Trends in Organized Crime (2022) 25:226–247
https://doi.org/10.1007/s12117-021-09422-1

The modus operandi of transnational computer fraud: a crime script analysis in Vietnam

Trong Van Nguyen[1,2]

Accepted: 17 May 2021 / Published online: 9 June 2021

Abstract

This study aims to better understand transnational computer fraud in Vietnam utilizing crime script analysis. 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 transnational computer fraud. 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. Technology can support criminals in defrauding victims transnationally without the need for direct interaction. Moreover, the study clarified the different roles of Vietnamese and foreign offenders in the two types of transnational computer fraud: bank card data fraud and phone scams. As the first study of this nature implemented in Vietnam, this research contributes to the knowledge of computer fraud, especially in Asia, providing a foundation for future investigations related to this kind of cybercrime.

Keywords Transnational computer fraud · Crime script analysis · Bank card data fraud · Phone scams · Vietnam

Introduction

Vietnam is considered one of the emerging operational centers for cybercrime along with Brazil, India, and North Korea (CSIS and McAfee 2018), because it is both host to and victim of transnational cybercrime as evidenced by the unfavorable statistics of cybercrime-related cases originating from and directed at Vietnam (Nguyen 2020). In May 2013, a US$200 million worldwide credit card fraud ring run by Vietnamese criminals was infiltrated through cooperation between

✉ Trong Van Nguyen
trongnv1607@toki.waseda.jp

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

[2] Counter-Cybercrime Police Faculty, People's Police Academy, Hanoi, Vietnam

the High-tech Crime Police (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). Vietnam has recorded notorious cases of transnational computer fraud in which fraudsters located in Vietnam cheated millions of dollars from global victims (HTCP Department 2015, 2017).

Given this serious situation, perceptions surrounding transnational computer fraud in Vietnam are vital. At present, 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. 2017a, b; Leukfeldt, Lavorgna, et al. 2017a, b; Ngo and Jaishankar 2017). However, little information has been published about methods of transnational computer fraud conducted by cybercriminals in Vietnam. The existing literature presents transnational computer fraud as among the most prevalent forms of Internet crime, in which perpetrators develop a scheme using one or more elements of information communication technologies (ICT) to defraud transnational victims (see Nguyen and Luong 2020). Accordingly, technology plays an important part in the modus operandi of transnational computer fraud, which makes its nature different from traditional fraud (Nguyen and Luong 2020). However, previous studies on computer fraud have not discussed in detail the role of technology within its modus operandi. Moreover, while studies on computer fraud are popular in the North American and European context (for example, Holt and Lampke 2010; Hutchings and Holt 2015; Leukfeldt 2014; Leukfeldt, Kleemans, et al. 2017a, b; Peretti 2008; Soudijn and Zegers 2012), there is a dearth of research that analyzes its methods in Asia, especially Vietnam.

Against this backdrop, the present work discusses specific methods employed by cyber fraudsters in the Vietnamese context. Besides presenting the distinctive characteristics of transnational computer fraud in Vietnam, the paper also focuses on technological factors exploited by fraudsters to defraud transnational victims. This paper addresses the question, "How is transnational computer fraud implemented in the Vietnamese context?". To answer this question, the study utilizes crime script analysis of Vietnamese case studies and interviews with cyber police officers. Crime script analysis can provide comprehensive insight into the entire process of crime commission, as well as propose counter-crime strategies (Dehghanniri and Borrion 2019).

This paper includes eight main sections. After the introduction, the context of transnational computer fraud in Vietnam is presented, followed by the extant literature on computer fraud and the current theoretical framework. Next, the methods used to collect and analyze the data are described. The subsequent section presents the findings through the crime scripts of two types of transnational computer fraud, while the final two sections discuss the remarkable characteristics of its modus operandi in Vietnam.

