INTERNATIONAL COOPERATION BETWEEN VIETNAM AND OTHER COUNTRIES IN ASEAN IN COMBATING CYBERCRIME: STATUS QUO, CHALLENGES AND ORIENTATION OF LEGAL PERFECTION

Abstract: Cyber security has become more heated problems of non-traditional security than ever before. There are over 400 million internet users in ASEAN region, including 30 million ones in Vietnam. This has been an ideal place for cyber attacks, especially for cybercrime. It is demanding to determine both crimes and victims since those activities are occurring not only within the domestic area but also region and worldwide. Hence, it requires a long-lasting practical cooperation of a lot of countries to deal with cybercrime and protect users in order to maintain e-commerce advancement stably. The article focuses on clarifying some aspects of status quo of cybercrime in Vietnam and some other countries in ASEAN as well as showing challenges and proposing some recommendations in perfecting legal system relating to this cooperative activity in the forthcoming time.

Key words: cybercrime; international cooperation; legal perfection

I. Introduction

International cooperation in the fight against crime, which is generally founded on international law, encompasses all required actions taken by members of the international community to prevent, punish, and eradicate crime from both international and national life. Cybercriminals, often known as computer criminals, utilize computers as a tool for additional illicit activities such identity theft, fraud, trafficking in child pornographic material, intellectual property, and other crimes against privacy. As computers become the core of government, entertainment, and commerce, cybercrime, particularly on the Internet, is becoming more significant.

In fact, because the internet is now accessible practically everywhere in the world, this is a crime type that is worldwide in character, meaning that it can be

committed on the soil of one or more countries. today's modern world. Therefore, resolving this issue demands strong international cooperation in addition to being a shared responsibility of one country. The ASEAN area, which includes Vietnam, is likewise evolving into the perfect breeding ground for cybercriminals and the delectable targets they hunt.

II. Status quo of international cooperation between Vietnam and ASEAN in combating cybercrime

1. Criminal situation

According to INTERPOL, cybercrime is evolving into a significant global problem with an estimated 400 billion USD in losses per year, more than double what drug trafficking criminals make. A high-tech crime is perpetrated every 14 seconds. Because of the broad adoption of the Internet, a trend of high-tech crime that crosses international borders without being detected is on the rise. This crime leaves significant damage and is very hard to track down. Anywhere that has access to the Internet is vulnerable to attack and invasion from cybercrime. Cybercrime acts spread fast and widely across the globe with the use of the Internet. Because criminals can commit crimes in numerous locations, there are a great number of victims and extensive property damage.

There are numerous potential hazards to Vietnam's national security, social order, and safety when computer network security and safety are violated. After terrorism-related crimes, high-tech crimes are the second most serious category of crimes, and Vietnam is among the top 7 countries in the world for cyberthreat activities. With the connection between local and foreign criminals through attack tactics, the number of cases where the subject uses the internet to perform high-tech crimes is growing daily and getting more complex. Phishing (phishing), defacing (intrusion), malware (malware), etc. are attacks on the system that target the user. In the period 2010–2019, there were 207,353 attacks on Vietnam, of which phishing

was 29,059 cases (14.01%), deface was 105,971 cases (51.11%), and malware was 72,323 cases (34.88%).

In the first, second, and third quarters of 2020, there were around 2.7 million ransomware assaults in ASEAN, with Indonesia receiving 1.3 million of those attacks. Ransomware frequently targets the manufacturing, retail, government, healthcare, and construction sectors of the economy. The subjects frequently step up their attacks on medical facilities, administrative offices, and hospitals, particularly in light of the COVID-19 pandemic.

That is only one of the few strategies used by people to compromise the security and safety of computer networks while utilizing cutting-edge technology. Additional techniques include leveraging computer networks for theft, buying and selling, using fraudulent credit cards unlawfully, and taking advantage of sales on online exchanges to defraud. Fraudulently obtaining personal information using spyware to appropriate property, scamming property in the form of online friendships or phony love, or fraudulently selling counterfeit goods, subpar goods, or moving money in advance to an account to appropriate without delivery.

