DOI: http://dx.doi.org/10.26483/ijarcs.v10i3.6414

ISSN No. 0976-5697

Volume 10, No. 3, May-June 2019

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

CYBERCRIME IN LEGISLATIVE PERSPECTIVES: A COMPARATIVE ANALYSIS BETWEEN THE BUDAPEST CONVENTION AND VIETNAM REGULATIONS

Hai Thanh Luong (PhD)
School of Global, Urban and Social Studies
RMIT University, Melbourne, Australia

Huy Duc Phan (MA)
Department of Criminal Investigation
Ministry of Public Security of Vietnam

Chu Van Dung (PhD)
Department of Criminal Investigation
Ministry of Public Security of Vietnam

Abstract: As one of the emergent countries in the Southeast Asia region facing to practical threats and potential risks from various types of cybercrimes, Vietnam has been continuing to improve their responsibilities and legislations to prevent, control and combat cyber-related crimes. The new Criminal Law of Vietnam (CCV) took effects in January 2018 with a number of specific points to legalize and penalize cybercrime's activities. Although this code is expected to be more effective than its precedence in combatting the impact of cybercrime, we are yet to ascertain whether the new code appropriately define cybercrime as per the common minimum standards stipulated by the Council of Europe's Convention on Cybercrime. This paper uses the comparative legal research to compare the definition of cybercrime with its related regulations in CCV with that of European Convention. Findings pointed out although CCV 2015 has sufficiently criminalised several criminal acts committed online such as illegal access, system interference, and computer related fraud; it has failed to criminalise other equally dangerous criminal acts committed using its cyberspace. The acts of data interference, computer – related forgery, misuse of device and child pornography are still not coded properly under the CCV to create massive loopholes in Vietnam's legal framework. Some practical recommendations also call for further updates and researches.

Keywords: cybercrime; cybersecurity; cyberspace; criminal law; Convention of Cybercrime; Vietnam

I. CYBERCRIME LEGISLATION

The European Convention on Cybercrime (CoC), also known as the Budapest Convention, is the first and the only multinational instrument to address cybercrime issue so far. The Convention was drafted by the Council of Europe together with the effective contribution of the United States, Japan, South Africa and Canada. The CoC were adopted by the Committee of Ministers of the Council of Europe on 8th November 2001 and opened for signature in Budapest on 23rd November 2001 and entered into force on 1st July 2004. It was supplemented by an additional protocol that focuses on the dissemination of racist and xenophobic materials via computers. The Additional Protocol opened on 28th January 2003 and came into force on 1st March 2006. To date, 47 countries European countries have singed and/or ratified the CoC and 29 countries have ratified the additional Protocol and is also globally recognized as a pillar of the international legal framework for combating cybercrime [1, 2]. It has established a solid foundation for cybercrime legislation in many countries and enabled the harmonization of different national laws [3, 4].

However, according to the latest survey about cybercrime legislation worldwide of United Nations Conference on Trade and Development [5], there are 138 countries, of which 95 are developing and transition economies, had passed their legislation; meanwhile more than 30 countries either do not have cybercrime legislation or are still working on drafting such laws. Additionally, there are still some disparities in these legislations as compared to the CoC and established its international scope rather than regional, status. Yilma [6] analysed the development of cybercrime legislation in Ethiopia and pointed out the Ethiopia as well as many other African countries has been remarkably sluggish to criminalize cybercrime and its cybercrime legal regime is defragmenting. The author also recommended that the government should build a draft law encompassing popular types of cybercrime according to the CoC. In the European region, when comparing between Lithuanian Criminal Code and the CoC, which Lithuania ratified the Convention as an official member, Sauliunas [7] pointed out significant disparities in accordance with the Convention. For instances, some illegal activities under the Convention as illegal access and computer-related forgery remain outside the scope of the Lithuanian Criminal Code [7]. On the other hand, another study of Moise [8] conducted in Romani showed that Romanian cybercrime legislation, including the Criminal Code as well as the Law no.161/2003 on some measures to ensure transparency to exercise public dignities, public office and business environment, prevention and to sanction corruption and its prevention and combating, is compatible with the majority of legal mechanisms at the European level, especially the CoC. Within the scope of comparative law across between Asia, Euro, and Americas' representatives, Wang [9] selected China and Singapore for first one, England for second one, and the United States of America for last one, to analyse differences and similarities among of legislative regulations. Case-by-case approaching from these legislative systems, the author concluded that the CoC is an international legal standard

© 2015-19, IJARCS All Rights Reserved

against cybercrime whereby each studied legislative approach has its own advantages and disadvantages and more importantly, this paper also pointed out the current China criminal laws causes many problems and therefore, it is necessary to have cyber-specific criminal law [9].

