ORIGINAL RESEARCH PAPER

Law

CYBERCRIME SITUATION IN VIETNAM AND RECOMMENDATIONS

KEY WORDS: cybercrime, Vietnam, technology, situation, recommendations, police force

Kien Le Trung Lieutenant Colonel, PhD, Vice Dean of the Post-graduate Training Institute, The People's Police Academy, Vietnam

Thu Nga Tran Thi* Major, PhD, Vice Dean of the Environmental Police Department, The People's Police Academy, Vietnam *Corresponding Author

ABSTRACT

Objectives: Cybercrime is taking place in a rising trend and is receiving the concern all over the world. This study analyzed, evaluated the cybercrime situation in Vietnam and gave recommendations as well as the solutions to these problems.

Methods/Statistical analysis: This paper was studied by synthesizing through the methods of research such as analysis, evaluation, synthesis; To study typical cases of violating law against cybercrime in a number of areas where violations frequently occur.

Findings: Survey article also describes typical cases of cybercrime occurring prominently and in specific locations in the whole territory of Vietnam; Point out the causes and conditions of the offense; issues about the offender's identity, procedures and operandis. Basing on each case, depicting the picture of the situation of cybercrime in Vietnam nowadays. From the analysis of cybercrime situation in the current period, the article gives forecasts, comments and some suitable solutions to apply in the prevention of restriction of crime; Towards the objective of detecting the investigation, dealing with violations. The solutions also promote the efficiency of the fight against cybercrime, continue amending its legistration, policies as well as raising public awareness and investing more resources. All soluotions are emphasized in the group of management solutions, technology application solutions, application of professional measures of the Vietnamese Police Force.

Application/Improvements: If these solutions could be applied, they will help to deal with cybercrime more feasible; therefore, raising and minimizing these types of violations in Vietnam.

1. INTRODUCTION

As one of the most blooming ICT markets over the world, Vietnam has experienced the fast development of the Internet and mobile network during the last decade. Despite a developing country with an average per capita income, its people spend a remarkable amount of their money on technology. The number of Internet access, basically through cable access, optical fiber, and mobile broadband, has increased rapidly due to people's need for knowledge acquisition and entertainment. People are also very interested in mobile devices for their convenience and flexibility. According to Nielsen Vietnam Smartphone Insights Report 2017 published on November 2017, the number of people using smartphone among mobile phone users was 84%. Furthermore, Vietnamese tend to spend much time on social networks, although it contributes to the poor work performance. Hootsuite in 2018 demonstrates 57% of the Vietnamese population is able to access social media. The number of social media users continues growing 20% compared to last year. On average, a Vietnamese user spends 2 hours and 37 minutes on social media every day. The most popular social network in Vietnam is Facebook with 55 million users which help it ranks 7th on top of the country have most users on this network. People also spend much time on Youtube, Tiktok (a short-video social platform powered by music) and some other domestic social networks (with integrated instant message application).

As of May 2018, there were about 12.5 million fixed broadband Internet subscriptions and 64.2 million mobile broadband subscriptions. The mobile network has been nation-wide penetrated with approximately 124 million subscriptions, including 51.6 million 3G/4G subscriptions compared to the nation's 96 million of the population. Currently, Vietnam has 5 mobile network operators, including Viettel (a military-run telecommunication corporation), Mobifone, Vinaphone, Vietnamobile, and Gmobile. Since October 2016, three biggest operators started providing 4G LTE technology [1, 10-11]. To catch up with the development of the society and leverage ICT achievements, the government of Vietnam has been proactive in executing social administrative management and changing its internal operation by applying more and more technology. Thanks to those efforts, Vietnam gradually reaches higher ranks in ICT indexes. In 2016, the Networked Readiness Index (NRI) of Vietnam ranked 79th while affordability to access ICT was estimated 3rd among 139 nations surveyed. Especially, the fixed broadband Internet tariff of Vietnam was cheapest globally. In this year, the report from the United Nations (UN) shows Vietnam's E-Government Development Index rates 88 over 193 nation members. However, there are many issues that Vietnam needs to improve to make sure a safe cyberspace. In 2016, its infrastructure and digital content index only ranked 121/139 countries. Last year, Vietnam ranked 100/164 countries in terms of the Global Cybersecurity Index, according to the International Telecommunication Union (ITU).

