C03-No.49	?	?	?	?	?	Unidentified suspect

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
44	Shipping mule 02 of N.X.C	C03-No.50	?	?	?	?	?	Unidentified suspect
45	Shipping mule 03 of N.X.C	C03-No.51	?	?	?	?	?	Unidentified suspect
46	S.P.V.N	C03-No.52	?	?	?	?	?	Unidentified suspect
47	b.fly…	C03-No.53	?	?	?	?	?	Unidentified suspect
48	k14…	C03-No.54	?	?	?	?	?	Unidentified suspect
49	omega…	C03-No.55	?	?	?	?	?	Unidentified suspect
50	freshcv…	C03-No.56	?	?	?	?	?	Unidentified suspect
51	nertvbep..	C03-No.57	?	?	?	?	?	Unidentified suspect
52	Shipping mule 01 of L.H.Q	C03-No.58	?	?	?	?	?	Unidentified suspect
53	Shipping mule 02 of L.H.Q	C03-No.59	?	?	?	?	?	Unidentified suspect
54	N.D.T	C01-No.01	Male	25	Vietnamese	Unstable	No	Also suspect of C01

Case study 04 (C04)

Buying and selling stolen bank card information by V.T.T and accomplices

Operation 226T – HTCP Department (2013)

Main content: Between 2007 and 2013, V.T.T, T.H.D & accomplices (often called as the *Mattfeuter* gang) designed the website *www.mattfeuter.cc*. This website was used for hackers to discuss and exchange tools, knowledge concerning stolen bank card data. The hacking forum had approximately 16,000 members. The *mattfeuter* forum was estimated to trade in 1.1 million stolen bank card data, causing at least US$200 million of damage for global victims. Most of the members listed in this case were core members operating the website *www.mattfeuter.cc.* Vietnamese culprits bought and sold stolen credit card data with foreign criminals. To solve the case, Vietnamese police cooperated with LEAs of US, and UK.

Clarified financial consequences: US$1.5 million

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	V.T.T	C04-No.01	Male	26	Vietnamese	Director of Company	No	Leader
2	T.H.D	C04-No.02	Male	24	Vietnamese	IT technician	No	Core member
3	L.V.K	C04-No.03	Male	31	Vietnamese	IT technician	No	Core member
4	T.T.D.H	C04-No.04	Female	32	Vietnamese	IT technician	No	Core member
5	M.T.T.T	C04-No.05	Female	24	Vietnamese	IT technician	No	Core member
6	N.V.Q	C04-No.06	Male	26	Vietnamese	IT technician	No	Core member
7	N.M.K	C04-No.07	Male	24	Vietnamese	IT technician	No	Core member
8	T.V.C	C04-No.08	Male	?	Vietnamese	Director of Company	No	Related person
9	Del..	C04-No.09	Male	?	Philippines	?	?	Unidentified suspect

Case study 05 (C05)

Buying and selling stolen bank card information; Using stolen bank card information to appropriate property by H.P.M & accomplices

Operation 258V – HTCP Department (2014)

Main content: From 2011 to 2014, H.P.M & accomplices designed and managed the website *vietexpert.info* to buy and sell stolen credit card data. They also attacked foreign websites to obtain credit card information. They used stolen credit card data to buy products online from US websites and transported them to Vietnam. Foreign shipping mules were recruited online to receive and ship the illegal products to Vietnam. *Vietexpert.info* is one of the most major hacking forums investigated by Vietnamese police. It had approximately 3,000 members, over 955,000 reports; operating under the administration of H.P.M from 2011 to 2014.

Clarified financial consequences: US$80,000

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	H.P.M	C05-No.01	Male	24	Vietnamese	Unstable	No	Leader Technical administrator of vefamily.com. After vefamily.com was cracked down in 2010, C05-No.01 copied its source code to design vietexpert.info.
2	V.D.H	C05-No.02	Male	26	Vietnamese	Unstable	No	Technical administrator
3	V.V.D	C05-No.03	Male	29	Vietnamese	Unstable	No	
4	N.T.D.N	C05-No.04	Female	32	Vietnamese	Unstable	No	
5	N.N.H	C05-No.05	Male	31	Vietnamese	Unstable	No	
6	L.V.A.V	C05-No.06	Male	24	Vietnamese	Unstable	No	
7	N.V.H	C05-No.07	Male	23	Vietnamese	Unstable	No	High-tech skills, graduated at Ho Chi Minh City University of Technology
8	N.X.L	C05-No.08	Male	30	Vietnamese	Unstable	Yes	
9	N.Q.N	C05-No.09	Male	35	Vietnamese	Unstable	No	

Case study 06 (C06)

Using stolen bank card information to make fake bank cards by Z.X.T & accomplices

Operation 981T – Hanoi Police (2014)

Main content: Z.X.T (nationality: Chinese) entered Vietnam, then cooperated with other Vietnamese criminals to make fake bank cards with stolen credit card information. Initially, fraudsters used fake bank cards to withdraw cash at ATMs or buy products at retail stores. After that, they conducted fake transactions through POS terminals to withdrawn money. The network leader Z.X.T directed members to found four "ghost" companies that did not carry out real business activities. The "ghost" companies were used to register for using POS terminals with banks. They used counterfeit bank cards to conduct fake transactions via these POS terminals. There were no any products and services in fake transactions.

