Cybercrime in Vietnam: An Analysis based on Routine Activity Theory

Trong Van Nguyen[1]
Waseda University, Japan

Abstract

Principally driven by a phenomenal increase in Internet users, Vietnam, amongst all the countries in Southeast Asia, leads with its gross merchandise value share in the GDP. However, Vietnam is regarded as not only a cybercrime center, but is also among countries hardest hit by targeted attacks. This study explores the context of cybercrime in Vietnam through published and unpublished reports of certain organizations. Subsequently, by adopting the Routine Activity Theory (RAT) based on three core factors, the study will examine the causation of cybercrime originating from Vietnam's social situation and will conclude by highlighting the significance of this theory in cyberspace.

Keywords: Cybercrime, High-tech Crime, Cybersecurity, Routine Activity Theory, Vietnam.

Introduction

The availability of the Internet coupled with powerful computing and communication in portable forms has been creating a technological evolution, influencing not only technical fields but also many aspects of the society (Leiner et al., 1997), especially in Vietnam, which has experienced a phenomenal growth in the Internet penetration rate. Within two decades of the Internet officially launching in Vietnam, the penetration rate reached 65.7% of the total population, or about 64 million users (Internet World Stats, n.d.). Moreover, the Vietnamese government has identified information and communications technology (ICT) as a key factor in developing the country and has clarified specific targets to transform Vietnam into an advanced ICT country by 2020 (BMI, 2016). 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 & Temasek, 2018).

However, the expansion of ICTs and increased Internet penetration have also raised concerns about cybercrime (Symantec, 2018). Increasingly, offenders take advantage of the convenience, speed, and anonymity of the Internet to indulge in a wide range of cybercrime, resulting in serious harm to victims worldwide (INTERPOL, 2018). Vietnam is no exception; it has coped with malicious acts in cyberspace from both internal and external territory (Dai, 2017). Although the Vietnamese government has stepped up efforts to secure

[1] PhD Candidate, Graduate School of Asia-Pacific Studies, Waseda University, 1-21-1 Nishiwaseda, Shinjuku, Tokyo, Japan. Email: trongnv1607@toki.waseda.jp

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). In February 2018, the Center for Strategic and International Studies (CSIS), in collaboration with McAfee, released a report which characterized Vietnam as a cybercrime center, along with other countries, including Brazil, India, and North Korea (CSIS, 2018).

To control and prevent cybercrime, researchers have attempted to understand the causation of cybercrime. In criminology, various theories have been developed to comprehensively elucidate the root causes of criminal behaviors in cyberspace. Despite some arguments, the RAT initially recommended by Lawrence E. Cohen and Marcus Felson for analyzing traditional crime has also been used to explain the causation of cybercrime. Yar (2005) states that the RAT might not be suitable to explain cybercrime as cyberspace is spatio-temporally "disorganized," whereas Grabosky (2001) suggests that individual incidents, as well as long-term trends of both conventional crime and cybercrime, can be explained by three factors: motivation, opportunity, and the lack of capable guardians. Eck and Clarke (2003) also suggest that the RAT can be expanded to explain crimes in cyberspace as they classify two connected dimensions: the behaviors of parties involved (offenders and targets), and the environment (network). Most empirical research to date attempt to use the RAT to explain certain typical categories of cybercrime at the individual level such as Internet fraud (Pratt, Holtfreter, & Reisig, 2010; Wilsem van, 2011), malware infection (Choi, 2008; Bossler & Holt, 2009), and ATM hacking (Hsieh & Wang, 2018). Kigerl (2011) is among the very few researchers explaining the victimization and criminalization of cybercrime at the national level. Moreover, currently, little is known about the causation of cybercrime in Southern Asian settings under the RAT.