2. CYBERCRIME SITUATION IN VIETNAM

The dynamic development of ICT in Vietnam creates chances for a comprehensive breakthrough but also poses serious challenges to national security, social order and safety, due to threats from cybercrime, which can be divided into 2 main types: cyber-dependent crimes and cyber-enabled crimes.

2.1. Cyber-dependent crimes

Cyber-dependent crimes are offenses that can only be committed using a computer, computer networks or other forms of information communications technology (ICT). In the first 8 months of 2018, there were over 6,500 network attack incidents to websites of Vietnam in different types (including 3,818 cases of defacement, 1,800 cases of phishing attacks and 949 cases of malware attack) reported. It can be said that most serious cyber threat in Vietnam is malware and spyware. In the past, malware was spread to disturb Internet users, but recently they have been designed to steal user's information, or encrypted data to require ransom from the victims (ransomware), or cryptocurrency mining malware as the global trend. Vietnam ranked 4th position in the top of 10 countries having most computers controlled by botnets last year. Latest statistic of Kaspersky Lab shows in last month, about Ľ computers in Vietnam was infected malware (local infection rate 26.8%). Besides, spyware is provided illegally in the country, mostly for smartphone surveillance. On January 2018, law enforcement nabbed a group of criminals who illegal provided surveillance services, eavesdropping software on mobile phone through the website spyphonevn.com, illegally appropriated more than VND 400 million (equivalent to US$ 17,400).

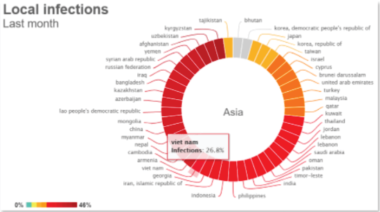


Figure 1. Malware local infection rate in Asia, statistics on October 27, 2018.

Beside malware, hackings also happen frequently, especially attacks or intrusions into computer networks of banks and financial institutions, airports, etc. caused extremely severe consequences. According to statistics from Kaspersky Lab on the first half of 2018, Vietnam was on top of the countries by the number of industrial control system (ICS) computers attacked, where 75.1% of ICS computers were attacked. In addition, many advanced persistent threat (APT) attacks targeted on systems (mostly by email phishing and software flaws exploit) of governmental agencies, financial system, banks or critical information infrastructure for the purpose of sabotage or stealing information. Recently on October 13, the website of Co-opbank of Vietnam was hacked and stolen all 275,000 information of online customers. Hackers required a ransom of US$ 100,000 to get the data back by advance payment in Bitcoin or Bitcoin Cash, otherwise they would sell them for others. On March 2017, websites of Tan Son Nhat International Airport (Ho Chi Minh City) and 4 other airports were hacked by two 15-year-old students. Back to May 2016, Tien Phong bank was hacked in a SWIFT cyberattack, fortunately they were able to identify and prevent loss.

Distributed Denial of Service Attack (DDoS) is another problem in cyberspace of Vietnam. Q2 2018's statistics from Kaspersky Lab indicates the country accounts for 0.5% of DDoS attacks and 0.64% of unique DDoS targets. It occupied 3.31% of botnets worldwide and ranked 7th on top countries by the number of botnets. Statistics for the same duration reveals Vietnam occupied 6th on top of email spam originating-countries. Because of the scale of DDoS and spam, these crimes are time and resource consuming and very difficult to investigate. Additionally, law enforcement received lots of online fraud complaints originating from email phishing ("romance scam"), which will be mentioned later on.

2.2. Cyber-enabled crimes

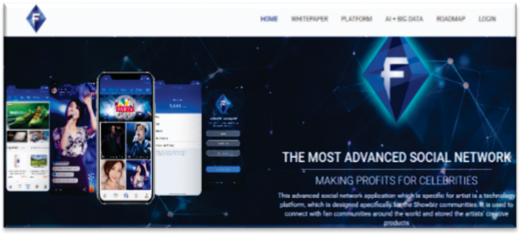
Cyber-enabled crimes are traditional crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT).

Cybercrime in the sector of finance and banking

Perpetrators are foreigners, mostly from China, Taiwan (China) or Africa. Previously they chose big cities like Hanoi, Ho Chi Minh City to commit their crimes. Now they operate their activities in less-developed areas where people do not have good awareness of cybercrime and local law enforcement are weak at cyber capacity. Border areas also are leveraged because criminals can depart to other countries immediately after they committed their crimes. The methods of criminal are also diverse, including abuse payment methods of banks and telecommunication services to appropriate property; hire people to open bank accounts then buy those accounts, bank card accounts or international debit accounts to receive money from their online fraudulent activities and finally withdraw the appropriated money abroad.