Clarified financial consequences: US$56,000

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	Z.X.T	C06-No.01	Male	30	Chinese	Director of Company	No	Leader
2	D.V.C	C06-No.02	Male	29	Vietnamese	Director of Company	No	Real occupation: unstable
3	L.T.H	C06-No.03	Male	22	Vietnamese	Director of Company	No	Real occupation: Unstable
4	N.T.P	C06-No.04	Female	26	Vietnamese	Director of Company	No	Real occupation: Unstable
5	H.T.T	C06-No.05	Male	21	Vietnamese	Director of Company	No	Real occupation: Unstable
6	Taiwanese associate 1	C06-No.06	?	?	Taiwanese	?	?	Unidentified suspect
7	Taiwanese associate 2	C06-No.07	?	?	Taiwanese	?	?	Unidentified suspect

Case study 07 (C07)

Buying and selling stolen bank card information; Using stolen bank card information to appropriate property by P.T.T & accomplices

Operation 113H – HTCP Department (2014)

Main content: After buying stolen credit card data on underground websites, P.T.T & accomplices used these bank card data to buy products online from US websites and shipped them to Vietnam. Stolen credit card data belonged to foreigners. Foreign shipping mules were recruited online to receive and ship the illegal products from the US to Vietnam.

Clarified financial consequences: US$174,000

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	P.T.T	C07-No.01	Male	31	Vietnamese	Unstable	No	Core member, founding member and admin of hkvfamily.info
2	L.V.H.H	C07-No.02	Male	49	Vietnamese	Unstable	No	Core member,

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
								founding member and admin of hkvfamily.info
3	P.T.N.Q	C07-No.03	Male	30	Vietnamese	Unstable	No	Core member, enthusiastic member of hkvfamily.info
4	V.Q.N	C07-No.04	Male	23	Vietnamese	Unstable	No	Core member, enthusiastic member of hkvfamily.info
5	N.T.D.N	C05-No.04	Female	32	Vietnamese	Unstable	No	Core member, admin of allcard.us, member of hkvfamily.info, also a suspect of Operation 258V
6	D.H.D.T	C07-No.05	Male	33	Vietnamese	Unstable	No	Core member, husband of N.T.D.N
7	H.P.M	C05-No.01	Male	24	Vietnamese	Unstable	No	Technical administrator of vefamily.com. After vefamily.com was cracked down in 2010, C05-No.01 copied its source code to design vietexpert.info. Also suspect of Operation 258V
8	V.V.D	C05-No.03	Male	29	Vietnamese	Unstable	No	Also a suspect of Operation 258V
9	L.V.A.V	C05-No.06	Male	24	Vietnamese	Unstable	No	Also a suspect of Operation 258V
10	T.N.A.K	C07-No.06	?	?	Vietnamese	?	?	Unidentified suspect
11	L.D.A	C07-No.07	?	?	Vietnamese	?	?	Unidentified suspect
12	P.B.A	C07-No.08	?	?	Vietnamese	?	?	Unidentified suspect
13	P.M.H	C07-No.09	?	?	Vietnamese	?	?	Unidentified suspect
14	CC provider 01 of P.T.T	C07-No.10	?	?	?	?	?	Unidentified suspect

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
15	CC provider 02 of P.T.T	C07-No.11	?	?	?	?	?	Unidentified suspect
16	Shipping mule 01 of P.T.T	C07-No.12	?	?	?	?	?	Unidentified suspect
17	Shipping mule 02 of P.T.T	C07-No.13	?	?	?	?	?	Unidentified suspect
18	Shipping mule 02 of P.T.T	C07-No.14	?	?	?	?	?	Unidentified suspect
19	N.X.H	C07-No.15	?	?	Vietnamese	?	?	Unidentified suspect
20	CC provider of L.V.H.H	C07-No.16	?	?	?	?	?	Unidentified suspect
21	Shipping mule 01 of L.V.H.H	C07-No.17	?	?	?	?	?	Unidentified suspect
22	Shipping mule 02 of L.V.H.H	C07-No.18	?	?	?	?	?	Unidentified suspect
23	D.D.M	C07-No.19	?	?	Vietnamese	?	?	Unidentified suspect
24	CC provider of N.T.D.N	C07-No.20	?	?	?	?	?	Unidentified suspect
25	Shipping mule 01 of N.T.D.N	C07-No.21	?	?	?	?	?	Unidentified suspect
26	Shipping mule 02 of N.T.D.N	C07-No.22	?	?	?	?	?	Unidentified suspect
27	Shipping mule 03 of N.T.D.N	C07-No.23	?	?	?	?	?	Unidentified suspect
28	CC provider of D.H.D.T	C07-No.24	?	?	?	?	?	Unidentified suspect
29	Shipping mule 01 of D.H.D.T	C07-No.25	?	?	?	?	?	Unidentified suspect
30	Shipping mule 02 of D.H.D.T	C07-No.26	?	?	?	?	?	Unidentified suspect

Case study 08 (C08)

Buying and selling stolen bank card information; Using stolen bank card information to appropriate property by N.T.Q & accomplices

Operation 111D – High-tech Crime Police Department (2011)

Main content: From 2009 to 2011, N.T.Q and accomplices used stolen credit card data to buy domain names of websites, software or products online from foreign websites and shipped them to Vietnam. Through relationships with other hackers via virtual hacking forums, fraudsters could be provided stolen bank card data, stolen mails and passwords. They also attacked websites to steal bank card data of customers; exchanged, traded stolen credit card data. They used stolen bank card data to buy domain names, mainly via *https://www.eurodns.com.* Stolen bank card data was also used to buy software or products.