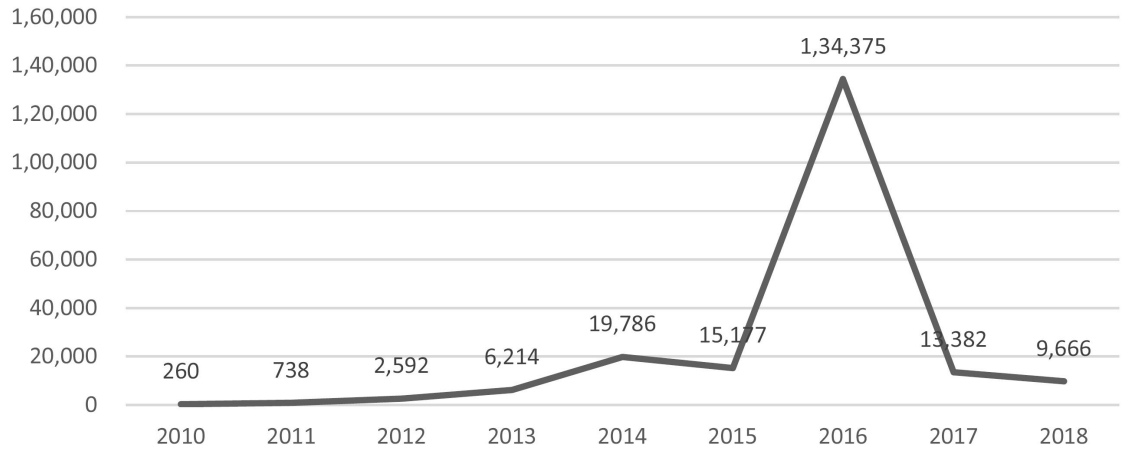
This study seeks to analyze the current situation of cybercrime in Vietnam, based on both published and unpublished reports of some international and domestic organizations. Subsequently, this paper will adopt the RAT based on three necessary factors — *likely offenders, suitable targets,* and the *absence of capable guardians* — to discuss the causation of cybercrime in Vietnam's social situation. Primarily, it will answer two questions: How much do dimensions inside each factor influence cybercrime in Vietnam? What is the most important factor in solutions against cybercrime? By reviewing some research results regarding the RAT, it also concludes whether or not the RAT can be applied to cybercrime in cyberspace. Therefore, this article seeks to contribute to the current debate regarding the use of RAT to elucidate cybercrime.

1. Vietnam's Cybercrime Context

Vietnam is among the top countries in the world to suffer a negative reputation concerning cybersecurity. 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; 2018c; 2018d). The country was listed among the top ten countries in the world with the highest malware encounter and infection rates for the period from July 2015 to June 2016 (Microsoft, 2015; 2016). It maintained the 3rd position among the top 25 countries in the world with the highest number of suspected botnet IPs in 2016-2017 (Botnet statistics for the year of 2016, 2017; 2018). It was ranked 3rd in 2017, 4th in 2018 in the list of spamming countries, and 6th among countries targeted by malicious mailshots in 2018 (Vergelis, Shcherbakova, & Sidorina, 2019).

Additionally, Vietnam is among the countries hardest hit by targeted attacks. Symantec (2018) ranked Vietnam 9th 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, & Chen, 2018). In 2017, Vietnam was ranked 3rd among countries attacked by encryptors, with 1.95% of users attacked, and 6th 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 5th 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).

Figure 1. Cyber-attacks on Vietnamese Websites Recorded by VNCERT (2010 - 2018)



Note. Data from (APCERT, 2019)