The crime of use and trade stolen credit card information continues causing serious damage: (i) Skimming device installation at ATM machines of Vietnamese banks; (ii) foreign suspects enter to Vietnam, illegally use credit card information and collude with domestic suspects to make counterfeit transactions on POS in order to withdraw money, appropriate dozen billion of Vietnam Dong; (iii) use stolen credit card to pay services or purchase goods. On April 23, 2017, police caught 2 suspects from China withdrawing money from ATM machine by fake cards in Hanoi, seized 23 fake cards. Four more suspects also from China were arrested during expanding the investigation. Those suspects admitted to illegal withdraw approximately VND 350 million (equivalent to US$ 15,200). In the year 2017, police investigated totally 60 cases of skimming device installation which caused a loss of VND 15 billion (over US$ 650,000).

Frauds abused cryptocurrency has been a trend for couple years due to the high interest rate of business. In the first 6 months of 2018, there has been a bloom of virtual currencies, electronic currencies and capital mobilization by initial coin offer (ICO). Though Vietnam has not had regulations on virtual currencies, many people still trade them online. With the rumor of high interest from Bitcoin and other virtual currencies investment, criminals set up their trap on the victim by launching Bitcoin-like ICO to mobilize money from people in the pyramid-scheme model. They organize events, sometimes even create media campaigns to advertise their ICO, targeting to unaware people. Reality shows victims are generally seniors, retired, students or shopkeepers. Once received a big certain amount of investment, suspects shut down the website and disappear. Last year, the public shocked on a cryptocurrency-based fraud running by the Modern Tech Company. This company called people invest money to buy tokens for its Pincoin ICO, then another token for iFan to make profits for celebrities.



THE MOST ADVANCED SOCIAL NETWORK

MAKING PROFITS FOR CELEBRITIES

This advanced social network application which is specific for artist is a technology platform, which is designed specifically for the Showbiz communities. It is used to connect with fan communities around the world and stored the artists' creative products

Figure 2. The Professional interface of iFan's website - https://ifan.io - which is still working.

These coins were introduced coming from Singapore or India and based on Ethereum platform. Investors receive the lowest interest rate 48% per month and 8% commission from the new member's investment at their invitation. On last April, a team consisting of 7 people who running the company went abroad, leaving investors with a loss of VND 15,000 billion (equivalent to US$ 600 million). This can be the largest ever scam and a typical case of virtual currency scams in Vietnam.

Cybercrime in the sector of telecommunication networks

In many localities, there were repeatedly situation in which suspects set up telecommunication switchboard, use VoIP technology to make impersonated calls of governmental agencies (posts, public security forces, courts, procuracies, etc.) to people for appropriating property. Initially foreign suspects swindle only their fellow citizens in their home country, however recently they have colluded and taught domestic criminals to swindle Vietnamese citizens. On June last year, Lang Son (a border province with China) provincial public security force found a group of fraudsters who conduct phone scam to Vietnamese citizens. The group leader lived in China and instructed his 2 Vietnamese accomplices living in Lang Son province to commit their crime. They hire people to open lots of bank accounts with the price of from VND 200,000 to 300,000 (from US$ 9 to US$28). Base on leaked personal information, they impersonated Vietnamese police to call to people in many localities, informing the victims are involving into an ongoing investigation, required them to transfer money in their accounts to police's accounts (actually criminal's accounts). Once received, they immediately withdrew and sent money to foreign countries by currency exchanging service. Over VND 4.6 billion was sent abroad among VND 7.2 billion (US$ 313,000) sent to their accounts. Police prevented VND 600 million by freezing relevant accounts. In this case, 5 suspects (1 Chinese, 4 Vietnamese) were charged with their crime. On June 19, 2018, Division of Criminal Investigation, Quang Nam province arrested 12 for "Swindle to appropriate property", including 6 Taiwanese (Chinese) and 6 Vietnamese.

Figure 3. Six Taiwanese (Chinese) arrested on June 19, 2018 in Quang Nam province.On social networks, criminals are even easier to approach potential victims.