In recent time, while the Southeast Asian region has been becoming increasingly to develop and apply ICT and its related application such as the Internet users and smartphones, it is tough to look for reliable data to show the negative impact of cybercrime and its specific forms on living [10, 11]. Even, to date, there is not any systematic analysis and scientific research through survey or report that deal with cybercrime in Asia [4, 12, 13]. Yet, as of April 2018, though there are at least 25 countries signed and ratified the European CoC as non-state Members, no ASEAN country follows it as being the first state. Thus, the key to ensure the effectiveness of combating cybercrime in this region, as Broadhurst and Chang [2] proposed that, there is at least to build a laws against cybercrime with its relevant regulations based on each countries and the whole of area. In comparison to the rest of countries in the Asian region, numerous comparative legal researches have been conducted to evaluate and compare the cybercrime legislation in the world, however none has yet ㄱㅗ″ㅇㅣˇ¸ on the Vietnam's context. Therefore, the main purpose of paper is focus on raise the legislative approaches and its related regulation about provisions, visions, and law enforcement's responses of Vietnam to address this battle. It will be delivered straightaway after providing very briefly about the current situation of cybercrime and its related forms in Vietnam.

II. VIETNAM CONTEXT

Cybercrime in Vietnam has its origin since early nineties and got impetus when first commercial Internet service originated in 1997. Within the scope of Vietnamese language and thought, undoubtedly, the phrases of "high-tech crime", "cybercrime", "and computer-related crime" have all been adopted by Vietnamese scholars as a form of advancement of non-traditional crimes. Another term 'crime using high technology' is used more commonly than term 'cybercrime' in varied official documents, in which it is defined as any crime that is stipulated in criminal code and using high technology [13, 14]. According to the Law on Information Technology of Vietnam [15, cited in Article 4], high technology includes information technology and telecommunication, whereby information technology is defined as a collection of modern scientific and technological methods as well as tools for producing, transmitting, collecting, processing, storing and exchanging digital information. As per this understanding crime using high technology could be any crime that uses/misuses high technology to commit crime. However, Duc [16] argues that cybercrime or crime using high technology has been differently understood by Vietnam's criminological researchers. While some researchers consider cybercrime as crimes where the criminals invade the normal operation of computer systems and computer networks, others contend that cybercrime happens when information technology are used as tools to conduct criminal activities [14, 17]. The People's Police Academy, a training center of the Ministry of Public Security of Vietnam give the definition of cybercrime as follows: "Cybercrime are crimes committed by deliberate use of knowledge, skills, tools and means of information technology at high levels to illegally impact on digital information stored, processed, transmitted in the computer system, violate the safety of information, damage the interests of the state, the legitimate rights and interests of organizations and individuals" [18]. All these arguments and statements belong to internal sharing among Vietnamese scholars with its original language which not clear comparison and relevant analysis to other international regulations and regional frameworks in terms of cybercrime. As a result, there is still dearth of research focusing on cybercrime-related activities and its international peer-review publications, except for some short presentation or brief reports at international and regional conferences, workshops or seminars. Perhaps, it is also the one of the specific causes to lead inadequate information and insufficient data to show the current situation of cybercrime in Vietnam for foreign scholars. In other words, as a result, till date there have not been any substantial research from other countries focusing on cybercrime activities in Vietnam region, though Vietnam has been identified as one of the potential targets to attack on cyberspace by hackers and offenders in recent times in the Asia region. The issue has till now evaded the attention of international researchers and whatever little research is done within Vietnam is carried out by legal enforcement officers, limiting their research focus on the specific "acts of crime" rather than the overall legal framework.