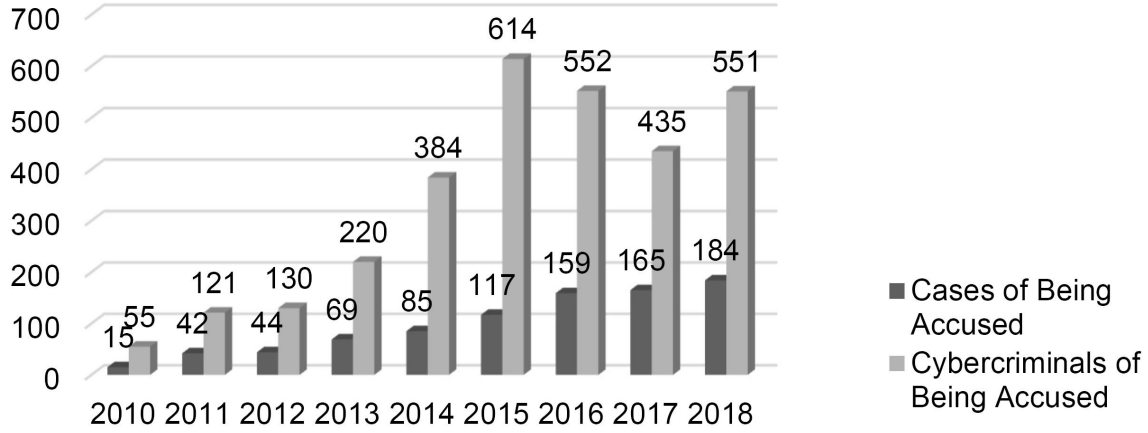
In addition to the data from international sources, some domestic organizations in Vietnam also monitor and produce statistics on malicious activities in cyberspace. The Vietnam Computer Emergency Response Team (VNCERT) recorded over 200,000 cyber-attacks on Vietnamese websites from 2010 to 2018 (*See Figure 1.*). In 2016, when the information systems of Vietnam's airports were first compromised, cyber-attacks spiraled upwards to 134,375 incidents.

The number of cybercrime cases investigated by the High-tech Crime Police 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 2.*). On an average, the number of accomplices was more than three persons per case during the 2010-2018 period. The standard interpretation of "organized crime" regulated in the UN Palermo Convention was formed on the basis of the participation of three or more persons (UN, 2004). Hence, analyzing the average number of cybercriminals per case can prove the organizational characteristic of cybercrime in Vietnam. Besides, one of the most

popular tricks in "cases of being accused" is computer fraud in which fraudsters use stolen foreign bank card information to purchase products, software, online tickets, or making fake bank cards to draw money (High-tech Crime Police Department, 2010; 2013; 2014; 2015). The syndicates of *mattfeuter, vefamily, vietexpert, hkvfamily* with thousands of online members used this trick to steal money from global victims (High-tech Crime Police Department, 2010; 2013; 2014).

In conclusion, based on some reports of international organizations, Vietnam has a bad reputation for certain criteria of cybersecurity such as sources of cyber-attacks or spam, countries targeted by malicious mailshots, and malware infection. The data provided by both domestic and international organizations show that Vietnam has faced cyber threats from both within its territory and outside. 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 High-tech Crime Police Forces. 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.

Figure 2. The Number of Cybercrime Cases and Cybercriminals of being Accused in Vietnam (2010-2018)



Note: Data from High-tech Crime Police Department (2010; 2011; 2012; 2013; 2014; 2015; 2016; 2017) & Department of Cybersecurity and Combating High-tech Crime (2018).

2. Routine Activity Theory

Felson and Cohen firstly presented the RAT for analyzing predatory crime rate change in the U.S. in the 1947-1974 period. Subsequently, the RAT has been broadly applied to 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 & Felson, 1979).

Taking into account a consensus on using the RAT to explain cybercrime, this paper will adopt the theory for analyzing the causation of cybercrime in Vietnam's social situation. Possibly, the degree of the importance of dimensions inside each factor is not similar for various kinds of cybercrime, but overall, the occurrence of crime includes all three factors — *likely offenders, suitable targets,* and *the absence of capable guardians*. Using published as well as unpublished reports with specific cybercrime cases, this paper will review some

results of researches of the RAT to explain the occurrence of cybercrime in Vietnam based on the existence of all three necessary factors.