The context of transnational computer fraud in Vietnam

Cybercrime can be viewed as a continuum in which some crimes feature only minor technological elements and others almost entirely technological elements (Gordon and Ford 2006). Representing one specific type of cybercrime, computer fraud or cyberfraud can possess three levels of cybercrime: cyber-assisted, cyber-enabled, and cyber-dependent aspects (Levi et al. 2017; Wall 2005). At the lowest level are cyber-assisted crimes, in which ICT is simply used to assist the crime. Next, cyber-enabled ones are traditional crimes that can be transformed in their scale and degree by the adoption of ICT. At the highest level, cyber-dependent crimes can be conducted only with the use of ICT. This study focuses upon cyber-enabled fraud with two types: bank card data fraud and phone scams.

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, or skimming 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 et al. 2017; Lee 2020). In some situations, therefore, phone scams may be known as "voice phishing" or "vishing" (Lee 2020). In Vietnam, the term "phone scam" is predominantly applied to one type of computer fraud in which computers (or other digital devices) and the Internet are used to conduct fraudulent "Voice over Internet Protocol" (VoIP) calls to gain access to victims' money (Nguyen and Luong 2020). This study examines the entire process of computer fraud: before, during, and after cyber fraudsters obtain money from transnational victims of bank card fraud and phone scams in Vietnam.

Vietnamese criminal policy clearly distinguishes computer fraud from traditional fraud. Computer fraud, regulated by Article 290 of the 2015 Penal Code, involves high-technology 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. The high-technology factor means cybercrime can fall under stricter penalties compared with respective traditional crime. Moreover, the Vietnamese Government has recently shown a strong determination to cooperate with the international community in combatting transnational cybercrime (Nguyen 2020). By ratifying international instruments, such as the 2000 United Nations Convention against Transnational Organized Crime, the 2003 Cybersecurity Strategy of APEC, and the ASEAN Declaration to Prevent and Combat Cybercrime presented at the 31st ASEAN Summit, Vietnam adopted international standards into its domestic criminal legislation related to transnational cybercrime. Accordingly, transnational crime is defined as involving more than one state in its preparation, planning, direction, control, execution, or impact (Thuan 2018). Combatting transnational cybercrime and ensuring cybersecurity are currently among the highest priorities of the Vietnamese police force (Lam 2020).

However, Vietnam is still one of the countries facing the worst publicity related to cybercrime, especially computer fraud (Lusthaus 2020; Nguyen 2020). In recent years, transnational computer fraud utilizing various crime scripts has become an increasing threat in Vietnam (Ministry of Public Security 2020). 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 as *vefamily, hkvfamily*, and *vietexpert,* were used as "virtual meeting points" for hackers and potential criminals (HTCP Department 2010, 2011, 2014, 2015). Vietnam is one of the top countries in terms of hacking capabilities, in which the local community of "black hat" hackers 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). More recently, Vietnam has had to cope with an increasing number of phone scams (Ministry of Public Security 2020). In the first half of 2020, the country's police forces received 776 reports about computer fraud, which caused the loss of trillions of Vietnamese Dong (VND) (Ministry of Public Security 2020). Remarkably, 65% of these reports were related to phone scams in which offenders pretended to be law enforcement officials to defraud victims (Ministry of Public Security 2020). To cope with transnational computer fraud, suitable counter-strategies must be designed and put into practice. However, the lack of knowledge on its modus operandi may hinder the fight against this crime. Filling this gap can assist law enforcement agencies (LEAs) in Vietnam and other countries to both prevent and investigate transnational computer fraud as it has become a global threat.

Commission of computer fraud

Cyber fraud has become a global threat due to the widespread application of ICT (The National Fraud Center 2000). The unprecedented ICT revolution has allowed the remote commission of cyber fraud, via the Internet and wireless communications. Cyber fraudsters no longer need to travel cross-border with visas and passports to approach victims; however, they 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). To explore the nature of computer fraud, 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, et al. 2017a, b; 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. At least two types of criminal networks commit Internet 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, et al. 2017a, b). However, few studies have presented an in-depth discussion of the role of technology in defrauding the cross-border victims of transnational computer fraud, particularly in the Asian context.

Credit card fraud is among the prevalent forms of cyber fraud that have received scholarly attention. 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. Fraudsters use online forums as "offender convergence settings," where cybercriminals meet to buy and sell stolen data (Holt 2013; Holt and Lampke 2010). 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 2013; Holt and Lampke 2010; 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 when compared with traditional fraud (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 South Korea; however, the author did not discuss how victims are defrauded, which is one of the main stages of cyber fraud.