The situation of foreigners collude with Vietnamese to make acquaintance with victims, build trust and promise to send them money or/and valuable gifts, then impersonate customs officers to call them requiring to transfer fee to finalize clearance procedures in order to appropriate property. This is so-called "roman scam" and it is also committed through email conversations with victims. Criminals often impersonate US soldiers in Africa or Western male who divorced to build confidence and emotion with Vietnamese victims, who are normally divorced, single or retired females. On March last year, a female living in Ho Chi Minh City reported she was a victim of her "online fiancé". She loved an American man named James Oscar Herera who was working in Syria. James promised to marry her, take her to the US and leave her an inheritance of millions USD. In that way, the fraudster convinced her to send him VND 11 billion (about US$ 500,000) and ran away.

Figure 4. A "romance scam" group arrested. Source: antg.cand.com.vn
(Source: Newspaper of Ministry of Public Security of Vietnam (MPS))

In several provinces, such as Quang Tri, Quang Nam, etc., some groups of criminal were formed and committed swindle to appropriate property by sending awards notifying message on social networks or instant message applications and require "lucky people" send money in order to finalize award delivery procedure. The problem gets worse because those groups consist of very young people mainly under 18. Some stopped their education at secondary or high school. Only groups' leaders are knowledgeable about IT, the rest are just click workers. On September 2015, police arrested a group of 9 subjects living in Duy Xuyen district, Quang Nam province, who set up 117 scam websites to swindle people as above method, illegally appropriate VND 8.3 billion (US$ 360,000). Police and local authorities have had some campaigns to educate the community, especially target on young people and their families do not involve into those activities.

Figure 5. The youngster group arrested in Quang Nam province on September 2015.

Cybercrime in the sector of e-commerce

Fraudulent activities are committed in different methods, such as: Create websites to sell genuine products with 40 - 60% discount but break the deal by delivering shoddy or unknown origin products; sell counterfeit cash, degrees, and certificates; hackers compromise email accounts of companies to monitor victims' business activities, after that modify receiving accounts to appropriate money in the contracts from victims' partners. In addition, pyramid-scheme business activities still happen very complicatedly though under the management and monitoring of authorities. Suspects abuse pyramid-scheme product sale to appropriate property in many different modi operandi, such as: (i) create websites to mobilize capital with high interest rate; (ii) abuse charity activities to commit swindle; (iii) create exchange platforms for sending and receiving money; (iv) create many exchange platforms for virtual currencies (Onecoin, ILcoin, Gemcoin, etc.) based on pyramid-scheme business model for attracting investors, money laundering, product shipping or playing sport bets, etc.; (v) establish companies, impersonate foreign projects' staff to mobilize capital with high rate of interest and commission based on pyramid-scheme model in order to appropriate property of investors.

Online gambling and gambling organization

Though declining, online gambling organization and gambling activities keep happening with the penetration of many abroad websites. Foreign leaders often connect with domestic suspects (so-called agents) to build up a large gambling ring for both Vietnamese and foreigner players. Their operations are well-organized and harder for police to identify and investigate. Payment methods are various, including cash, bank transfer or mobile top-up card. Some of the gambling dens have guards and equipped security cameras to detect police appearance. On Mach 28, police arrested a group of 7 criminals who commit online gambling and gambling organization through football bet. Investigation result shows they started their crime in 2015 and the total amount of betting money is about VND 1,176 billion (US$ 51.13 million). The government estimates dozens of millions of USD is daily leaked to foreign countries as a result of online gambling.

By perceiving the abuse of mobile top-up card in payment for online gambling, on April, the government requires all telecommunication service providers to stop providing mobile phone top-up card payment for digital content services due to shortcomings when it was used as a payment mean to online gambling games, illegal advertisement, or online trade swindles, etc. with a big amount of transactions. Governmental administrating agencies are researching to adopt new adequate measures for this issue.