2.1. 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 & Felson, 1979). It means that there are potential offenders out there seeking 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 & 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 the 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, n.d.). 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 High-tech Crime Police Forces 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 Van Tien Tu from 2009 to 2013 (High-tech Crime Police Department, 2013). Besides, *vefamily.com* operated from 2008 to 2010 with over 2,000 members and about 500,000 reports (High-tech Crime Police Department, 2010). The content of this site was divided into 11 sub-forums related to hacking (High-tech Crime Police Department, 2010). Additionally, v*ietexpert.info* which was managed by Huynh Phuoc Man from 2011 to 2014 had about 3,000 members (High-tech Crime Police Department, 2014). The site had nine sub-forums with over 955,000 reports which helped members discuss hacking skills and exchange tools of cybercrime (High-tech Crime Police Department, 2014). *Hkvfamily.info* which was managed by Pham Thai Thanh 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 (High-tech Crime Police Department, 2014). The availability of online hacking forums could provide members with a tremendous source of knowledge and tools to commit cybercrime.

The 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 (Nexusguard, 2017; 2018a; 2018b; 2018c; 2018d) (Vergelis, Shcherbakova, & Sidorina, 2019). Therefore, unemployment is not significantly related to cybercrime in Vietnam.

The RAT is combined with the 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, 2018). The European Cybercrime Center (2014) includes 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 "Ponzi scheme" 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 (High-tech Crime Police Department, 2011). In the *muaban24* case, fraudsters used the "Ponzi scheme" to steal over US$31.5 million from investors (High-tech Crime Police Department, 2012).

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. 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 dispute (High-tech Crime Police 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 (High-tech Crime Police Department, 2016). It is assumed that the cyber-attacks on Vietnam's airports were "politically-colored" (Goel, 2016). A China-based hacking group called 1937CN, which had previously attacked websites in Vietnam and the Philippines, 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 (High-tech Crime Police 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 law enforcement agencies. The nature of cybercrime, which is committed through cyberspace, reduces the ability of prosecution for cybercriminals (Granja & Rafael, 2017). Cybercrime is significantly under-reported across the globe (ISACA, 2019). 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 the 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. However, to prevent cybercrime, it is not easy to change the conditions influencing likely offenders. For example, it is nearly impossible to reduce Internet users and online benefits in modern society because the expansion of ICT leads to an increasing number of Internet users and online benefits. Therefore, solutions originating from likely offenders are difficult to provide an efficient result in combating cybercrime in Vietnam.

2.2. Suitable Targets

Incitement of likely offenders cannot supply a sufficient condition for turning criminal intentions into illegal activities (Cohen & 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. The RAT clarifies suitable targets as a person, an object or a place with four dimensions — value, inertia, visibility, and accessibility. 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 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 & Felson, 1979). In the *vefamily* case, during interrogation by investigators, Vuong Huy Long confessed that he used SQL Injection 2.0 as a tool to illegally access certain foreign websites to steal bank card data of customers, but he could not exactly identify the valuation of these bank card accounts (High-tech Crime Police Department, 2010). The most important issue which he was concerned about was whether or not the stolen bank card information could be *"alive"* (usable); therefore, before selling or using stolen data, he used some tools to check the situation of the bank card data including "Support Check CVV From Wallet 2009," and "Cong Cu Ho Tro Fake Proxy Sock Nhap Info CC Nhanh" (High-tech Crime Police Department, 2010). However, he was aware that credit card data could bring him a huge

amount of money because each *alive* card data could cost US$0.30-2.00 and they could be used to get the money of card owners (High-tech Crime Police 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 (High-tech Crime Police Department, 2014; 2015; 2016; 2017; Department of Cybersecurity and Combating High-tech Crime, 2018). 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 all 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 & 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 64 million users (Internet World Stats, n.d.). Vietnam demonstrated impressive progress in the number of social media users, with an annual 20% increase, ranking 6th worldwide (We Are Social & 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, Holtfreter, & Reisig, 2010; Wilsem van, 2011). Pratt et al (2010) prove the association between the hours spent online and the odds of Internet 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 & 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 Vietnam police investigated are not Vietnamese, but from foreign countries such as the

U.S., the U.K., Australia, Canada, and China (High-tech Crime Police 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 U.S., the U.K., 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, Shari, Kabir, & Al-Maimani, 2012; Chowdappa, Lakshmi, & Kumar, 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 & 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 has applied additional ICT to many aspects of the society. Expanding information systems in Vietnam without capable guardians will result in more suitable targets for likely offenders to execute cyber-attacks.