As one type of transnational cybercrime, cyber fraud attacks can be conducted from anywhere worldwide 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. Transnational computer fraud has become a real threat to some developing Asian countries like Vietnam (Broadhurst and Chang 2012; Lusthaus 2020; Nguyen 2020). Foreign cyber fraudsters attack Vietnamese victims, while domestic fraudsters attack foreign victims (Nguyen 2020; Nguyen and Luong 2020). 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 transnational computer fraud in the Vietnamese context: bank card fraud and phone scams.

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). These components generalize the modus operandi of a crime with a sequential flow (Cornish 1994).

Crime script analysis is not simply a descriptive tool; it also supports the development of effective situational crime prevention strategies (Dehghanniri and Borrion 2019). By identifying key scenes, crime script analysis supports LEAs to clarify and intervene in the weak spots of a crime with the purpose of changing potential offenders' acknowledgment of its rewards and risks (Dehghanniri and Borrion 2019). Owing to these advantages, crime script analysis has been increasingly applied in the analysis of both territorial crime and cybercrime (see Dehghanniri and Borrion 2019). It has also been adopted in the analysis of some forms of cyber fraud, such as phishing (Leukfeldt 2014), identity fraud (Lee 2020), and credit card fraud (Meijerink 2013; van Hardeveld et al. 2016).

As mentioned above, international research on computer fraud has focused mainly on the American and European contexts; however, little is known about computer fraud in Asia, especially in Vietnam, which serves as a cybercrime hub in the region. More research into the modus operandi of computer fraud is required to map counter-strategies. As a follow-up to the extant studies on cyber fraud, the present study utilizes crime script analysis to clarify two types of transnational computer fraud in the Vietnamese context. In particular, it aims to explore how cyber fraudsters are involved in criminal activities, as well as what tools and techniques are used to defraud transnational victims. Examining these processes may assist LEAs in the design and application of counter-crime strategies against transnational computer fraud.

Method

This study applied a multiple qualitative approach to analyze the modus operandi of transnational computer fraud. Data were extracted from 20 case studies and in-depth interviews with 14 cyber police officers at both central and provincial levels. Crime script analysis was then used to clarify the process of Internet fraud commission.

There is no central registration system in Vietnam that provides a quick overview of all criminal cases; therefore, case studies were selected via snowball sampling. Using the Police Academy's personnel database, the author asked Vietnamese cyber police officers whether they knew of any transnational computer fraud cases investigated by their organization or other organizations between 2010 and 2018. Through their recommendations, the researcher established relationships with investigators responsible for these cases. Thereafter, with official authorization letters signed by the Director of the Police Academy, the researcher could access the investigation files, including both confidential and public documents. Semi-structured interviews were conducted with the investigators who were responsible for these cases.

In total, the author obtained 20 cases that were investigated by the HTCP Forces between 2010 and 2018. Nine cases were investigated at the central level by the HTCP Department (now the Department of Cybersecurity and Counter

High-tech Crime) and 11 cases were processed by provincial police forces. The modus operandi of these 20 cases can be divided into bank card data fraud and phone scams (see Table 1). The 12 cases of bank card data fraud can be further divided into two sub-categories: using bank card data for online purchases and producing counterfeit cards.

Data collection was complemented by semi-structured interviews conducted with 14 cybercrime investigators. Among the investigators, one had covered two cases, two had been involved in three cases, and the rest had conducted one case each. In-depth interviews provided primary data, which was supplemented with the data from official documents. Some participants shared valuable information that was not shown in the investigation documents. All participants were informed of the study purpose and gave their oral/written consent to take part. To respect human rights and protect confidentiality, all real names of cases, suspects, and interviewees were coded with letters and numbers.