Clarified financial consequences: US$30,000

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	N.T.Q	C08-No.01	Male	22	Vietnamese	Student	No	
2	N.V.Q	C08-No.02	Male	23	Vietnamese	Student	No	
3	N.H.T	C08-No.03	Male	22	Vietnamese	Student	No	
4	N.P.K	C08-No.04	Male	24	Vietnamese	Unstable	No	
5	H.H.H	C08-No.05	?	?	Vietnamese	?	?	Unidentified suspect

Case study 09 (C09)

Using stolen bank card information to make fake bank cards by L.Z.Q & accomplices

Haiduong Provincial Police (2014)

Main content: L.Z.Q (nationality: Chinese) entered Vietnam in 2013, then cooperated with other Vietnamese criminals to make fake bank cards with stolen credit card information. Under the leadership of L.Z.Q, Vietnamese culprits founded a company. This company that did not focus on conducting real business activities. It was founded with the aim of registering for a

POS terminal with banks. They used counterfeit bank cards to conduct fake transactions via the POS terminal. There were no any products and services in fake transactions.

Clarified financial consequences: US$44,000

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	L.Z.Q	C09-No.01	Male	34	Chinese	Business Man	No	Leader
2	L.T.T	C09-No.02	Male	46	Vietnamese	Vice Director of Company	No	Real occupation: Unstable
3	N.V.H	C09-No.03	Male	57	Vietnamese	Director of Company	No	
4	L.X.T	C09-No.04	Male	57	Vietnamese	Director of Company	No	Real occupation: Unstable
5	CC provider	C09-No.05	?	?	Chinese	?	?	Unidentified suspect

Case study 10 (C10)

Using stolen bank card information to make fake bank cards by L.D.J & accomplices

Hanoi Police (2015)

Main content: L.D.J (nationality: Chinese) entered Vietnam in 2015, then cooperated with other Chinese criminals to make fake bank cards with stolen credit card information. After that, they conducted fake transactions through a POS terminal to withdrawn money. The POS terminal was managed by the company of L.Q.G. There were no any products and services in fake transactions.

Clarified financial consequences: US$5,075

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	L.D.J	C10-No.01	Male	34	Chinese	Unstable	No	Leader
2	L.F.H	C10-No.02	Male	31	Chinese	Unstable	No	
3	L.P.F	C10-No.03	Male	51	Chinese	Unstable	No	

4	L.Q.G	C10-No.04	Male	43	Chinese	Director	No	
5	F.S.Z	C10-No.05	?	?	Chinese	?	?	Unidentified suspect
6	Thien…	C10-No.06	?	?	Chinese	?	?	Unidentified suspect
7	Li…	C10-No.07	?	?	Chinese	?	?	Unidentified suspect
8	CC…	C10-No.08	?	?	Chinese	?	?	Unidentified suspect
9	Nguoidai…	C10-No.09	?	?	?	?	?	Unidentified suspect

Case study 11 (C11)

Money mule group of phone scams

Operation 195H - Hanoi Police (2015)

Main content: Under the instruction of Chinese criminals, in 2015, V.V.L & V.V.T (nationality: Vietnamese) borrowed identity cards of some people or cooperated with other accomplices to open bank accounts. Subsequently, these bank accounts were used to receive illegal money from phone scams' Vietnamese victims. After being informed that illegal money was transferred to these bank accounts, they would withdraw and transfer the money to A.B via banks or gold shops. Fraudulent calls were implemented via VoIP calling systems originating outside Vietnam. Fraudulent callers often pretended to be law enforcement officials to threaten and lure victims into transferring money. Vietnamese LEAs could not identify group leaders and fraudulent callers.

Clarified financial consequences: US$362,000

Information about suspects:

No	Name	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	V.V.L	C11-No.01	Male	28	Vietnamese	Unstable	Yes	01 record about robbery
2	V.V.T	C11-No.02	Male	28	Vietnamese	Unstable	Yes	02 records about theft
3	P.T.H	C11-No.03	Female	25	Vietnamese	Unstable	No	
4	L.V.D	C11-No.04	Male	28	Vietnamese	Unstable	Yes	01 record about robbery

No	Name	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
5	V.V.C	C11-No.05	Male	26	Vietnamese	Unstable	No	
6	P.V.H	C11-No.06	Male	26	Vietnamese	Unstable	Yes	01 record about concealing offenses
7	B.D.D	C11-No.07	Male	33	Vietnamese	Unstable	Yes	
8	V.T.T.H	C11-No.08	Female	?	Vietnamese	?	?	Unidentified suspect
9	T.X.H	C11-No.09	Male	?	Vietnamese	?	?	Unidentified suspect
10	Chinese leader 01	C11-No.10	?	?	Chinese	?	?	Leader 01 Unidentified suspect
11	Chinese leader 02	C11-No.11	?	?	Chinese	?	?	Leader 02 Unidentified suspect

Case study 12 (C12)

Money mule group of phone scams

Operation 201D - Hanoi Police (2014)

Main content: Under the instruction of A.B.E - a Chinese person, in 2015, V.D.H, T.T.M.N, T.T.L. (nationality: Vietnamese) borrowed identity cards of other people or cooperated with other accomplices to open bank accounts. Afterwards, these bank accounts would be used to receive illegal money from phone scams' Vietnamese victims. They were responsible for withdrawing and transferring illegal money to A.B.E via banks. Fraudulent calls were conducted via VoIP calling systems originating outside Vietnam. Fraudulent callers often pretended to be law enforcement officials to threaten and lure victims into transferring money. Vietnamese police could not identify group leaders and fraudulent callers.