2.3. Absence of Capable Guardians

The presence of capable guardians is believed to prevent likely offenders from deciding to commit crimes (Cohen & 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 & Holt, 2009; Williams, 2016).

Although the development of Vietnam's 2018 Global Cybersecurity Index (GCI) illustrates an increasing commitment to cybersecurity (ITU, 2018), vulnerability to cyber-attacks was still grave in the absence of national guardians. In 2017, Vietnam was listed in the "initiating stage" group of countries for introducing moves to preserve cybersecurity (ITU, 2017). According to an evaluation of the 2017 GCI, Vietnam had only four

indicators labeled "green" (good), two indicators classified as "yellow" (medium), and the 19 remaining indicators tagged "red" (bad) (ITU, 2017). The progress of Vietnam in 2018 helped the country to be categorized among the "medium countries" group (ITU, 2018). 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. The positive progress coincided with a reduction in the number of cyber-attacks recorded by VNCERT in 2018 (APCERT, 2019). 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 (High-tech Crime Police 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 (High-tech Crime Police 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 (High-tech Crime Police 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 (High-tech Crime Police 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, amended in 2017, and the 2018 Cybersecurity Law closed the loopholes, which is expected to create a positive country-level guardianship against cybercrime in Vietnam.

Being a formal guardian, the Ministry of Public Security has two main entities dedicated to cybercrime and cybersecurity, including High-tech Crime Police Department and the Cybersecurity Department. High-tech Police Forces are specialized in preventing and investigating cybercrime, including, for example, computer fraud, malware distribution, and DDoS attacks. The High-tech Crime Police Department in 2010 officially marked a milestone in combating cybercrime. Subsequently, the High-tech Crime Police Forces were established at the Provincial Police level of 31 provinces (in all 63 provinces of Vietnam) (as of November 30, 2017) (High-tech Crime Police Department, 2017). The Cybersecurity Department which was officially established in 2014 oversees the management and administration of information system security and cybersecurity related to sovereignty. In 2018, the Cybersecurity Department and the

High-tech Crime Police Department merged into the Department of Cybersecurity and Combating High-tech Crime. Additionally, the Ministry of Information and Communications has some agencies which perform the role of government administration in cybersecurity. For example, the Vietnam Computer Emergency Response Team (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.

In the fight against cybercrime, the Vietnam police have faced challenges including technical snags, lack of human resources, financial problems, and cooperation issues (High-tech Crime Police 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 & 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 (High-tech Crime Police Department, 2013; 2016), 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 (High-tech Crime Police Department, 2016; 2017). Two 15-year-old hackers launching cyber-attacks on Vietnam's airports in 2017 were only charged with administrative violations.

However, the significant role of the High-tech Crime Police Forces to combat cybercrime is ostensible. Since the foundation, High-tech Crime Police 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 (High-tech Crime Police 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 (High-tech Crime Police Department, 2010). The Vietnam police established and employed two investigative operations to arrest nine culprits (High-tech Crime Police Department, 2010). Subsequently, the rate of frauds reduced visibly, and VISA and MasterCard continued to accept transactions (High-tech Crime Police Department, 2010). Therefore, the strong suppression of High-tech Crime Police 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 (M.T, 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.

Conclusion

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 fight against cybercrime in Vietnam has met many challenges affecting three conditions: *likely offenders, suitable targets*, and *the absence of*

capable guardians. Although it is difficult to prevent the concurrence of likely offenders and suitable targets in cyberspace, using all or either governmental, organizational, and personal guardianship may frustrate motivated offenders and reduce the capacity of cyber victimization and criminalization.

Even though there are some arguments about applying the RAT to cybercrime, there is no denying that the RAT plays an important role in understanding the causation of victimization and criminalization in cyberspace. 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.* Therefore, it is imperative to use *capable guardians* as a "shield" against cybercrime.

