International Journal of Social Science And Human Research

ISSN(print): 2644-0679, ISSN(online): 2644-0695

Volume 05 Issue 11 November 2022

DOI: 10.47191/ijsshr/v5-i11-36, Impact factor- 5.871

Page No: 5082-5086

Cybercrime in the Digital Age: Challenges and Implication for Prevention

Nguyen The Sang[1], Bui Bao Trung[2]

[1,2]Institute of Police Science, People's Police Academy, Hanoi, Vietnam

ABSTRACT: The development of the internet and the widened access to computer technology has not only granted new opportunities for economic activities but has also created opportunities for those involved in illegal activities on the Internet. The main purpose of the articles is to present the different viewpoints of cybercrime, its impacts on individual, organisation and society and propose the prevention strategy.

KEYWORDS: cybercrime, digital age, crime prevention, cybercriminal

I. INTRODUCTION

Cyber space is the most used platform these days, in all aspects of human lives. It is involved in all domains whether it is business, entertainment, banking, education, logistics, military services or research.[1] The growth of information and communication technology facilitate our everyday life. The evolution of the Internet can, on the one hand, transform an inefficient world into one that is more convenient and immediate. On the other side, the Internet also introduces the issue of cybercrime, a new form of sophisticated crime. Information technology can have both positive and harmful effects on the lives of individuals. The positive influence of information and communication technology can be utilised, among other things, as a communication medium, for data sharing, or to facilitate trading transactions and commercial operations. While the negative effects of information technology include all types of criminal behaviour on the Internet that can be abused or contain risks to its security, particularly security when the transfer of data on the network, the dangers to its security are greatest during data transfer. Data flowing over a computer network is susceptible to being intercepted, stolen, or altered. The stolen and abused data are subsequently utilized for personal advantage, can even be used for illegal acts such as pornographic media, information media of cruelty, fraud, gambling, and theft of money.

II. CYBERCRIME DEFINITION AND CLASSIFICATION

Despite of the fact that cybercrime is the term used frequently these days, cybercrime is still not clearly and precisely defined. It is sometimes called "electronic crime", "computer crime", "computer-related crime", "hi-tech crime", "technology-enabled crime".[2] Cybercrime is defined as the use of a computer system in the commission of a crime or as a tool in the commission of an offence. A cybercriminal may use a tool to gain access to a customer's private information, personal service information, and federal government-related data. According to some academics, cybercrime is a crime in which computer technology is a primary criminal tool. On the basis of the sophistication of the development of information technology, it may also refer to illegal acts that employ computer technology.

Although cybercrime and traditional crimes have similarities, there are major variations between cyber and physical crimes, making cybercrime an essential academic issue.[3] The primary distinction between cybercrimes and physical crimes is that the limits of the cybercrime scene are not clearly delineated. Cybercrime may stretch beyond a single room, city, nation, or globe. Cybercrime is illegal, unethical, and unauthorized behaviour within an information processing or transmission system.

Cybercrimes can occur in numerous scenarios and have different facets. For example the council of Europe's Cybercrime treaty uses the term that refers to the criminal activity perform against the data content and copyright violation. Other researcher believes that cybercrime has two types; type 1 and type 2. Type 1 crimes are more technical in nature like bots Trojans or phishing

[1] Crowther, G. A. (2017). National Defense and the Cyber Domain. *The Heritage Foundation*, 83-97.

[2] Chang, Y. C. (2012). *Cybercrime in the Greater China Region: Regulatory responses and crime prevention across the Taiwan Strait*. Edward Elgar Publishing.