Clarified financial consequences: US$47,500

Information about suspects:

No	Name/ nicks	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	V.D.H	C12-No.01	Male	22	Vietnamese	Unstable	No	
2	T.T.M.N	C12-No.02	Female	24	Vietnamese	Unstable	No	

No	Name/ nicks	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
3	T.T.L	C12-No.03	Female	32	Vietnamese	Unstable	No	
4	N.T.D	C12-No.04	Male	22	Vietnamese	Unstable	No	
5	P.T.H	C12-No.05	Female	24	Vietnamese	Unstable	No	
6	P.V.Q	C12-No.06	Male	23	Vietnamese	Unstable	No	Related person
7	N.V.D	C12-No.07	Male	22	Vietnamese	Unstable	No	Related person
8	N.K.T	C12-No.08	Male	25	Vietnamese	Unstable	No	Related person
9	A.B.E	C12-No.09	Male	?	Chinese	?	?	Leader Unidentified suspect

Case study 13 (C13)

Using bank card data for making fake bank cards

Operation 112Q - Hanoi Police (2015)

Main content: In 2015, three Korean fraudsters, K.S.H., K.Y.Y., Y.D.K. cooperated with a Vietnamese fraudster T.N.T. to make fake bank cards with stolen credit card information. After that, they borrowed three POS terminals from V.T.T, T.T.V, D.L.H. They conducted fake transactions through POS terminals to withdrawn money. No products and/or services were exchanged.

Clarified financial consequences: US$15,000

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	K.S.H	C13-No.01	Male	33	Korean	Unstable	Yes	Leader 02 records of fraud and theft
2	T.N.T	C13-No.02	Male	40	Vietnamese	Unstable	No	Leader
3	K.Y.Y	C13-No.03	Male	40	Korean	Unstable	Yes	02 records of military law violence, fraud
4	Y.D.K	C13-No.04	Male	51	Korean	Unstable	Yes	02 records of labor law and traffic law violence

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
5	P.H.N	C13-No.05	Male	39	Vietnamese	Unstable	No	Related person
6	V.T.T	C13-No.06	Female	28	Vietnamese	Small business manager	No	Related person
7	N.B.K	C13-No.07	Male	27	Vietnamese	Unstable	No	Related person
8	T.T.V	C13-No.08	Female	31	Vietnamese	Director of a company	No	Related person
9	D.L.H	C13-No.09	Female	31	Vietnamese	Director of a company	No	Related person
10	A.Y.S	C13-No.10	Male	?	Korean	?	?	Unidentified suspect
11	J.D.S	C13-No.11	Male	?	Korean	?	?	Unidentified suspect
12	C.W.B	C13-No.12	?	?	?	?	?	Unidentified suspect

Case study 14 (C14)

Money mule group of phone scams

Operation 201D - Hanoi Police (2014)

Main content: Under the instruction of two Taiwanese criminals: L.C.M and T.J.C, Vietnamese suspects borrowed identity cards of other individuals to open bank accounts. Then, they sent these bank accounts to the Taiwanese criminals to receive illegal money. These bank accounts would be used to receive illegal money from Vietnamese victims of phone scam cases. Fraudulent calls were conducted via VoIP calling systems originating outside Vietnam. Fraudulent callers often pretended to be law enforcement officials to threaten and lure victims into transferring money. Vietnamese police could not identify and arrest fraudulent callers.

Clarified financial consequences: US$278,500

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	L.C.M	C14-No.01	Male	37	Taiwanese	Unstable	No	Leader
2	T.J.C	C14-No.02	Male	38	Taiwanese	Unstable	No	Leader

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
3	V.V.D	C14-No.03	Male	23	Vietnamese	Translator	No	
4	N.T.D	C14-No.04	Male	25	Vietnamese	Unstable	No	
5	N.X.D	C14-No.05	Male	24	Vietnamese	Unstable	No	
6	T.N.B	C14-No.06	Male	25	Vietnamese	Worker	No	
7	T.X.H	C14-No.07	Male	28	Vietnamese	Unstable	No	
8	D.D.P	C14-No.08	Male	42	Vietnamese	Official of company	No	Related person
9	D.T.H	C14-No.09	Female	22	Vietnamese	Receptionist	No	Related person
10	D.T.HA	C14-No.10	Female	22	Vietnamese	Customer Officer	No	Related person

Case study 15 (C15)

Caller group of phone scams by Korean criminals

Operation HQ2015 – HTCP Department (2015)

Main content: This Korean gang operated in many countries of South East Asia before being captured in Vietnam. Under the management of They managed and lived at a hotel when implementing computer frauds. Korean fraudsters uploaded information about products to Korean e-commerce websites or forums. When Korean customers attempted to buy these products, fraudulent callers contacted them via VoIP calling systems from Vietnam using fake numbers that seemed to originate from Korea. After customers transferred money to purchase the goods, fraudsters ceased contact with them without sending the products.