This paper is aimed at analysing the definition of cybercrime in CCV 2015, paying special attention to clarifying the possible discrepancies between CCV 2015 and the CoC. The purpose is to identify whether the criminalization of cybercrime in Vietnam Criminal Code would satisfy the requirements of the Convention and then propose recommendations to reform laws against cybercrime in the future. With such objectives, the minor paper asks two research questions, including

1. Are cybercrimes objectively stated in the European Convention on Cybercrime also criminalized in the CCV?

2. How are cyber-related crimes criminalized in the CCV?

Although CCV 2015 is more advanced than all previous Vietnam codes in terms of provisions on cybercrime, there have not been any reports or research to evaluate if it meets the widely accepted minimum demands set by the CoC. It is noticed that Vietnams is not obligated to fulfil all responsibility set by the CoC especially when it has not been a party of the Convention. Additionally, Vietnam and Europe have their own perspectives about crime impacted by social and cultural factors as well as legal traditions. However, it is noticed that cybercrime has become a global problem that almost all countries including European countries and Vietnam cannot escape from. With the advancement of technology, criminals are able to move quickly their activities among countries. Indeed, Vietnam and European countries have experienced many common types of criminal conducts such as spreading virus, denial of service attacks, and identity theft [19]. Furthermore, as cybercrime happens in cyberspace that is not limited by geographical boundaries, cybercrime can be committed in any countries regardless of the physical appearance of perpetrators or victims' locations. For instances,

© 2015-19, IJARCS All Rights Reserved

hackers might attack a computer system in Vietnam while they still stay in Europe and vice versa. Clough [1] asserts that since all countries are facing with the same problem, it is valuable to learn from others in terms of legal frameworks, education and technical solutions. Therefore, a comparison between the CCV 2015 and an "ideal type" like the Convention is reasonable and necessary for the development and reform of Vietnam cybercrime legislation.

III. METHODS

This part aims at giving the explanation for the choice of comparative legal research as the main method of this paper and how this method is carried out to answer research questions. Accordingly, comparative law or comparative legal research is a process of comparing rules of law of different systems [20]. Since nineteenth century, Raymond Saleilles and others saw comparative law mainly as an instrument for improving domestic law and legal doctrine [21]. Van Hoecke [20] contends that the comparison between legal documents have become crucial in doctrinal legal research, especially in the era of globalization. Van Hoecke [20] asserted that "when one tries to improve one's own legal system, be it as a legislator or as a scholar, it has become obvious to look at the other side of the borders". The comparison with legal documents of other systems are able to give the observers a critical view about their laws, help them to see possible difficulties and bring about plans for further developments [22]. Indeed, to improve cybercrime legislation, numerous studies have used the comparative approach to compare the criminal code of a country with others. For instances, with the aim to compare the Lithuania law with the CoC, Sauliunas [7] used a comparative legal analysis and linguistic analysis to discover "several serious gaps in the field of criminalization" between these two instruments. Sepec [23] also used comparative approach to point out the differences between Slovenian Criminal Code with other countries such as Germany, Austria, Finland and United Kingdom. In another research, Markopoulou [24] also used comparative legal research method to point out the gap between Greek criminal code and the COC. The same method is also used by Wang [9] to discover how China criminal law be adapted to regulate cybercrime. Wang [9] analyzed and compared cybercrime legislation of China, Singapore, the United State of America, England and the Council of Europe. Thus, with objective to evaluate Vietnam cybercrime legislation in comparison with the COC, the comparative legal research can be used to point out the disparity between these two legal documents.

To some extent, this paper presents an analysis merely relying on contents of the two legal documents in terms of cybercrime, the Budapest Convention on Cybercrime and Criminal Code of Vietnam 2015 (CCV), and thus, it is basically a doctrinal legal research. The Convention on Cybercrime and its Additional Protocol, and CCV are main primary sources that will be investigated and analyzed. During the process of analyzing the content of specific provision, the opinions from the scholars as well as the legislature and materials accumulated from the previous researches can be explored.