2. Current international cooperation

High-tech crime is also international, following the trend of the globalization of the world economy. Vietnam is home to a wide range of high-tech crimes that threaten the country's economy, political stability, and social order and safety. In order to combat this kind of crime, there must be international coordination and cooperation. In addition, several nations have provided Vietnam with a lot of equipment assistance. In the meantime, Vietnam actively collaborates with ASEAN to organize training on skills for authorities and soldiers in Vietnam for gathering, conserving, recovering, and evaluating data and electronic evidence. Those with experience using cutting-edge technologies to investigate crimes, regularly sending representatives to ASEAN-regional conferences and seminars on cyber security

helps to develop capacity and trust in this area. The Police Department for High-Tech Crime Prevention Vietnam has also set up hotlines with a number of agencies and joined the "G8 Communication Network" on high-tech crime prevention and control, which includes 67 nations and other foreign law enforcements.

It is obvious that without the cooperation of the Vietnamese authorities and with the support of the relevant national judicial authorities, it is impossible to carry out criminal prosecution, conduct investigation, prosecution, and adjudication activities against foreigners committing crimes or Vietnamese committing crimes who are abroad. Vietnam has increased collaboration with other nations since 2010 and has received and processed close to 100 pieces of information about cybercrime while carrying out the duties and functions of crime prevention and combat.

Vietnam has worked with other nations worldwide, including ASEAN, to carry out investigation actions pertaining to cybercrime. Through the practical survey, it was discovered that the following international cooperation activities are frequently used in the process of investigating cybercrime:

- Coordinating, at a party's request, the gathering and verification of data and documents for the purpose of identifying and looking into cybercrime This is regarded as one of the standard guidelines for cooperation between the Vietnamese police force and those of other nations. The range of documents related to cybercrime that must be verified is enormous. It can involve checking the IP addresses that offenders use to commit crimes.

- Coordinating verification to find high-tech criminals who are hiding, subjects with arrest warrants, wanted people for high-tech crimes, INTERPOL, and ASEANAPOL. An agreement on cooperation in criminal justice and extradition for cybercrime was signed by all parties. The Vietnamese Those's Police and the police forces of other nations are working closely together to find and apprehend people who are wanted on an international level and who commit crimes using cutting-edge

technology. The quantity of requests from INTERPOL, ASEANAPOL, or other foreign police forces that the Vietnamese People's Police force receives reflects this.

In particular, they work closely together within the frameworks of the ASEAN Ministerial Meeting on Transnational Crime Prevention and Control (AMMTC), the ASEAN Ministerial Conference on Cybersecurity (AMCC), the ASEAN Police Commanders' Meeting (ASEANAPOL), and other regional political and security cooperation mechanisms to prevent and combat transnational crimes.

Defense relations between the two nations have recently been fascinating, as seen by the Agreement on Bilateral Defense Cooperation (August 2008) and the Letter of Intent on Defense Cooperation (February 2015). promote and produce real outcomes in a variety of fields. Exchanges of delegations at all levels, as well as exchanges, training, and experience sharing across the army and branches, all serve to preserve defense cooperation. Cooperation in security is continually marketed. The two parties improved information sharing pertaining to the prevention and management of transnational crime, cybercrime, and terrorism. An agreement on cooperation in preventing and combatting transnational crimes was reached by the two parties in 2015.

III. Challenges ahead

The cooperation partnership will be demonstrated in the next years as Vietnam and the other ASEAN nations deal with complex advancements in crime, particularly high-tech crimes. The following challenges will also be faced by some of the specialist forces:

Firstly, a serious crime that results from this kind of crime can be committed anywhere in the world as long as there is an internet connection. The operation's reach is broad, making it difficult to identify the victim. It must also be simple to gauge the severity of the repercussions. The investigation and combat against this kind of crime also confront numerous difficulties because it is also utilized as a

means of money laundering, financing for terrorism, etc. There is no agreement on how nations should handle this kind of crime, and developing nations like those in the ASEAN region have not yet gained expertise in dealing with cases of high-tech crimes. much.