As a foundational method of qualitative analysis, thematic analysis is widely used to identify, analyze, and report themes (or patterns) in research (Braun and Clarke 2006; Joffe and Yardley 2004). In this study, an inductive approach was applied to find patterns for analyzing the modus operandi of transnational computer fraud. As such, six phases recommended by Braun and Clarke (2006) were employed to define and analyze the themes. Adapting the suggestions from Cornish's (1994) crime script analysis, with appropriate adjustments to link to the current data, the three final themes were "preparation," "activity," and "post-activity," which represent certain primary stages (or "script scenes") of crime commission. At each stage, cyber 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" (see Table 2).

Findings

The crime scripts of the two forms of transnational computer fraud in Vietnam are shown in Table 2.

Table 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 produce counterfeit cards	
C02, C11, C12, C14, C15, C16, C17, C18	Phone scams	

Table 2 Modus operandi of transnational computer fraud

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 - Prepare tools for obtaining illegal money	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
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

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, Kleemans, et al. 2017a, b; Peretti 2008), did not exist among the Vietnamese sample cases in the present study. In Vietnam, culprits obtained bank card data directly from automated teller machines (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; thus, 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 few 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; however, 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 point-of-sale (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 were 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, et al. 2017a, b). 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 (2017a, b) 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. Therefore, 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, cyber 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 cyber 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 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 1 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 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 Fig. 2).

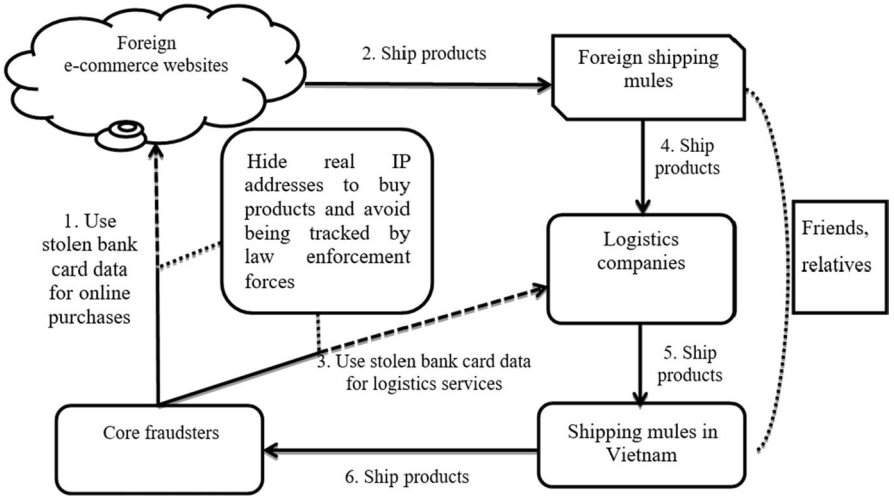

Fig. 1 Crime scripts of bank card data fraud for online purchase at the "activity" stage

Fig. 2 A shipping label in case C03

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

Stolen bank card data were 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 one Chinese leader. 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 transnational computer fraud. 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.

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 conduct scam VoIP calls to victims. According to Leukfeldt, Kleemans, et al.'s (2017a, b) 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 they could be recruited from migrant laborers living in Mainland China or Taiwan.

There was little detailed information about how fraudulent callers were 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—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 conduct 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 (Leukfeldt, Kleemans, et al. 2017a, b; Leukfeldt, Lavorgna, et al. 2017a, b; Soudijn and Zegers 2012). 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 online and offline processes, 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, et al. 2017a, b).

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 South 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 Fig. 3). 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.