IV. FINDINGS

This chapter presents the key findings from the comparative analysis of CCV and the Budapest Convention and its additional Protocol. The findings are presented in six sections based on key terms and categories of offenses classified by the Convention and its Additional Protocol.

A. The use of terms

Article 1 of the CoC establishes the definitions of four important terms which are adopted throughout the Convention including: 'Computer system', 'Computer data', 'Service provider' and 'Traffic data'. A computer system is defined as a device or a group of devices that processes data automatically according to a program. Computer data refers to any 'representation of facts, information or concepts' including a program that can be processed by a computer system [25]. Service providers are public or private bodies which provide their clients with the ability to communicate via a computer system or entities that store or process computer data on behalf of communication service or users of such service [26]. 'Traffic data' is a sort of computer data relating communication that specify 'the communication's origin, destination, route, time, date, size, duration, or type of underlying service' [25]. Parties of the Convention are not obligated to adopt identically these terms in their domestic laws, but their own concepts must be principally consistent with Article 1 of the CoC [25]. Indeed, many member states of the CoC have introduced these definitions partly in national laws such as Albania, Croatia, France, Lithuania and Slovakia [3].

These key terms are not defined either CCV 2015 or any other legal documents related to cybercrime. Instead, other terms including 'computer networks', 'telecommunication networks', 'electronic devices' and 'electronic data' are used numerous times by the CCV 2015. To understand these terms, however, we have to refer to other legal documents. 'Computer network' is described by Joint Circular number 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC as a collection of connected computers that can share data. This Circular also defines 'Electronic data' as the operating system, software, information contained in electronic device (Article 2). 'Telecommunication network' is described by the Law on Telecommunications 2009 as a set of telecommunications equipment connected by transmission lines to provide telecommunications services and telecommunications application services. 'Electronic devices' have not been defined in any legal document so far. The lack of a united legal document that define all cybercrime-related terms may result in the difficulties in understanding and applying the relevant provisions.

A comparison between definitions of basic terms in the CoC and their equivalents in the Vietnam laws reveals some disparities between them. Vietnam laws uses the term 'computer network' instead of 'computer system' adopted by the CoC. Indeed, computer system is one unit whereas computer network could be a network of many systems. In other words, Vietnam legislature provides the definition of a set without a clear description of its elements. The usage of this term reflects an obsolete and outdated understanding of

© 2015-19, IJARCS All Rights Reserved

communications technologies and their integration. 'The Net' is an outdated term, whereas 'system' enables an appreciation of the dynamic nature of modern technology-mediated communication. The usage of the term 'computer system' facilitates the identification of the rights of the system's owner to the system while it is hard to identify who the administrators of a 'network' is. Moreover, other terms 'service providers' and 'traffic data' are not defined or used in the CCV 2015. The absence of definitions of these key terms is a big challenge to the interpretation and application of domestic laws. Also, as a result of the disparity in key terms, Vietnam might struggle to join the international legal framework on cybercrime as well as cooperate with other law enforcement agencies in mutual legal assistance and extradition.

B. Offences against the confidentiality, integrity and availability of computer data and systems

Title 1 of the CoC includes articles related to 'offences against the confidentiality, integrity and availability of computer data and systems' which are common types of computer-related crimes. As its name, this title aims at dealing with crime harmful to 'confidentiality, integrity and availability of computer data and systems' [25]. It includes five Articles, from Article 2 to Article 6, that contain five types of criminal conducts: 'Illegal access', 'Illegal interception', 'Data interference', 'System interference' and 'Misuse of device'.

1) Illegal access

The activity of illegal access is stipulated in Article 2 of the CoC that demands each party to outlaw the unauthorized access to a computer system. "Access", also called as "hacking" by some jurisdictions, is clearly explained by Explanatory Report to the Convention on Cybercrime as the action of entering a computer system or any elements of computer system such as hardware or traffic data. The mere sending email or file is not considered as 'access.' The Article also exclude authorized access to a computer system such as maintenance or install software. Because the article only requests for the criminalization of the mere entering, there were some opposite ideas arguing that the mere intrusion is not dangerous but help to discover weaknesses of the protection for the computer system. Thus, the Convention allow the signatories to be free to decide whether or not to add some conditions such as 'Infringing security measures' or 'dishonest intent' when they criminalize this activity in their domestic laws [25].