Clarified financial consequences: US$4,000,000

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	K.W.S	C15-No.01	Male	42	Korean	Manager of Hotel	Yes	Leader Red-notice wanted
2	K.D.Y	C15-No.02	Male	32	Korean	Unstable	Yes	Leader Red-notice wanted

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
3	S.S	C15-No.03	Male	27	Korean	Unstable	No	
4	J.J	C15-No.04	Male	30	Korean	Unstable	No	
5	C.K.S	C15-No.05	Male	28	Korean	Unstable	No	
6	S.M	C15-No.06	Female	29	Korean	Unstable	No	
7	J.JA	C15-No.07	Male	29	Korean	Unstable	No	

Case study 16 (C16)

Money mule group of phone scams

Operation 917L - Nghean Provincial Police (2017)

Main content: Under the guidance of N.V.P. (nationality: Vietnamese, living in Taiwan), three Vietnamese criminals P.D.L., N.H.T., and P.D.P. used their identity cards or fake cards to open bank accounts. These bank accounts would be used to receive illegal money from Vietnamese victims of phone scam cases. There were two groups inside this ring. The first group operating from Taiwan implemented fraudulent calls to Vietnamese victims through VoIP systems. N.V.P directed the second group to receive illegal money. Fraudulent calls were conducted via VoIP calling systems originating outside Vietnam. Callers often pretended to be law enforcement officials to threaten and lure victims into transferring money. Vietnamese LEAs could not clarify and arrest group leaders and fraudulent callers.

Clarified financial consequences: US$167,600

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	P.D.L	C16-No.01	Male	24	Vietnamese	Student	No	
2	N.H.T	C16-No.02	Male	26	Vietnamese	Unstable	Yes	One theft record
3	P.D.P	C16-No.03	Male	18	Vietnamese	Unstable	No	
4	N.V.P	C16-No.04	Male	27	Vietnamese	Unstable	No	Leader Work, live in Taiwan

Case study 17 (C17)

Money mule group of phone scams

Vinhphuc Provincial Police (2017)

Main content: Under the guidance of Chinese ringleaders, Vietnamese suspects implemented VoIP fraudulent calls to Vietnamese citizens. There were two groups in this ring. The first group operating outside Vietnam implemented VoIP fraudulent calls to Vietnamese victims. Callers often pretended to be law enforcement officials to threaten and lure victims into transferring money. Vietnamese LEAs could not clarify and arrest the caller group. Whereas, H.D.G (a Chinese person) directed the second group to receive illegal money from Vietnamese victims.

Clarified financial consequences: US$167,933

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	H.D.G	C17-No.01	Male	46	Chinese	Unstable	No	Leader
2	N.V.T	C17-No.02	Male	30	Vietnamese	Fisherman	Yes	
3	B.V.H	C17-No.03	Male	31	Vietnamese	Worker	No	
4	N.D.P	C17-No.04	Male	24	Vietnamese	Unstable	No	
5	N.T.H	C17-No.05	Female	43	Vietnamese	Money exchanger	No	Related person
6	D.	C17-No.06	Male	?	Vietnamese	?	?	Unidentified suspect
7	A.C	C17-No.07	Male	?	?	?	?	Unidentified suspect

Case study 18 (C18)

Caller groups of phone scams by 24 Chinese and Taiwanese criminals

Operation TQ2015 – HTCP Department (2015)

Main content: In 2015, 24 Chinese and Taiwanese criminals entered Vietnam and hired two apartments in Ho Chi Minh City, to implement phone scams to Mainland China via VoIP calling systems. They pretended to be law enforcement officials, then threatened and lured victims into transferring money. In these cases, all victims and criminals were Chinese and Taiwanese. The places of transferring and withdrawing illegal money were in Mainland China and Taiwan. Vietnam's territory was used to conduct fraudulent VoIP calls. Vietnamese LEAs cooperated with counterparts of Mainland China, Taiwan to deport foreign fraudsters back to their country.

Clarified financial consequences: US$2,733,000

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	L. Y. X	C18-No.01	Female	36	Taiwanese	Unstable	No	Leader
2	C. Y. H	C18-No.02	Male	26	Taiwanese	Unstable	No	
3	L. Y. D	C18-No.03	Male	22	Taiwanese	Unstable	No	
4	L. Z. C	C18-No.04	Male	26	Taiwanese	Unstable	No	
5	C. M. H	C18-No.05	Male	18	Taiwanese	Unstable	No	
6	D. K. X	C18-No.06	Male	22	Taiwanese	Unstable	No	
7	C. W. C	C18-No.07	Male	29	Taiwanese	Unstable	No	
8	P. T. Y	C18-No.08	Male	22	Taiwanese	Unstable	No	
9	L. Z. Y	C18-No.09	Male	33	Taiwanese	Unstable	No	
10	C. W. H	C18-No.10	Male	19	Taiwanese	Unstable	No	
11	C. C. H	C18-No.11	Male	40	Taiwanese	Unstable	No	
12	F. G. H	C18-No.12	Male	25	Taiwanese	Unstable	No	
13	L. Q	C18-No.13	Male	26	Chinese	Unstable	No	
14	H. J. X	C18-No.14	Male	20	Chinese	Unstable	No	
15	C. Y. Q	C18-No.15	Male	27	Chinese	Unstable	No	
16	H. Z. M	C18-No.16	Male	23	Chinese	Unstable	No	
17	Q. M. C	C18-No.17	Male	30	Chinese	Unstable	No	
18	Z. X. Q	C18-No.18	Male	37	Chinese	Unstable	No	
19	H. F. P	C18-No.19	Male	32	Chinese	Unstable	No	

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
20	L. Q. Y	C18-No.20	Female	23	Chinese	Unstable	No	Leader
21	Q. L	C18-No.21	Female	26	Chinese	Unstable	No	
22	T. M. H	C18-No.22	Male	25	Chinese	Unstable	No	
23	W. Z	C18-No.23	Male	26	Chinese	Unstable	No	
24	W. K. M	C18-No.24	Male	24	Chinese	Unstable	No	

Case study 19 (C19)

Using stolen bank card information to make fake bank cards by four Chinese criminals

Operation H213 - HTCP Department (2013)

Main content: Four Chinese fraudsters: X.J., L.W., L.J.J., and L.L.H. entered Vietnam in 2013, then made fake bank cards with stolen credit card information. After that, they borrowed POS terminals from Vietnamese individuals. They conducted fake transactions through POS terminals to withdrawn money. No products and/or services were exchanged.