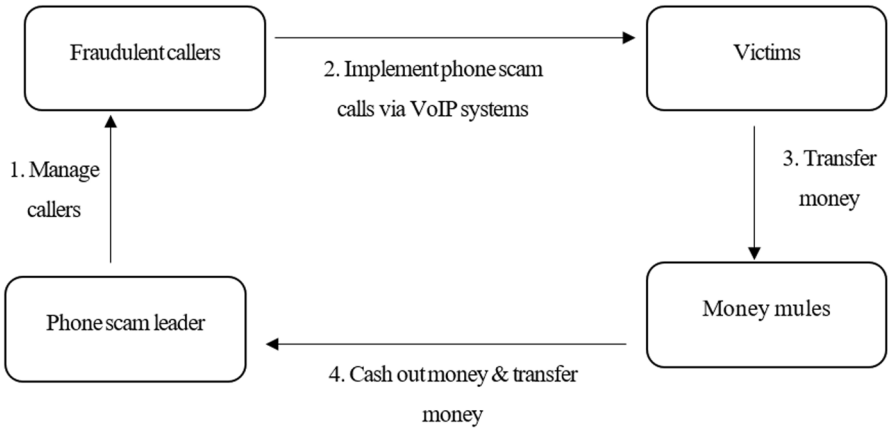

Fig. 3 Crime scripts of standard phone scams at the "activity" stage

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

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 Fig. 3). 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.

Discussion

Vietnam: An operational base for domestic and foreign cyber fraudsters

Vietnam can be regarded as an operational base for cybercrime, posing one of the most serious criminal threats in Southeast Asia (CSIS 2018; Lusthaus 2020; Nguyen 2020). This position is reinforced by both local and foreign cyber 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 few 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, et al. 2017a, b; 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 cyber fraud networks. Bank card data buyers can use data for online purchases, or resell it to others for 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 transnational computer fraud is the result of multiple factors, such as the rapid development of ICT and the slow progress of LEAs in crime suppression (Nguyen 2020). 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 (Nguyen 2020). 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 (Nguyen 2020). 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 normal

individuals into cybercriminals who are not specialized in ICT but can obtain illegal money via virtual space.

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, cyber 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, transnational computer fraud 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. Like the concept of "old wine in new bottles," technology enables fraudsters to call victims from other countries using fake phone numbers. As per the continuum illustrated by Gordon and Ford (2006), transnational computer fraud 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, Kleemans, et al. 2017a, b), there is a strict correlation between the extent of the technology used and the interaction between offenders and victims. Compared with bank card fraud, phone scams require a lower degree of technology but feature a higher degree of interaction between offenders and 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 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 victims (Hutchings and Holt 2015), which means that technology plays an important role in the indirect interaction between them (Leukfeldt, Kleemans, et al. 2017a, b).

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 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.

Conclusion

This study elucidated the process of transnational computer fraud in Vietnam using crime script analysis to examine two types of crime: bank card data fraud and phone scams. Vietnam is likely to become an operational base for both domestic and foreign criminals to conduct Internet fraud. The study found that transnational computer fraud, as an intersection between fraud, technology, and transnationality, does not require a direct interaction between offenders and victims. There are also certain big differences in the modus operandi between bank card fraud and phone scams: bank card fraud requires greater use of technology, and both types involve different roles of Vietnamese and foreign offenders.

The study has practical implications for counter-cybercrime strategies. First, the borderless nature of cybercrime means international cooperation must be a central part of LEAs' counter-crime strategies. Without close international cooperation among LEAs, transnational computer fraud cannot be eradicated as technology enables cybercriminals to easily commit it. Second, counter-cybercrime strategies should emphasize prevention methods that raise citizens' awareness. Any individual can become a potential victim of transnational computer fraud, while investigations surely face many obstacles because of the transnational and contactless characteristics of this crime. Third, awareness-raising activities should aim to hinder the recruitment of auxiliaries, especially money mules. Some members of transnational computer fraud networks are not aware of their criminal behaviors. Lastly, according to Vietnam's criminal policies, proving the members' awareness of their criminal

purpose is important in deciding whether they bear legal responsibility; therefore, LEAs must be fastidious in clarifying members' awareness.

Although the study provided a unique view of computer fraud, there are some limitations. First, the data were obtained through investigation files, which can be influenced by investigators' opinions and the limited abilities of LEAs. Furthermore, there was an issue with missing data because of the international dimension of the cases since many foreign fraudsters and victims could not be identified. Limited information on certain aspects of the crime scripts of transnational computer fraud, such as recruitment of fraudulent callers, sourcing of lists of potential victims' phone numbers, and fleeing should be clarified. In future research, it may be beneficial to interview cyber fraudsters to clarify and refine these crime scripts. Finally, the findings of this study might not be generalizable to other types of computer fraud or to other countries, as only two types of transnational computer fraud—bank card data fraud and phone scams—were analyzed in the Vietnamese context. Future research on this topic should consider other data sources, methods, and related contexts.