Secondly, cyberspace approaches and methods of cooperation do not generally agree. Many nations are currently calling for broader adherence to the Budapest Convention's procedures. Still, there are differing perspectives on this tradition. Some nations voiced concern that because they did not take part in the convention's negotiation process, their national interests were not adequately represented. They argued that a new, more inclusive convention was required. The Budapest Convention, according to Russia, China, and Brazil, contains some virtues but cannot be viewed as a universal agreement on cybercrime.

Thirdly, there are still disparities between countries' capacities and levels for ensuring cyberspace. Due to limited capability and information technology infrastructure, countries have historically had trouble responding to, preventing, and defeating cyber threats. Legal documents on measures and fines are frequently promulgated slowly, so by the time they are released they are out of date in comparison to the newest news tactics. Between-authorities rigorous coordination is lacking.

Fourthly, collaboration and conflict between agents have the properties of two opposing forces acting concurrently. However, it is generally agreed that in international relations today, collaboration is seen as being more important than conflict. In fact, the partnerships between the two organizations stated above emphasize cooperation, information exchange, and corporate network security expertise in their agreements and contracts that set forth how cybersecurity cooperation would be carried out. Each agreement's scope of cooperation is

dependent on the state of relations between the parties and has not yet been implemented.

Fifthly, a number of ASEAN nations, including Vietnam, lack cybersecurity legal frameworks and have not kept up with the quick developments in cyberspace and the constantly changing nature of cybercrime both intricate and sophisticated. There is still no uniform legal framework guiding regional cooperation efforts in the fight against and prevention of cybercrime within ASEAN. New nations first concentrated on creating their own laws, and there are still some distinctions in each nation's legal perspectives. Additionally, lack of technology advancements is a hindrance in the effort.

IV. Some recommendations

Occurrences and incidents related to the security environment in cyberspace are also very complex in Vietnam and other ASEAN nations. Cyberattacks by hostile forces and cybercriminals, who use the internet, particularly social networking sites, and a variety of sophisticated techniques and tactics for financial gain and other negative ends, are constantly increasing.

The domains of technology, information, and the digital economy are becoming more and more crucial to the overall growth in the contexts of long-term innovation, global integration, and socioeconomic development. While important for socioeconomic development, national sovereignty and security, regime stability, social order and safety, etc. are only a few of the complicated and unpredictable variables that the topic of cybersecurity and cyberspace also involves. Vietnam and the ASEAN nations must have the right policies in place to address these issues while simultaneously enhancing the efficacy of cyber security assurance to ensure safety. With the aim of ensuring and enhancing social order, cyberspace safety, regime security, and national security, the following recommendations are suggested:

First, ASEAN member states must perfect the legislative framework for ensuring cyber security in order to advance cybersecurity and safeguard national sovereignty and interests online. Protecting national sovereignty involves securing control over cyberspace in addition to physical territory, the sea, the air, and other spheres of influence. The entire political system has an urgent and lengthy duty to do. It plays a crucial role in the development of a secure and stable national cyberspace, bringing about advancements in national building and defense. To accomplish these aims, we must develop the technical and human resources necessary to guarantee network security, successfully combat cyberattacks and cybercrime, and uphold national sovereignty in cyberspace. Assuring network security, protecting national sovereignty in cyberspace, taking part in international collaboration in the field of cyberspace, while avoiding getting entangled in international rivalry, are all important considerations in the formation of policies in the field of cyber security. These components work together harmoniously to strengthen and complement one another. To ensure the efficacy of the network security policy, a comprehensive approach to implementation is therefore required.

Second, improve regional coordination and promote, monitor, and support cybersecurity. Given the disparities in actual technical capability and national perspectives on cybersecurity, it is anticipated that there would be significant challenges in the discussion and implementation of cyber security law. Therefore, a variety of stakeholders must take part in this process. Some nations have even suggested that the global discussion on cybersecurity challenges be put on hold to ensure effectiveness. Countries should instead concentrate on debates in regional forums.