Clarified financial consequences: US$278,400

Information about suspects:

No	Name/ nick	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	Y.B	C19-No.01	?	?	Chinese	?	?	Leader Unidentified suspect
2	X.J	C19-No.02	Male	34	Chinese	Unstable	No	
3	L.W	C19-No.03	Male	49	Chinese	Unstable	No	
4	L.J.J	C19-No.04	Male	20	Chinese	Unstable	No	
5	L.L.H	C19-No.05	Male	32	Chinese	Unstable	No	
6	P.T.C	C19-No.06	Female	?	Vietnamese	Director of Company	No	related person
7	N.T.H	C19-No.07	Female	?	Vietnamese	Director of Company	No	related person

8	N.V.M	C19-No.08	Male	?	Vietnamese	Director of Company	No	related person

Case study 20 (C20)

Stealing bank card data to make fake cards by Chinese criminals

Quangninh Provincial Police (2018)

Main content: In March 2017, four Chinese fraudsters: Z.R.X, L.D.Y, F.Y.H, W.T entered Vietnam illegally. Then, they went to Thaibinh province to set up skimming tools to steal the information of debit/credit cards at ATMs. After that, they went back to China to clone bank cards. In February 2018, they reentered Vietnam to withdrawn cash at ATMs with fake cards.

Clarified financial consequences: US$4,150

Information about suspects:

No	Name	Code	Gender	Age	Nationality	Occupation	Criminal records	Note
1	Z.R.X	C20-No.01	Male	28	Chinese	Unstable	No	Leader
2	L.D.Y	C20-No.02	Male	29	Chinese	Unstable	No	
3	F.Y.H	C20-No.03	Male	30	Chinese	Unstable	No	
4	W.T	C20-No.04	Male	27	Chinese	Unstable	No	

Appendix 3. Interviewee details

Investigator	**Age**	**Rank**	**Gender**	**Case**	**Organization**
I01	49	Senior Colonel	Male	C01	HTCP Department
I02	35	Major	Male	C02	Haiphong Police Station
I03	46	Senior Colonel	Male	C03, C04, C05	HTCP Department
I04	42	Colonel	Female	C11, C12, C14	Hanoi Police Station
I05	37	Major	Male	C07	HTCP Department
I06	38	Lieutenant Colonel	Male	C09	Haiduong Police Station
I07	43	Colonel	Male	C06, C13	Hanoi Police Station
I08	33	Captain	Male	C10	Hanoi Police Station
I09	28	Senior Lieutenant	Male	C15	Hanoi Police Station
I10	28	Lieutenant	Male	C16	Nghean Police Station
I11	42	Colonel	Male	C17	Vinhphuc Police Station
I12	35	Major	Male	C18	HTCP Department
I13	33	Captain	Female	C19	HTCP Department
I14	29	Senior Lieutenant	Male	C20	Hanoi Police Station

Note: The HTCP Department now is the Department of Cybersecurity and Counter High-tech Crime.

Waseda University
Graduate School of Asia-Pacific Studies
早稲田大学 大学院アジア太平洋研究科

Appendix 4. Interview Protocol

The research title: “Analyzing cybercrime networks: Transnational computer fraud in Vietnam”

Thank you very much for participating in the research.

My name is Nguyen Van Trong, a Ph.D. student of Graduate School of Asia-Pacific Studies (GSAPS), Waseda University, Tokyo, Japan. My email is trongnv1607@toki.waseda.jp. My phone number is (+81) 080 8721 6613.

This research is implemented as one part of my Ph.D. program at Graduate School of Asia-Pacific Studies (GSAPS), Waseda University under the supervision of Professor Ken Miichi (email: miichi@waseda.jp). The target of research is to clarify the characteristics of transnational computer fraud in Vietnam. Please consider that your answers can be used for further studies and publications in same disciplines of this research. The interview will be expected to last less than one hour.

I want to confirm that all responses will be kept anonymously. Your name will be coded instead of real names when being used in my research. You have the right to end the interview at any time. You don’t have to tell about anything you don’t want. You have the right to ask collected data to be withdrawn and destroyed before publication. If you have any questions, please don’t hesitate to contact me.

Are you willing to participate in the interview?

□ Yes □ No

_________________________ _________________________

Participant Date

Part I: Introduction

Name:

Gender:

Age:

Rank:

Position:

Role in the case:

Part II: General information about the case

Please you tell me some main information about the content of the case?

Part III: Specific questions

A. Modus operandi

What is the modus operandi of the case?

How could culprits avoid the detection of law enforcement agencies?

What is the role of technology inside the case?

What about transnational factors presented in the case?

What do you comment on the modus operandi of this case, as compared to other TCF cases?

B. Structure

What about roles of actors inside the network?

How strong was the relationship between actors in the network?