Acknowledgements I would like to thank Prof. Ken Miichi (Waseda University) for his advice and his comments on earlier versions of the article. Besides, I also sincerely thank the anonymous reviewers for their comments and suggestions.

Funding This study was funded by Japan International Cooperation Agency (JICA).

Declarations

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

Consent to participate Informed consent was obtained from all individual participants included in the study.

Consent to publish Additional informed consent was obtained from all individual participants for whom identifying information is included in this article.

Conflicts of interest The author declares no potential conflicts of interest.

References

Bossler AM, Berenblum T (2019) Introduction: New directions in cybercrime research. J Crime Justice 42:495–499. https://doi.org/10.1080/0735648X.2019.1692426

Braun V, Clarke V (2006) Using thematic analysis in psychology. Qual Res Psychol 3:77–101

Broadhurst RG, Chang LYC (2012) Cybercrime in Asia: Trends and challenges. In: Liu J, Hebenton B, Jou S (eds) Handbook of Asian Criminology (pp. 49–63). Springer, New York. https://doi.org/10.1007/978-1-4614-5218-8_4

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

Cornish D (1994) The procedural analysis of offending and its relevance for situational prevention. Crime Prev Stud 3:151–196

CSIS, McAfee (2018) Economic impact of cybercrime - No slowing down. Available via https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf. Cited 16 Oct 2020

de Bie JL, de Poot CJ, van der Leun JP (2015) Shifting modus operandi of Jihadist foreign fighters from the Netherlands between 2000 and 2013: A crime script analysis. Terror Pol Violence 27:416–440. https://doi.org/10.1080/09546553.2015.1021038

Dehghanniri H, Borrion H (2019) Crime scripting: A systematic review. Eur J Criminol:1–22. https://doi.org/10.1177/1477370819850943

FBI (2013) Leader in $200 million international stolen data ring charged in New Jersey as part of worldwide takedown. Available via 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. Cited 21 Oct 2020

Flitter E (2013) Global $200 million credit card hacking ring busted. *Reuters*. Available via https://www.reuters.com/article/us-cybercrime-hacking-arrests/global-200-million-credit-card-hacking-ring-busted-idUSBRE95419G20130605. Cited 20 Jan 2021

Goodman M (2010) International dimensions of cybercrime. In: Ghosh S, Turrini E (eds) Cybercrimes: A multidisciplinary analysis (pp. 311–339). Springer, Heidelberg. 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. Available via https://www.thinkwithgoogle.com/_qs/documents/6730/Report_e-Conomy_SEA_2018_by_Google_Temasek_v.pdf. Cited 20 Jan 2021

Gordon S, Ford R (2006) On the definition and classification of cybercrime. J Comput Virol 2:13–20. https://doi.org/10.1007/s11416-006-0015-z

Hao S, Borgolte K, Nikiforakis N et al. (2015) Drops for stuff: An analysis of reshipping mule scams. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 1081–1092). https://doi.org/10.1145/2810103.2813620

Holt TJ (2013) Exploring the social organisation and structure of stolen data markets. Glob Crime 14:155–174. https://doi.org/10.1080/17440572.2013.787925

Holt TJ, Lampke E (2010) Exploring stolen data markets online: Products and market forces. Crim Justice Stud 23:33–50. https://doi.org/10.1080/14786011003634415

HSN Consultants (2019) The Nilson report. Available via https://nilsonreport.com/upload/content_promo/The_Nilson_Report_Issue_1164.pdf.m. Cited 20 Jan 2021

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

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

Hutchings A, Holt TJ (2015) A crime script analysis of the online stolen data market. Br J Criminol 55:596–614. https://doi.org/10.1093/bjc/azu106

IMPERVA (2008) SQL Injection 2.0. Available via https://pdfs.semanticscholar.org/9e33/338f42d2d97349063cf24db36a74936f0613.pdf. Cited 20 Jan 2021.