[3] Katos, V., & Bednar, P. M. (2008). A cyber-crime investigation framework. *Computer Standards & Interfaces*, *30*(4), 223-228.

scams. On the other hand, Type 2 crimes include; sexual harassment, black mailing, planning terrorist activities online. These types of crimes are facilitated using different chat software.[4]

Others presented two particular terminologies for categorizing cybercrime; "cyber-dependent crime" and "cyber-enabled crime".[5] Cyber-dependent crime is conducted with and through the engagement of the computers or other forms of information technology; including crimes encompassing hacking, denial of service attacks or insertion of malicious and mischievous software. Cyber-dependent crimes are ones that would not be possible without the use of cyber technology. Cyber-enabled crimes are preexisting types of crime that are enhanced in scope and intensity thorough the internet. Economic and social networking fraud falls under this category. There are many different kinds of "cyber-enabled" crimes, from white-collar crimes like fraud, identity theft, and the theft of electronic information for commercial gain to drug trafficking, harassment, stalking, and other dangerous actions. Even though these things have always been illegal, they are much easier to do now with a computer.

Grabosky categorized three general types of computer crimes based on his research into legislation and the common law: crimes in which the computer is used as the instrument of the crime, crimes in which the computer is an incidental part of the offence, and crimes in which the computer is the target of the crime. Although incomplete, these classifications are important for understanding cybercrime.[6]

Cybercrimes can be also categories into three group according to its target, including:

- Individual: It is a cybercrime for a single person to spread harmful or illegal information over the internet. For example, distributing pornographic material, selling people, and stalking people online;
- Property: This type of cybercrime involves getting people's bank or credit card information, using their money, making online purchases, or using phishing schemes to get people to give out personal information; or
- Government/organization: Even though these cybercrimes don't happen very often, they are still considered serious crimes. It involves breaking into government databases and hacking official websites.

Smith classifies cybercrimes as semantic, syntactic and blended.[7] Semantic crimes refer to social networking, syntactic crimes are purely technical and often involve self-replicating viruses that the victim unwittingly opens, as often seen in ransomware attacks, and blended crimes combine elements of both. The strategy often employed in blended crimes involves the perpetrator contacting the victim and offering the solution to a plausible problem persuasively enough that the victim willingly provides access to personal and financial information to the criminal. In this case, the personal information stolen from victims is sold and used to commit further frauds.

Cybercriminals can do a lot of damage to businesses by using the internet. In fact, it is now easier and safer for a criminal to disrupt a business by destroying its database through malware.[8]

There are several types of typical cybercrimes. as follows:

- Spamming
- Hacking(Unauthorized access)
- Malware
- Distributed Denial Of Service (DDOS)
- Social engineering and phishing
- Online Identity theft
- Cyber-stalking
- Cyber bulling
- Copyright violation
- File distribution via peer-to-peer networks
- Email scams
- Online gambling
- Child exploitation and maltreatment
- Frauds committed with credit cards
- Data breaches and cyberattacks
- Frauds involving Disaster
- Botnets
- Ransomware

[4] Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in computer virology*, *2*(1), 13-20.
[5] Gordon, S., & Ford, R. (2002). Cyberterrorism?. *Computers & Security*, *21*(7), 636-647.
[6] Grabosky, P. N. (2007). *Electronic crime*. Prentice Hall.
[7] Smith, R. G. (2013). Identity theft and fraud. In *Handbook of internet crime* (pp. 291-319). Willan.
[8] McGuire, M., & Dowling, S. (2013). Cyber-crime: A review of the evidence Summary of key findings and implications Home Office Research Report 75, Home Office, United Kingdom. *October*.

- Publication of Derogatory Materials
- Laundering and Taxation trough E-money
- Cyber Harassment
- Cyber Terrorism
- Industrial espionage

III. IMPACTS OF CYBERCRIMES/THE COSTS OF CYBERCRIMES

According to Cybersecurity Ventures, during the next five years, the cost of cybercrime would increase by 15% yearly, reaching $10.5 trillion USD annually by 2025 from $3 trillion USD in 2015. This is the largest transfer of economic wealth in human history, threatens the incentives for innovation and investment, is tenfold greater than the annual damage caused by natural disasters, and will be more profitable than the global trade of all major illegal narcotics combined. Cybercrime costs include data damage and destruction, stolen funds, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption of business operations, forensic investigation, restoration and deletion of hacked data and systems, and reputational damage.[9]