Limited attempts have been made to review the context of cybercrime in Vietnam using the RAT with three crucial factors. Without primary data, the influence of dimensions inside each factor is difficult to assess well. Despite this, the paper has attempted to present such an analysis. Further studies can be conducted with the primary data to analyze the correlation comprehensively.

Acknowledgements

I would like to thank Dr. Ken Miichi (Waseda University) for his advice and his comments on earlier versions of the article; Anti-Cybercrime Police Faculty (People's Police Academy) for fruitful discussions and their assistance in collecting reports.

References

Ahmed, M., Shari, L., Kabir, M., & Al-Maimani, M. (2012, July - August). 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.

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

Bennett, R. R. (1991). Routine activities: A cross-national assessment of a criminological perspective. *Social Forces, 70*(1), 147-163. doi: 10.2307/2580066

BKAV. (2016, August 8). *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 26, 2019, from BKAV: http://m.bkav.com.vn/en_GB/ho_tro_khach_hang/-/chi_tiet/400028/trang-tin-tuc?cur=8

BKAV. (2017, December 27). *Tong ket an ninh mang nam 2017 va du bao xu huong 2018* [Cybersecurity summary 2017 and trend 2018]. Retrieved from BKAV: 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.

BMI. (2016). *Vietnam information technology report.* New York. Retrieved from http://www.alacrastore.com/storecontent/Business-Monitor-International-Industry-Reports/Vietnam-Information-Technology-Report-2026-1262

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.

Botnet statistics for the year of 2016. (2017, January 9). Retrieved from Botnet-tracker: http://botnet-tracker.blogspot.com/2017/01/botnet-statistics-for-year-of-2016.html.

Botnet statistics for the year of 2017. (2018, February 20). Retrieved from Botnet-tracker: https://botnet-tracker.blogspot.com/2018/02/botnet-statistics-for-year-of-2017.html.

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

Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308-333.

Chowdappa, K., Lakshmi, S., & Kumar, 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.

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

CSIS. (2018). *Economic impact of cybercrime - no slowing down.* Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime.

Dai, C. T. (2017). Cybersecurity governance framework in Vietnam: State of play, progress and future prospects. *Asian Research Policy, 8*(1), 86-97. Retrieved from http://www.arpjournal.org/download/usr_downloadFile.do?requestedFile=20170804118248150.pdf&path=journal&tp=isdwn&seq=148.

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

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

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

European Cybercrime Center. (2014). *The Internet organised crime threat assessment (iOCTA) 2014.* doi:10.2813/16

Felson, M. (1998). *Crime and everyday life.* Thousand Oaks, CA: Pine Forge Press.

Forexbonuses. (n.d.). *The World's most cashless countries*. Retrieved from Forexbonuses: http://www.forexbonuses.org/cashless-countries.

Goel, A. (2016, August 12). *The great cyber game in South China Sea*. Retrieved from Cyware: https://cyware.com/news/the-great-cyber-game-in-south-china-sea-883f7f39?PageSpeed=noscript.

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.

Grabosky, P. (2001). Virtual criminality: old wine in new bottles? *Social and Legal Studies, 10*(2), 243-249.

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*, 1-18. doi:10.1504/IJESDF.2017.081749

High-tech Crime Police Department. (2010). *Bao cao tong ket nam 2010* [Annual report 2010].

High-tech Crime Police Department. (2011). *Bao cao tong ket nam 2011* [Annual report 2011].

High-tech Crime Police Department. (2012). *Bao cao tong ket nam 2012* [Annual report 2012].

High-tech Crime Police Department. (2013). *Bao cao tong ket nam 2013* [Annual report 2013].

High-tech Crime Police Department. (2014). *Bao cao tong ket nam 2014* [Annual report 2014].

High-tech Crime Police Department. (2015). *Bao cao tong ket nam 2015* [Annual report 2015].

High-tech Crime Police Department. (2016). *Bao cao tong ket nam 2016* [Annual report 2016].