Online depraved materials dissemination and personal information trade

Many websites and forums continue sharing pornographic images and movies which affect our fine customs and practices. Especially, child pornographic material dissemination has caused many bad consequences for the society, impacted on the psychobiological development of children and increased child sexual abuse crime. Criminal even make money from running those websites. On December 2016, police arrested Nguyen Duy Hai and his 3 accomplices who built, managed and operated many different websites contains depraved materials, especially child porn materials, including hzfile.asia; hzfile.com; hzfile.asia; hzfile.al; http://1artbbs.net; http://1artbbs.org; http://vipbabe.tokyo; http://1artbbs.in; http://1babe.hk; http://1babe.al; http://prebabe.in; http://1babe.ae; http://1babe.ph in order to illegally gain profits by selling paid memberships on those websites which allow downloading child porn movies. The price for paid membership is US$ 16.99 for 30 days; US$ 27.99 for 60 days; US$ 35.99 for 90 days and US$ 63.99 for 180 days. Suspects posted 4,400 child porn movies and clips on those websites, which have over 40,000 members, including 612 paid members. The amount of money was appropriated is about VND 3.6 billion (US$ 156,000). In this case, MPS of Vietnam also received many cooperation requests from foreign law enforcement agencies, including Australian Federal Police (AFP), Ireland Police, UK, France, and German.

On those websites, hackers spread various malware or scam websites in order to unauthorized collect internet users' information to serve their criminal activities. This behavior, plus poor customer information management in many businesses, make personal information trade pretty popular and publicly on the Internet, which facilitates the increase of some types of crime, such as SMS spam, swindle on social networks, phone scam, etc.

Digital Piracy

Software, digital music and movie piracy; infringement of copyrights in general and television program copyrights in particular, become a serious concern. Though software piracy rate in Vietnam dropped from 78% in 2015 to 74% in 2017, it is still a factor weakening our competitiveness and intelligent economy, as well as posing users to high risks of malware attack.**3. THE OUTCOME OF FIGHT AGAINST CYBERCRIME**Statistics from 2014 to the first half of 2018 show optimistic result of the fight against cybercrime in Vietnam.

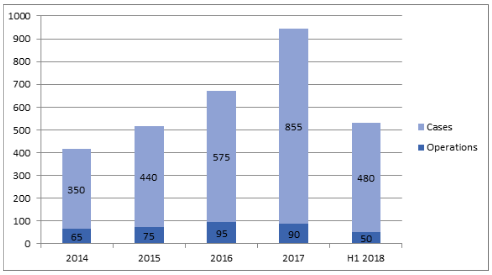


Figure 6. The number of operations and cases were undertaken from 2014 to the first half of 2018 [2].

An operation means a serious case which law enforcement need to mobilize resources and measures during the investigation. A case can be a complaint from citizen which not a cybercrime case after verification.

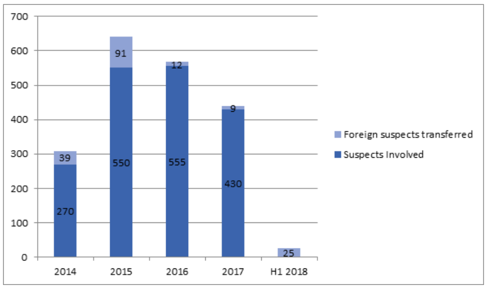


Figure 7. The number of suspects involved and foreign suspects transferred from 2014 to the first half of 2018

The number of defendants can be lower than the number of suspects involved due to the consideration of investigating police and procuracies. Foreign suspects transferred are who committed crimes in Vietnam but not harm to Vietnam and were transferred to their home countries.As can be seen from the above charts, the total number of cases and operations has increased year by year. Practically it is very difficult to assess the situation of cybercrime, because of hidden crime. There are many petty cybercrimes were not reported to police in different reasons, for instance, individual victim of SMS scam for a small loss, victim of "romance scam" for the scare of public opinion, or victim of malware and ransomware for not able to pursue the case, etc. On the other hand, the number of cases also depends on the capacity of law enforcement in identify and investigate cybercrime.

Statistics of cybercrime exposes shortcomings in practice. A cyber-enabled case could be calculated as traditional crime case, causing duplication in crime statistics. Cybercrime has not been categorized into details to see the crime trend, which is the basic to propose and implement crime preventive measures.

4. The Legal framework for Cybercrime Prevention and Suppression

In 2015, the National Assembly of Vietnam has passed the Penal Code 2015 (amended in 2017) which contains 9 articles on cybercrime, from Article 285 to Article 294 (Article 292 "Unauthorized business" was dismissed). Besides, there is the Decree 25/2014/NĐ-CP dated April 7, 2014, issued by the Prime Minister on prevention and suppression of high-tech used crime and legal violations. After being applicable in several years, this Decree is considering to be amended early.

On last June, Cybersecurity Law was passed and will come into effect on January 1, 2019. The regulations in this Law facilitate cybercrime fight and prevention, for example data localization requirement, data retention and business representative office establishment in Vietnam.