In November 2019, the Accenture "Cost of Cybercrime" study indicated that the average annual costs businesses were incurring was ballooning for various types of cybercrimes. For instance, a single malware attack in 2018 costed businesses more than $2.6 million. Additionally, ransomware costs increased the most between 2017–2018, rising by 21% from $533,000 to $646,000. There have also been predictions that cybercrime will cost the world $10.5 trillion annually by the year 2025.[10] Examining the costs and losses of cybercrime, analysts at Costs of Cyber Crime Working Group emphasize the complexity of their measurement and further use in international regulation. Three categories are suggested for the expenses: costs associated with anticipating cybercrime; costs associated with cybercrime's effects; and costs associated with responding to cybercrime.[11]

Recent theoretical and practical advances have produced alternative views of forms, prevention and recovery costs of cybercrime. In 2016, cybercrime cost the global economy more than $450 billion.[12] Due to such a situation and an increasing operational risk, it is vital to understand the importance of the investment in the information security.

The high-tech crime costs the global economy trillions of dollars per an annum. Those are estimated results, while many believe that the consequences are far more dramatic. The internet is assumed as a critical infrastructure and its missing can catastrophically impact the entire countries and their nations. Indeed, talking about the cybercrime is not the matter of the media's stories as there should be taken much serious actions in order to combat that criminality. At the moment, only the very few countries in the world give promising signals, while the rest still waits for someone to wake them up. Apparently, the socio-economical impacts to communities are more than critical and if we do not raise awareness fully and do not take so powerful actions we can expect a crisis in the virtual environment that can affect both - our physical lives and businesses.

Cybercrime is increasing because it pays, it can be easy, and the risk to cybercriminals can be low. Although cyber law enforcement has also improved, the most sophisticated cybercriminals usually escape arrest prosecution and jail time. Cybercrime is also increasing because we rely on cyberspace to conduct our daily lives and business. Faster adoption of new technologies by cybercriminals - artificial intelligence, synthetically generated images like deep fakes, and more - gives them an edge and explains some of this increase. The bottom line is that cybercrime is safe and profitable, occurs in an environment that is constantly expanding, and thrives in vulnerable systems.[13]

Cybercrime has many hidden costs, ranging from opportunity costs, time and money spent on cybersecurity decision-making, the effect of downtime, loss of productivity, and damage to brand and image. Most of these costs do not have an easily assigned dollar value, but we must consider them in assessing the effect of cybercrime.

Cybercrimes also have negative effects on some key sectors, such as: Government sector - Government services are a tempting target for state actors, cybercriminals, and hacktivists; Healthcare - Medical records often contain financial details and social security numbers in addition to confidential and sensitive health information, making the health sector a particularly appealing target for cybercriminals. Hospitals also often rely on poorly secured systems that are vital to their operations, so the healthcare sector has been a ripe target for cybercrime; or Financial sector - Cybercriminals are naturally attracted to the financial sector. It is, after all, where the money is. That there have been fewer dramatic successes is a tribute to the intense effort the sector has put into cybersecurity both at individual institutions and collectively.

---

[9] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[10] https://www.entrepreneur.com/business-news/cybercrime-could-cost-the-world-105-trillion-annually-by/364015

[11] Sviatun, O., Goncharuk, O., Chernysh, R., Kuzmenko, O., & Kozych, I. (2021). Combating cybercrime: economic and legal aspects. *WSEAS Transactions on Business and Economics*, *18*, 751-762.

[12] Kuklytė, J. (2017). Challenges and vulnerabilities of analysing cybercrime costs. *European Journal of Business Science and Technology*, *3*(2), 81-89.

[13] Smith, Z. M., & Lostri, E. (2020). *The hidden costs of cybercrime*. McAfee.

IV. REGULATIONS COMBATING CYBERCRIMES

Some of the most significant international regulations regarding cybercrimes are:

1. The Council of Europe's 2001 Convention on Cybercrime, often referred to as the Budapest Convention is a multi-national agreement that now provides for the prosecution of cybercriminals and represents a significant attempt to govern cyberspace.