Please describe the most powerful influencer inside the network?

What do you comment on the structure of this network, as compared to other TCF networks?

Part IV: Conclusion

Is there anything more you want to add?

Do you mind if I contact you again to clarify some unclear points?

Many thanks for your participation!

Waseda University
Graduate School of Asia-Pacific Studies
早稲田大学 大学院アジア太平洋研究科

DỰ KIẾN CÂ U HỎI PHỎNG VẤN

Tên đề tài: "Phân tích mạng lưới tội phạm mạng: Tội phạm máy tính chiếm đoạt tài sản xuyên quốc gia tại Việt Nam"

Trân trọng cảm ơn anh/chị đã tham gia vào chương trình nghiên cứu.

Tên tôi là: Nguyễn Văn Trọng, nghiên cứu sinh của Trường Cao học Nghiên cứu Châu Á – Thái Bình Dương (GSAPS), Đại học Waseda, Tokyo, Nhật Bản. Địa chỉ email của tôi là: trongnv1607@toki.waseda.jp. Số điện thoại của tôi là: (+81) 080 8721 6613.

Hoạt động nghiên cứu này được tiến hành như một phần trong chương trình nghiên cứu sinh của tôi tại Trường Cao học Nghiên cứu Châu Á – Thái Bình Dương (GSAPS), Đại học Waseda, dưới sự hướng dẫn của Giáo sư Ken Miichi (email: miichi@waseda.jp). Mục tiêu nghiên cứu nhằm làm rõ các đặc điểm của tội phạm máy tính chiếm đoạt tài sản xuyên quốc gia tại Việt Nam. Cũng cần chú ý rằng, những phản hồi của anh/chị có thể được sử dụng cho chương trình nghiên cứu khác và xuất bản với các quy định tương tự như của chương trình nghiên cứu này. Hoạt động phỏng vấn dự kiến kéo dài ít hơn một giờ.

Tôi xác nhận rằng tất cả các phản hồi sẽ được giữ nặc danh. Tên của anh/chị sẽ được mã hóa, thay thế tên thật khi được sử dụng trong chương trình nghiên cứu. Anh/chị có quyền kết thúc phỏng vấn tại bất kỳ thời điểm nào. Anh/chị không phải nói bất cứ thứ gì mà anh/chị không muốn. Anh/chị có quyền đề nghị rút lại hoặc hủy dữ liệu đã được thu thập trước khi tôi công bố chúng. Nếu anh/chị có bất kỳ câu hỏi nào, hãy liên lạc với tôi.

Anh/chị có sẵn lòng tham gia vào cuộc phỏng vấn này không?

□ Có □ Không

________________________ ________________________

Chữ ký người tham gia Thời gian

Phần I: Giới thiệu

Tên:

Giới tính:

Tuổi:

Cấp hàm:

Chức vụ:

Vai trò trong điều tra vụ án:

Phần II: Thông tin chung về vụ án

Anh/chị có thể cung cấp một số thông tin chính liên quan đến vụ án?

Phần III: Câu hỏi chi tiết

A. Phương thức, thủ đoạn phạm tội

Anh/chị có nhận xét gì về phương thức, thủ đoạn mà đối tượng sử dụng trong vụ án?

Đối tượng đã sử dụng cách thức nào để trốn tránh sự phát hiện của lực lượng thực thi pháp luật?

Vai trò của công nghệ được thể hiện trong vụ án như thế nào?

Yếu tố xuyên quốc gia được thể hiện như thế nào trong vụ án?

Anh/chị có nhận xét gì về phương thức, thủ đoạn trong vụ án, khi so sánh với các vụ án khác về tội phạm máy tính chiếm đoạt tài sản?

B. Cấu trúc nhóm

Vai trò của các thành viên trong nhóm được thể hiện như thế nào?

Mức độ chặt chẽ của mối quan hệ giữa các thành viên trong nhóm được thể hiện như thế nào?

Anh/chị hãy nói rõ hơn về người ảnh hưởng có quyền lực cao nhất trong nhóm?

Anh/chị có nhận xét gì về cấu trúc nhóm của mạng lưới tội phạm này, khi so sánh với các vụ án khác về tội phạm máy tính chiếm đoạt tài sản?

Phần IV: Kết luận

Có bất kỳ thông tin nào khác anh/chị muốn bổ sung không?

Anh/chị có phiền nếu tôi liên lạc lại để làm rõ những điểm chưa rõ ràng không?

Trân trọng cảm ơn sự tham gia của anh/chị!

Appendix 5. Network metrics

Cases	Vertices (V)	Density (D)	Average Degree (DC)	Average Closeness Centrality (CC)	Average Betweenness Centrality (BC)
C01	37	0.066	2.378	0.010	33.514
C02	42	0.049	2.000	0.010	30.976
C03	54	0.045	2.407	0.006	60.519
C04	9	0.222	1.778	0.073	3.111
C05	9	0.222	1.778	0.057	5.111
C06	7	0.286	1.714	0.087	3.000
C07	30	0.069	2.000	0.011	32.533
C08	5	0.400	1.600	0.130	2.000
C09	5	0.500	2.000	0.153	1.400
C10	9	0.306	2.444	0.076	2.778
C11	11	0.273	2.727	0.045	6.545
C12	9	0.278	2.222	0.070	3.444
C13	12	0.242	2.667	0.038	8.250
C14	10	0.222	2.000	0.050	5.900
C15	7	0.524	3.143	0.119	1.429
C16	4	0.667	2.000	0.258	0.500
C17	7	0.286	1.714	0.073	4.143
C18	24	0.083	1.917	0.021	13.542
C19	8	0.357	2.500	0.090	2.250
C20	4	0.667	2.000	0.258	0.500