Therefore, despite increasing global and regional cybersecurity collaboration both multilaterally and bilaterally, it is important to consider the likelihood of a stalemate in the elaboration of global laws and practices. The next step is to decide

how much Vietnam should participate in this framework, while also concentrating resources and energy on relevant structures for collaboration that offer immediate advantages for Vietnam as well as promising futures. make strides. ARF and ASEAN are currently two security cooperation institutions in the region with many important partners of Vietnam, including not just neighbors but also significant nations that have a role and influence in the region and globally, such as the US, Russia, China, Japan, and others. For Vietnam, the security situation is also tight. Prioritizing and concentrating resources on these two mechanisms thus has a broad range of significant influence.

Third, strongly encourage global cybersecurity collaboration. Since these processes are still in their early stages, ASEAN countries have the conditions and opportunities to: 1-Build partnerships and join multilateral institutions to strengthen collective action and cooperation in preventing and combating common cybersecurity threats; 2-Promote cooperation, collective action, and response to cyber incidents, contributing to incident resolution and preventing harmful activities in cyberspace.

Currently, governments are paying special attention to the issue of cybersecurity, but there is still disagreement among nations, particularly among large nations, on many other subjects. As a result, in addition to channel 1 diplomatic forums (14), channel 2 diplomacy actions on cybersecurity are vital in fostering communication, mutual trust, and understanding between nations on fundamental ideas as well as contentious topics connected to the sphere of cyberspace. Therefore, utilize channel 2 diplomatic networks like ISIS, the Network of ASEAN Institutes of International and Strategic Studies (ASEAN-ARF), and the Council for Security Cooperation in Asia-Pacific (CSCAP-channel 2 of ARF). Hence, it is essential to encourage the convergence of cybersecurity understanding and practices among ASEAN nations, and work toward the creation of similar legal frameworks to make

international coordination and collaboration in the security sector easier. The construction of the ASEAN Cybersecurity Center was tightly coordinated. With the aid of discussion partner nations with expertise in this area, establish an ASEAN-wide, extensive training cooperation structure (China, Japan, Korea,…).

In order to protect network security and safety as well as the privacy of information in a network environment, it is important to develop mechanisms and policies. At the same time, it is important to make sure that management measures do not violate the legitimate rights and interests of individuals. Through international treaties, cooperation agreements, memorandums of understanding, hotlines, direct communication channels, etc., establish a coordination mechanism to improve the effectiveness of dealing with cybercrimes and high-tech crimes between law enforcement agencies of the two countries in order to promptly coordinate, respond to, and handle incidents of cyberattacks and law violations in cyberspace that happen very quickly and unpredictably./.

REFERENCE

1. Report on violations and high-tech crimes in Hanoi city - PC50 – Hanoi, Vietnam

2. Decree No. 25/2014/ND-CP of the Government - Regulations on prevention and combat of crimes and other law violations using high technology

3. Decree 25/2014/ND-CP on prevention and combat of crime and other law violations using high technology

4. https://backan.gov.vn/pages/viet-nam--singapore-hop-tac-phong-chong-toi-pham-mang-6f9b.aspx <access 10 Oct 2022>

5. VNISA (2018), Overview Report Vietnam Information Security Day 2018, https://drive.google.com/file/d/12DgkTjdNxLHdZeqxSD5bUuZTxXzyxMme/view

6. Các quốc gia có nguồn tấn công vào Việt Nam nhiều nhất, http://www.vncert.gov.vn/baiviet.php?id=20, <access 11 Oct 2022>

7. View: https://luatvietnam.vn/an-ninh-quoc-gia/chi-thi-14-ct-ttg-2019-bao-dam-an-ninh-mang-de-cai-thien-chi-so-xep-hang-173482-d1.html

8. Law on Cyber Security, Vietnam, 2018

9. Textbook on International law, People's Security Academy, 2021

10. Report on Cyber Security in Vietnam, People's Security Academy 2020.

11. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security <access 10 Oct 2022>