The Council of Europe's Convention on Cybercrime (the Convention) has four parts: Chapter I outlines the terms used, Chapter II details the national actions to be performed, including substantive criminal law and procedural legislation, Chapter III lays out broad guidelines for international cooperation and mutual aid, and Chapter IV covers other issues including ratification of the Convention.

The Convention lists four chapters in terms of substantive laws: (1) offences against the confidentiality, integrity, and availability of computer data and systems, including unauthorized access to a computer system, intercepting private computer data transmissions to, from, or within a computer system, interfering with computer data; interfering with computer systems, including computer sabotage; and abusing computer-related devices; (2) offences involving computers, including those that include fraud and forgery when done through a computer system; (3) offences involving material, to prevent the use of computers as platforms for the sexual exploitation of children, as well as acts of racism or xenophobia, (4) Crimes involving the violation of copyright and related rights. The Convention also makes it clear that international cooperation is to be provided among contracting states 'to the widest extent possible'. This principle requires them to provide extensive cooperation and to minimize impediments to the rapid flow of information and evidence.

2. United Nations Convention against Transnational Organized Crime.

The goal of this United Nations Convention, which went into effect in 2003, is to strengthen international collaboration between governments and their protection against organised crime in general. Although it does not mention cybercrime specifically, it is believed to be of great assistance in this regard, as cybercrime is linked to organised crime and this convention gives a wealth of information on crime preventive methods and cooperation in combating the same. In addition, it comprises specific investigative tactics, the transfer of criminal procedures, the protection of witnesses, and the support and protection of victims.

3. Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems

The scope of the Cybercrime Convention, as well as its substantive, procedural, and international cooperation elements, will be expanded by this protocol in order to include offences of racist or xenophobic propaganda. So, in addition to unifying the substantive law aspects of such behaviour, the Protocol strives to increase the members' capacity to utilise the methods and opportunities for international cooperation outlined in the Convention.

4. Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse

It was necessary to establish a convention to safeguard children from sexual exploitation and abuse given the importance of protecting children and, on the other hand, the abuse perpetrated against them, as prostitution and child pornography are two of these crimes that are becoming more common and pervasive. The convention's Article 1 "Purposes" said that its goals were to "encourage national and international cooperation against sexual exploitation and sexual abuse of children, prevent and combat sexual exploitation and sexual abuse of children, and defend the rights of child victims of such abuse."

5. In addition, European Union is actively involved in the process of combating and preventing cybercrime through continuous and adapted measures and actions by issuing directives such as

- The convention on the Prevention of Terrorism in 2005.
- Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual exploitation of children and child pornography.
- Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems by which Member States are required to introduce more severe criminal sanctions and to strengthen their national laws.
- Proposals for Regulation and Directive facilitating cross-border access to electronic evidence for criminal investigation in 2018
- EU Directive 2019/713 of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment.

For each country's security and economic prosperity, key information infrastructure protection and cyber security are crucial. Because of this, some of the key international organisations that are actively tackling this issue on a constant basis have made cyber security a top priority.

The Global Cyber Security Agenda of the International Union of Telecommunications provides a framework for international cooperation and conversation in order to coordinate global responses to the growing threats to cyber security and to improve the safety and security of the information society. There are five key pillars that support the Agenda: Organizational structures, capacity building, legal measures, technical and procedural procedures, and international cooperation. According to this Agenda, the legal aspects should focus on the means by which the state will address the legal issues posed by criminal activities in

a manner that is compliant with international law. In addition, technical and procedural procedures should emphasize essential steps for promoting and adopting a strategy aimed at enhancing cyberspace security and risk management, such as accreditation schemes, protocols, and standards. Organizational structures refer to preventing, detecting, responding to, and managing cyber assaults, as well as protecting the systems of key information infrastructure. Developing plans for capacity-building methods that raise awareness, transmit knowledge, and increase cyber security should be the goal of capacity building. Finally, international collaboration involves cooperation, consultation, and coordination in the face of cyber threats.[14]