Joffe H, Yardley L (2004) Content and thematic analysis. In: Marks D, Yardley L (eds) Research methods for clinical and health psychology. SAGE, Riverside County, pp 56–69

Lam T (2020) Bao dam an ninh mang trong tinh hinh moi [Ensure cybersecurity in the new situation]. Vietnam Communist Party's Central Committee. Available via https://www.tapchicongsan.org.vn/web/guest/tin-tieu-diem/-/asset_publisher/s5L7xhQiJeKe/content/bao-dam-an-ninh-mang-trong-tinh-hinh-moi. Cited 25 Jan 2021

Lee CS (2020) A crime script analysis of transnational identity fraud: Migrant offenders' use of technology in South Korea. Crime Law Soc Change 74:201–218. https://doi.org/10.1007/s10611-020-09885-3

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

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

Leukfeldt ER, Lavorgna A, Kleemans ER (2017) Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. Eur J Crim Pol Res 23:287–300. https://doi.org/10.1007/s10610-016-9332-z

Levi M, Doig A, Gundur R, Wall D, Williams M (2017) Cyberfraud and the implications for effective risk-based responses: Themes from UK research. Crime, Law and Soc Change 67:77–96. https://doi.org/10.1007/s10611-016-9648-0

Lusthaus J (2020) Cybercrime in Southeast Asia: Combating a global threat locally. Available via https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-05/Cybercrime%20in%20Southeast%20Asia.pdf?naTsKQp2jtSPYsWpSo4YmE1sVBNv_exJ. Cited 19 Jan 2021

Meijerink TJ (2013) Carding: Crime prevention analysis. Available via http://purl.utwente.nl/essays/63027. Cited 18 Jan 2021.

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]. Available via 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. Cited 20 Oct 2020

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. Int J Cyber Criminol 11:1–9. https://doi.org/10.5281/zenodo.495762

Nguyen T, Luong HT (2020) The structure of cybercrime networks: Transnational computer fraud in Vietnam. J Crime Justice 1–22. https://doi.org/10.1080/0735648X.2020.1818605

Nguyen TV (2020) Cybercrime in Vietnam: An analysis based on routine activity theory. Int J Cyber Criminol 14:156–173. https://doi.org/10.5281/zenodo.3747516

Peretti K (2008) Data breaches: What the underground world of carding reveals. Santa Clara High Technol Law J 25:375–413. Available via https://core.ac.uk/download/pdf/149256649.pdf. Cited 20 Jan 2021

Shin S-C (2018) An analysis on the activities of Taiwanese voice phishing crime organizations in Korea. JAS 21:151–192. https://doi.org/10.21740/jas.2018.08.21.3.151

Soudijn MRJ, Zegers BCHT (2012) Cybercrime and virtual offender convergence settings. Trends Organ Crime 15:111–129. https://doi.org/10.1007/s12117-012-9159-z

The Internet Society (2017) Paths to our digital future. Available via https://future.internetsociety.org/2017/wp-content/uploads/sites/3/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf. Cited 20 Jan 2021

The National Fraud Center, Inc (2000) The growing global threat of economic and cyber crime. Available via https://www.utica.edu/academic/institutes/ecii/publications/media/global_threat_crime.pdf. Cited 20 Jan 2021

Thuan NT (2018) Toi pham co to chuc xuyen quoc gia va Cong uoc Palermo nam 2000 [Trasnational organized crime and the Palermo Convention of 2000]. Legis Stud 23:3–10. Available via http://lapphap.vn/Pages/tintuc/tinchitiet.aspx?tintucid=208308. Cited 20 Jan 2021

Tropina T (2012) The evolving structure of online criminality. EUCRIM 4:158–165. Available via http://www.corteidh.or.cr/tablas/r15111.pdf. Cited 20 Jan 2021

van Hardeveld GJ, Webber C, O'Hara K (2016) Discovering credit card fraud methods in online tutorials. Proceedings of the 1st International Workshop on Online Safety, Trust and Fraud Prevention 1–5. https://doi.org/10.1145/2915368.2915369

Wall DS (2005) The Internet as a conduit for criminal activity. In: Pattavina A (Eds) Information technology and the criminal justice system pp 77–98, SAGE, California