High-tech Crime Police Department. (2017). *Bao cao tong ket nam 2017* [Annual report 2017].

Hsieh, M.-l., & Wang, S.-Y. K. (2018). Routine activities in a virtual space: A Taiwanese Case of an ATM hacking spree. *International Journal of Cyber Criminology, 12*(1), 333-352. doi: 10.5281/zenodo.1467935

Hung, G. (2018, May 2). *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 from Dantri: https://dantri.com.vn/suc-manh-so/160-trieu-tai-khoan-zing-id-lo-lot-mat-khau-de-chiem-rat-nhieu-20180502063917763.htm.

Internet World Stats. (n.d.). *Top 20 countries with the highest number of Internet users*. Retrieved from Internetworldstats: https://www.internetworldstats.com/top20.htm

INTERPOL. (2018). *Annual Report 2017.* Retrieved from https://www.interpol.int/content/download/5258/file/Annual%20Report%202017-EN.pdf.

ISACA. (2019). *State of cybersecurity 2019 part 2: Current trends in attacks, awareness and governance.* Retrieved from https://www.isaca.org/Pages/DocumentDownloadRegistration.aspx?file=http%3a%2f%2fwww.isaca.org%2fKnowledge-Center%2fResearch%2fDocuments%2fcyber%2fstate-of-cybersecurity-2019-part-2_res_eng_0619.pdf&ReturnUrl=%2fPages%2fFileDownload.aspx%3ffile%3dhttp%3a%2.

ITU. (2017). *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. (2018). *Global Cybersecurity Index (GCI) 2018.* Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf.

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.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Wolff, S. (1997). *Brief history of the Internet.* Retrieved from Internet Society: https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf.

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.

M.T. (2018, June 11). *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 from Ict News: 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.

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.

Ministry of Public Security. (2017). *Bao cao tong ket tinh hinh thuc tien cong tac bao ve an ninh mang* [Report about protecting cybersecurity]. Retrieved from http://duthaoonline.quochoi.vn/DuThao/Lists/DT_DUTHAO_LUAT/View_Detail.aspx?ItemID=1382&TabIndex=2&TaiLieuID=2898.

Miró, F. (2014). Routine Activity Theory. In J. M. Miller (Ed), *The encyclopedia of theoretical criminology.* Blackwell Publishing Ltd.
doi: 10.1002/9781118517390/wbetc198.

Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using Routine Activities Theory predict cyberbullying experiences. *Sociological Spectrum*, 81-94.
doi: 10.1080/02732173.2012.628560

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.

Nguyen, T. (2016, August 3). *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 from Thanhtra: 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.

PCA. (2016). *PCA press release: The South China Sea Arbitration (The Republic of the Philippines v. The People's Republic of China).* Retrieved from PCA-CPA: 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/

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (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. doi: 10.1177/0022427810365903

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.

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

The World Bank. (2019). *Unemployment, total (% of total labor force) (modeled ILO estimate).* Retrieved from The World Bank: https://data.worldbank.org/indicator/SL.UEM.TOTL.ZS?end=2018&locations=VN&start=2008.

UN. (2004). *United Nations Convention against transnational organized crime and the protocols thereto.* Retrieved from UNODC: https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf.

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, March 12). *Spam and phishing in 2018.* Retrieved June 16, 2019, from Securelist: https://securelist.com/spam-and-phishing-in-2018/89701.

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 cyber attacks on the systems of Vietnam Airlines]. Retrieved from VNISA: 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].

We Are Social & Hootsuite. (2018). *Digital in 2018.* Retrieved from https://wearesocial.com/blog/2018/01/global-digital-report-2018.

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. doi: 10.1093/bjc/azv011

Wilsem van, J. A. (2011). 'Bought it, but never got it' assessing risk factors for online consumer fraud victimization. *European Sociologic Review, 29*(2), 168-178. doi:10.1093/esr/jcr053

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of Routine Activity Theory. *European Journal of Criminology, 2*(4), 407-427. doi: 10.1177/147737080556056

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. doi: 10.1016/j.icte.2017.12.007