V. IMPLICATION FOR PREVENTION CYBERCRIMES

It is commonly acknowledged that a global agreement with universal application is necessary to combat transnational cybercrime. It is not surprising that ensuring that there is a plan in place for preventing and responding to information technology security incidents is key to successfully managing one when the time comes. In the same manner that criminals utilise social media to commit crimes, technological innovations can be used to manage, dissuade, protect, and prosecute illegal activity. On the one hand, offenders can use social media sites to search for potential victims; on the other hand, law enforcement agencies can utilise similar media to push charges against perpetrators.

Furthermore, in order to combat cybercrimes effectively, it is pivotal that the existing laws must be updated regularly. Cybercrime laws must be more detailed and unambiguous in order to avoid doubts about their applicability when dealing with court proceedings and criminal verdicts specifically for these offences. In addition, the continuous work of international organizations and agencies, which increases the efficiency of cooperation between countries the social awareness for the protection and prevention of cybercrime, through various different initiatives is crucial. States must have the political will and the right management on which depends the proper provision of cyber security. In turn, proper management necessitates the redistribution of duties and the improvement of coordinating systems. When a country is in a permanent state of conflict and the potential of a catastrophic cyber-attack is considerable, its resources should be mobilized to refine and strengthen the existing organizational framework.

VI. CONCLUSION

The development of technology has been a major step in improving lives, but it has provided new opportunities for criminals to commit illegal actions, especially through the Internet, which has allowed them to operate anonymously and even remotely. The phenomenon of cybercrime has become more and more present in the lives of individuals and organizations

In order to combat cybercrimes effectively, it is pivotal to update the existing laws regularly and clearly in order not to doubt its applicability when dealing with cybercrimes. In addition, the cooperation of international organizations, agencies and countries is also important.

REFERENCES

1) Chang, Y. C. (2012). Cybercrime in the Greater China Region: Regulatory responses and crime prevention across the Taiwan Strait. Edward Elgar Publishing.
2) Crowther, G. A. (2017). National Defense and the Cyber Domain. The Heritage Foundation, 83-97.
3) Gordon, S., & Ford, R. (2002). Cyberterrorism?. Computers & Security, 21(7), 636-647.
4) Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in computer virology, 2(1), 13-20.
5) Grabosky, P. N. (2007). Electronic crime. Prentice Hall.
6) https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
7) https://www.entrepreneur.com/business-news/cybercrime-could-cost-the-world-105-trillion-annually-by/364015
8) Katos, V., & Bednar, P. M. (2008). A cyber-crime investigation framework. Computer Standards & Interfaces, 30(4), 223-228.
9) Kuklytė, J. (2017). Challenges and vulnerabilities of analysing cybercrime costs. European Journal of Business Science and Technology, 3(2), 81-89.
10) McGuire, M., & Dowling, S. (2013). Cyber-crime: A review of the evidence Summary of key findings and implications Home Office Research Report 75, Home Office, United Kingdom. October. 30p.
11) Smith, R. G. (2013). Identity theft and fraud. In Handbook of internet crime (pp. 291-319). Willan.
12) Smith, Z. M., & Lostri, E. (2020). The hidden costs of cybercrime. McAfee.
13) Sviatun, O., Goncharuk, O., Chernysh, R., Kuzmenko, O., & Kozych, I. (2021). Combating cybercrime: economic and legal aspects. WSEAS Transactions on Business and Economics, 18, 751-762.
14) Taneski, N., & Karovska Andonovska, B. (2020). Legal aspects of security in cyberspace. Security Dialogues–International Peer Reviewed, 11(1), 99-110.

[14] Taneski, N., & Karovska Andonovska, B. (2020). Legal aspects of security in cyberspace. *Security Dialogues–International Peer Reviewed*, *11*(1), 99-110.