Previously, the High Tech Crime Department, under the General Department of Police, MPS was the designated agency concentrated on the fight against cybercrime in Vietnam. Recently, after the reconstruction, the Department was merged with another one, becoming the Cyber Security and Counter High-Tech Crime Department, directly under the MPS which does both cybersecurity assurance and fight against cybercrime.

4. RECOMMENDATIONS FOR THE FIGHT OF CYBERCRIME IN VIETNAM

Base on the analysis of cybercrime situation, as well as cybercrime statistics and its legal framework, I have some recommendations to promote the efficiency of the fight against cybercrime in Vietnam as follows:

- The government of Vietnam should have coherent policies on ICT development and management to support the digital economy as well as prevent legal loopholes which can be exploited, such as using mobile top-up cards to pay for digital services, online gambling or online games, and then convert it back to cash. Cryptocurrency legalization and management are also needed to take into account in order to take its advantages but still ensure the national financial and monetary system.

- The Ministry of Public Security should cooperate with other relevant ministries and agencies to review and amend regulations of the Penal Code, the applicable Decree 25/2014/NĐ-CP and implementing documents of the Cybersecurity Law. Those regulations should be up-to-date while ensuring national cyberspace security, as well as supporting digital business activities in the country. It should have suitable categories that describe what type of business organizations must fully or partly comply with the requirements of Cybersecurity Law, what type of information must be stored in Vietnam, and what kind of business corporations must open branches or representative offices in our country.

- The government should implement proactive cybersecurity measures which focus on deterring and preventing cybercrime. Once cybercrime happened, it will be very challenged to identify and investigate. The government should have many mass-media campaigns to educate organizations and people about self-protect skills online and cyberspace threats. The greater awareness they have, the less chance they will be victims of cybercrime.

- Cyber Security and Counter High-Tech Crime Department should invest more human resource as well as budget in science research, technical equipment and training for its staff. Without those, it will be left behind the rapid development of ICT and cybercrime evolution. It also needs to build its nationwide provincial cyber police force which covers the situation of the whole country.

- The Department should build up a close public-private partnership (PPP), not only with domestic business but also, and especially with international Internet service providers, such as Google, Facebook, Microsoft, Yahoo, etc. to facilitate data and evidence acquisition during cybercrime investigation. The private sector also can support the Department on training and technical issues.

- The Department should change the way of cybercrime statistics, which has a hierarchical category. This can be a suggestion:

Figure 8. The suggestion of cybercrime statistics which has a hierarchical category

This category can create a big picture of cybercrime and may help to observe every kind of cybercrime to propose suitable preventive measures. It is also necessary to eliminate duplication in cybercrime and crime statistics.