The access without right is criminalized by Article 289 of the CCV 2015 titled "Illegal infiltration into the computer network, telecommunications network, or electronic device of another person". It reads:

> "Any person who deliberately bypasses the warning, hacks the password or firewall, or uses the administrator's right of another person to infiltrate another person's computer network, telecommunications network, or electronic device in order to take control, interfere the operation of the electronic device; steal, change, destroy, fabricate data or illegally use services shall be liable to a fine of from VND 50,000,000 (US$2,500) to VND 300,000,000 (US$15,000) or face a penalty of 01 - 05 years' imprisonment".

In comparison with Article 2 of the Convention, the Article 289 of CCV 2015 describes 'illegal access' in more detail by listing some possible methods to illegally intrude a computer system including "bypasses the warning', 'hacks the password or firewall', and 'uses the administrator's right'. This is a common feature of legislative technique in Vietnam that legislators tend to specify criminal conducts in the content of provision with a view to facilitating law enforcement agencies in handling cybercrime cases. The drafting of the Convention also encourages member states to make their own laws with 'as much clarity and specificity as possible' [25]. However, the act of illegal assess set by Article 289 of CCV 2015 requires an underlying dishonest intent such as taking control; interfering the operation of the object; stealing, changing, destroying, fabricating data; and using services illegally. This is a narrower approach in comparison with Article 2 of the CoC. In short, although the difference in terms 'computer system' and 'computer network' still exist between the compared provisions, it can be concluded that the crime of illegal access stated by the CoC is criminalized properly in CCV 2015.

2) Illegal interception

Article 3 "Illegal interception" of the CoC set the requirement to criminalize the interception that is committed intentionally without right. This provision is built with the aim to ensure protection for the privacy of communication [25]. The violation against the privacy includes 'recording', 'listening to', 'monitoring' or 'surveillance' of the content of communication. It can be conducted by 'technical means' such as setting up devices tied to transmission lines or using devices to 'record wireless communications' [25]. The criminal object of the interception is 'non-public transmissions of computer data'. The term 'non-public transmission' is used to emphasize on the privacy of communication rather than transmitted contents. It means that whether or not the data is private, the private transmission cannot be intercepted [25].

In the CCV 2015, the privacy of information transmission is protected by Article 159 titled 'Infringement upon confidentiality and safety of mail, telephone, telegraph, or other means of private information exchange'. It reads:

> '1. A person who recommits any of the following acts after being disciplined or incurring an administrative penalty shall receive a warning, be liable to a fine of from VND 20,000,000 (US$1,000) to VND 50,000,000 (US$2,500) or face a penalty of up to 03 years' community sentence:
> a) Appropriation of another person's mails, telegraphs, telex, faxes, or other documents which are transmitted on the postal or telecommunications network in any shape or form;
> b) Deliberately damaging, losing, or obtaining another person's mails, telegraphs, telex, faxes, or other documents which are transmitted on the postal or telecommunications network;
> c) Listening or recording conversations illegally;
> d) Searching, confiscating mails or telegraphs illegally;
> dd) Other acts that infringe upon confidentiality and safety of mail, telephone, telegraph or other means of private information exchange.

The conducts of 'listening or recording conversations illegally', that are main criminal conducts in Article 3 of the Convention, are covered literally by the Article 159. Although this article pays attention to the privacy of communication via the portal and telecommunications network, it still encompasses 'others means of private information exchange' and thus, it can be used to deal with illegal interception against

© 2015-19, IJARCS All Rights Reserved

private transmission of computer data such as email and file transfer. Generally speaking, the requirement of the Article 3 on 'illegal interception' is basically satisfied by Article 159 of CCV 2015. Notwithstanding, Article 159 does not focus on the technical aspect of the interception but the privacy of people. As a result, it is put in a chapter on 'Offenses against personal liberty, citizen's rights to freedom and democracy' (Chapter XV).

In case perpetrators acquire the data of transmission by the unauthorized access to computer systems, their actions can be regulated by Article 289 'Illegal infiltration into the computer network, telecommunications network, or electronic device of another person' of the CCV 2015 as above mentioned. According to this article, the activity of stealing data is a subsequent activity of the crime of illegal access.