▨	Network for using bank card data for online purchases
🟩	Network for using bank card data to make fake cards
🟦	Network of caller group
□	Network of money mule group

Appendix 6. Core concepts of social network analysis

Concepts	**Contents**
Actor	Actors are participants or members in the collaboration or competition within a social network. They can be called nodes, vertices (V).
Relation	Relations can be called relationships, ties, edges, or links that connect actors in a social network.
Density	Density (D) shows the general level of connectedness among nodes in a graph. It is calculated by the number of actual ties divided by the possible ties within a network.
Degree centrality	Degree centrality (DC) illustrates the number of unique edges that link one actor with the others in a network.
Closeness centrality	Closeness centrality (CC) indicates how close an actor is to all others inside a network. It refers to the index of network cohesion.
Betweenness centrality	Betweenness centrality (BC) measures the extent to which a node influences the communication paths between other nodes.
Broker	Brokers refer to intermediary actors who assist transactions and the flow of information or resources between unconnected actors within a network.
Leader	A leader can be the powerful actor with the "highest cognitive load" or the member who shows the most qualities concerning leadership capacity.

Appendix 7. Criminal roles inside cybercrime networks, recommended by Leukfeldt, Lavorgna, and Kleemans (2017)

Roles	Tasks
Core members	They initiate, direct and/or control other members to implement cybercrime.
Professional enablers	They supply core members with high-quality services such as hacking tools, stolen credit card data.
Recruited enablers	They provide core members with simple services such as information about potential victims.
Money mules	They are responsible for opening bank accounts, receiving illegal money, helping core members avoid financial investigations.

Appendix 8. Ten subject matter experts (SMEs) within cybercrime networks, recommended by Chabinsky (2010)

Roles	Tasks
Coders or programmers	They specialize in writing and designing malware and tools to commit cybercrime.
Distributors or vendors	They are responsible for trading, selling illegal products and software (e.g., stolen data), and guaranteeing these goods provided by others.
Techies	They are in charge of technical infrastructures such as servers, encryption, and bulletproof hosting.
Hackers	They search for and exploit vulnerabilities of information systems and applications to get illegal access.
Fraud specialists	They design and conduct social engineering schemes consisting of spamming, phishing, and domain squatting.
Hosts	They supply the hosting services of illegal content servers and websites, mainly such as elaborate botnets and proxy services.
Cashers	They handle accounts of drops, and provide information about these drops to other criminals for a fee, also manage the operation of money mules.
Money mules	They receive and transfer illegal money from victims to a secure location.
Tellers	They support core cybercriminals to transfer and launder illegal proceeds via digital money services as well as between different national currencies.
Leaders	They keep the highest position at the specialty list as they choose targets, members, manage the operation of the whole group, distribute sources and benefits.

Appendix 9. Categories of cybercrime-related networks, recommended by Choo and Smith (2008) and Broadhurst et al. (2014)

Types of networks	Contents
Traditional organized criminals	They take advantage of cyberspace and technology to enhance their offline criminal behaviors.
Organized cybercriminal groups	They often only operate online, such as underground credit card fraud groups or underground phishing groups.
Ideologically and politically motivated organized cyber groups	They include terrorists and hacktivists who use the Internet and ICTs as a medium for propaganda or to raise funds, collect information as well as recruiting members.
State-sponsored cybercrime groups	They involve state-private interactions, ranging from state's monopoly on cyberattacks to state's ignorance of private cyberattacks.

Appendix 10. Categories of cybercrime networks, recommended by McGuire (2012)

Types of networks	**Contents**
Type I – operate primarily online	
Swarm groups	They are disorganized networks; while they have no clear leadership, they share a common purpose.
Hub groups	They possess a command network, with a hub of core actors surrounded by more peripheral players.
Type II – operate both online and offline activities	
Cluster hybrids	They involve criminals gathering around a small group of individuals and conducting online and offline criminal activities.
Extended hybrids	They are less centralized and more diffuse, and include many members and subgroups.
Type III – operate predominantly offline, but make use of technology to facilitate their crimes	
Hierarchies	They are like traditional criminal groups—such as the Mafia—but transfer their illegal activities to cyberspace.
Aggregates	They are loosely organized and constitute themselves as short-lived groups without clear targets.

Appendix 11. Comparison of cybercriminal behaviors between Vietnamese criminal law and the Budapest Convention

The Budapest Convention	The 2015 Vietnamese 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

The Budapest Convention	**The 2015 Vietnamese Penal Code, amended in 2017**
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 organization'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

Appendix 12. The new typology of cybercrime networks based on the clear degree of leadership

Types of networks	**Contents**	**Specific networks in case studies**
Swarm networks	They operate freely without any leadership, and have high degree of online activity, low centrality	Hacking forums at the start-up stage
Distributed networks	They have one or a few centered actors, but unclear leadership, no agreed upon leader, and high degree of online activity	C01, C03, C05, C07, C08
Single-directed networks	They are organized and led by one leader, suitably for small groups	C04, C06, C09, C10, C19, C20
Group-directed networks	They are organized and managed by a core subgroup of leaders, suitably for big groups	Hacking forums at the mature stage, C02, C11, C12, C13, C14, C15, C16, C17, C18