REFERENCES

1. Ministry of Information and Telecommunication (MIC) of Vietnam, ICT White Book of Vietnam 2017, published on August 2017
2. Ministry of Public Security Vietnam (SPS), Annual reports of High Tech Crime Department, from 2014 to the first half of 2018.
3. Ministry of Information and Telecommunication of Vietnam, Report of Statistics of Vietnam Telecommunication Agency (VNTA), December 2017
4. Ministry of Public Security of Vietnam, Report of suspects installed skimming devices on ATM machine to steal customers' card information in many localities, including Vinh Long, Bac Lieu, Can Tho, Khanh Hoa, Hanoi, Ho Chi Minh City, Da Nang, etc.
5. Ministry of Public Security of Vietnam, Report of typical case is on January 2018, 3 suspects were nabbed for "Use internet to commit property appropriation", January 2018
6. Mike McGuire (University of Surrey) and Samantha Dowling (Home Office Science), Cyber crime: A review of the evidence Research Report 75 - Chapter 1: Cyber-dependent Crime (2003)
7. Parliament of Vietnam, The Penal Code 2015 of Vietnam (amended 2017).
8. Prime Minister of Vietnam, The Decree 25/2014/NĐ-CP dated April 7, 2014 issued on prevention and suppression of high-tech used crime and legal violations.
9. Parliament of Vietnam, The Cybersecurity Law of Vietnam.
10. Society for Worldwide Interbank and Financial Telecommunication, Report of leading provider of secure financial messaging services, June 2018. Internet source
11. Nielsen, Press Release, see at https://www.nielsen.com/ content/dam/nielsenglobal/vn/docs/PR_EN/Web_Nielsen_Smartphones%20Insights_EN.pdf&pdf=true [accessed on October 27, 2018]
12. World Economic Forum (WEF), see at http://reports.weforum.org/global-information-technology-report-2016/economies/#indexId=NRI&economy=VNM [accessed on October 27, 2018]
13. Data-Center base, see at https://publicadministration.un.org/egovkb/Data-Center [accessed on October 27, 2018]
14. ITU, Global Cybersecurity Index (GCI) 2018, pg. 62, see athttps://www.itu.int/dms_ pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf [accessed on October 27, 2018]
15. ITCNews - Ministr of Information and Information of Vietnam, see at https://ictnews.vn/cntt/bao-mat/hon-6-500-su-co-tan-cong-vao-cac-website-cua-viet-nam-trong-8-thang-dau-nam-nay-172090.ict [accessed on October 27, 2018].
16. Kaspersky Lab, see at https://securelist.com/statistics/ [accessed on October 27, 2018]
17. Kaspersky Lab, see at https://www.kaspersky.com/about/press-releases/2018_ics-computers-attacked-in-h1 [accessed on October 27, 2018]
18. Voice of Vietnam newspaper, see at https://vov.vn/cong-nghe/khong-chi-ngan-hang-hop-tac-xa-bi-tan-cong-hacker-khong-chua-ai-826106.vov [accessed on October 27, 2018]
19. Kaspersky Lab, DDoS Attacks in Q2 2018, see at https://securelist.com/ddos-report-in-q2-2018/86537/ [accessed on October 27, 2018]
20. Kaspersky Lab, Spam and phishing in Q2 2018, see at https://securelist.com/spam-and-phishing-in-q2-2018/87368/ [accessed on October 27, 2018]
23. Techcrunch, Exit scammers run off with $660 million in ICO earnings, see at https://techcrunch.com/2018/04/13/exit-scammers-run-off-with-660-million-in-ico-earnings/ [accessed on October 27, 2018]
24. Online newspapers of Vietnam General Confederation of Labor, Ch n đ ng các v l a đ o ti n o Vi t Nam, see at https://laodong.vn/kinh-te/chan-dong-cac-vu-lua-dao-tien-ao-o-viet-nam-621810.ldo [accessed on October 27, 2018]
25. Central Vietnam Association for Learning Promotion newspaper, Đ ng dây gi danh cán b B Công an, l a đ o h n 7 t đ ng, see at https://dantri.com.vn/phap-luat/duong -day-gia-danh-can-bo-bo-cong-an-lua-dao-hon-7-ty-dong-20170616143757362.htm [accessed on October 29, 2018]
26. Online newspaper of MPS of Vietnam, Lŕm gě đ không b m c b y "Tây l a těnh" trẹn m ng?, see at http://antg.cand.com.vn/Vu-an-noi-tieng/Lam-gi-de-khong-bi-mac-bay-Tay-lua-tinh-tren-mang-432379/ [accessed on October 29, 2018]
27. Online newspaper of MPS of Vietnam, L p 117 trang web l a đ o 8,3 t đ ng, see at http://cand.com.vn/Phap-luat/Khoi-to-tam-giam-9-doi-tuong-trong-duong-day-lua-trung-thuong-qua-mang-8-3-ti-dong-365231/ [accessed on October 29, 2018]
28. On May 30, 2017, police arrested 12 gamblers in Ha Tinh province after deactivating guards and security camera system. See athttp://cadn.com.vn/news/145 _ 167615_nguo-i-co-uy-to-chu-c-da-nh-ba-c-.aspx [accessed on October 30, 2018]
29. Online newspaper of MPS of Vietnam, Tri t phá đ ng dây đánh b c bong88ag.com, see at http://cand.com.vn/Ban-tin-113/Duong-day-danh-bac-bong88ag-com-bi-triet-pha-nhu-the-nao-484581/ [accessed on October 29, 2018]
30. Online newspaper of MPS of Vietnam, Ki m ti n t t vi c l p 15 trang web sex, see at http://cand.com.vn/Ban-tin-113/Lap-web-sex-chuyen-phim-khieu-dam-kich-duc-thu-loi-160-000-USD-420426/ [accessed on October 30, 2018]
31. Business Software Alliance (BSA), Software Management: Security Imperative, Business Opportunity - BSA Global Software Survey June 2018, see at https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf [accessed on October]