3) Data interference

The criminalization of data interference is necessitated by Article 4 of the CoC. The aim of this provision is to protect 'the integrity' and 'the proper functioning' of 'computer data' or 'computer programs' [25]. The actions of interfere computer data can be 'damaging, deletion, deterioration, alteration or suppression' that are conducted without right. "Damaging" and "deteriorating" are to alter the integrity of the content negatively. "Deletion" is destructing computer data so that it is unrecognizable. 'Suppressing' means 'prevents or terminates the availability of the data'. "Alteration" is explained as any actions that modifies existing data. Article 4 of the Convention also accepts the addition of 'serious harm' to the equivalent provisions in domestic laws [25].

Actions of data interference are mentioned in Articles 286, 287 and 289 of the CCV 2015. The Paragraph 1 of Article 287 reads:

> 'Any person who deletes, damages, or changes a software program or electronic data, or illegally obstructs the transmission of data of a computer network, telecommunications network, or an electronic device, or otherwise obstructs or disturbs a computer network, telecommunications network, or an electronic device in any of the following cases, except for the cases in Article 286 and Article 289 hereof, shall be liable to a fine of from VND 30,000,000 (US$1,500) to VND 200,000,000 (US$10,000) or face a penalty of 06 -36 months' imprisonment'

The Article criminalizes the actions of deleting, damaging or changing a software program or electronic data as an alternative expression for acts of 'damaging, deletion, deterioration, alteration or suppression of computer data' in the Article 4 of the CoC. In which, the action of deterioration, alteration or suppression can be equated to the act of changing. However, these wrongdoings are not the core criminal actions of Article 287 but obstructing and disturbing a computer network. Deleting, damaging, or changing computer data are only a precedence or a condition or a modus operandi to obstruct and disturb the operation of the targets. As a result, these harmful activities are not prosecuted unless they influence the operation of a computer network. The mere data interference such as deleting a personal photos or document is not the conduct criminalized by the Article 287 of the CCV 2015.

The activities of modifying and damaging computer data are also mentioned as a part of the crime of illegal access that is stipulated in the Article 289 'Illegal infiltration into the computer network, telecommunications network, or electronic device of another person' of CCV 2015. Nonetheless, Article 289 prioritize the protection for the safety of the computer networks, telecommunications network, and electronic devices instead of computer data as required by Article 4 of the CoC. The main criminal conduct regulated by this Article is 'unauthorized access' or 'hacking' instead of modifying or destroying data as in Article 4 of the Convention. In more detail, interfering data is considered a subsequent activity or the 'dishonest intent' of the core action. Thus, there is a significant disparity between the two provisions.

An activity to interfere data is the input of malicious codes such as viruses and Trojan horses that leads to the changes of computer data [25]. This conduct is stipulated in the Article 286 'Spreading software programs harmful for computer networks, telecommunications networks, or electronic devices' of the CCV 2015. Paragraph 1 of this Article reads:

> 'Any person who deliberately spreads a software program that is harmful for a computer network, telecommunications network, or an electronic device in any of the following cases shall be liable to a fine of from VND 50,000,000 (US$2,500) to VND 200,000,000 (US$10,000) or face a penalty of up to 03 years' community sentence or 06 - 36 months' imprisonment'

A harmful program is defined as a program that automates the processing of information, causes abnormal activity for a digital device or copies, modifies or removes information stored in a digital device ("Joint Circular Guiding the Application of Provisions on Crime involving Information Technology and Telecomunications," 2012).

There is a difference between this article and Article 4 of the CoC in terms of criminal objects. The criminal object of the crime in the Article 286 is devices or network instead of computer data as in Article 4 of the CoC. Although it is likely that damaging computer data may result in the abnormal operation of the computer network or system, they are still two separate objects. In many cases, the alteration of computer data does not influence the operation of a network. For instances, deleting a private picture or a video stored in a personal computer which is not connected with other computers does not impact on the operation of the computer. In such cases, the application of Article 286 is inappropriate although that action actually causes harms to 'the integrity of the computer data'.

With all above analysis, it can be concluded that mere interference against computer data have not been criminalized clearly and sufficiently by any specific articles in the CCV 2015. Instead, it is only mentioned as a part or a stage of other types of cybercrime such as spreading harmful software programs and Illegal access. Thus, the requirement of criminalizing the conduct of 'data interference' is not satisfied by the CCV 2015.

4) System interference

Article 5 of the CoC require each party to criminalize the conduct of hindering 'the functioning of a computer system inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data illegally'. The term "hindering" refers to making a computer system function improperly [25].

'System interference' is criminalized by the Article 287 of the CCV 2015 which reads:

> 'Any person who deletes, damages, or changes a software program or electronic data, or illegally obstructs the transmission of data of a computer network,

© 2015-19, IJARCS All Rights Reserved

> telecommunications network, or an electronic device, or otherwise obstructs or disturbs a computer network, telecommunications network, or an electronic device in any of the following cases, except for the cases in Article 286 and Article 289 hereof, shall be liable to a fine of from VND 30,000,000 (US$1,500) to VND 200,000,000 (US$10,000) or face a penalty of 06 - 36 months' imprisonment'.

The conduct of hindering the functioning of a computer system is represented by the actions of obstructing or disturbing the operation of 'a computer network, telecommunications network, or an electronic device' in this Article. Like the Article 5 of the CoC, the obstruction and disturbance must take place by the deletion, damaging, changing of data. Literally, 'system interference' is criminalized adequately by the Article 287 of the CCV 2015. In addition to criminal conducts included in Article 287, the activity of spreading harmful software that cause devastating harm to computer data and computer system is particularly criminalized by the Article 286 of CCV2015. This conduct is also a type of system interference covered by the Article 5 of the Convention [25]. Therefore, with the Article 286 and 289, the crime of system interference is criminalized sufficiently in the CCV 2015.

It is noticed that Vietnam law makers do not only criminalize conducts mentioned in Articles 3 through 5 of the Convention but also require the exact level of consequences caused by these conducts. For instance, Article 289 of the CCV 2015 require that the minimum amount of money earned by perpetrators is from 50 million VND (US$2,500) or the minimum damage caused the crime is at 100 million VND. This supplement aims to facilitate Vietnam law enforcement agencies in identifying exactly whether a violation is a crime or not. Additionally, this way of criminalization emphasizes these offenses as result crimes rather than conduct crimes.

5) Misuse of device

'Misuse of devices' is a crime mentioned in Article 6 of the CoC. The term 'device' in this article is referred to 'a computer program', 'a computer password', 'access code' or 'similar data' that is likely to be used to commit any crimes mentioned in Articles 2 through 5 of the CoC. These devices are an essential part in the process of committing crime. They do not only facilitate the commission of cybercrime but also help perpetrators circumvent investigation and avoid criminal liability [25]. Therefore, it is necessary to constrain the production and dissemination of such devices to prevent cybercrime [25]. This is the goal of Article 6 of the CoC. This Article require each party of the CoC criminalize the activities of 'production, sale, procurement for use, import, distribution, making available of and 'possession' of these devices with intent to use them to commit crimes in Articles 2 through 5 of the CoC.

The CCV 2015 has criminalized these activities by Article 285 "Manufacturing, trading, exchanging, giving instruments, equipment, software serving illegal purposes" which reads:

> "Any person who manufactures, deals in, exchanges, gives out instruments, equipment, or software meant to attack a computer network, telecommunications network, or an electronic device serving illegal purposes shall be liable to a fine of from VND 20,000,000 (US$1,000) to VND 100,000,000 (US$5,000) or face a penalty of up to 02 years' community sentence or 03 - 24 months' imprisonment".

This article marks a significant improvement in Vietnam cyber regulation when producing and trading equipment or software that are used for illegal purposes are criminalized in a criminal code of Vietnam for the first time. It shows that Vietnam legislators has paid attention to the danger of the creation and circulation of the harmful tools to computer systems and data.

However, the comparison between the two provisions reveals some difference in terms of criminal conducts and objects. In terms of criminal conducts, although the activities of "production, sale, procurement for use, import, distribution" of the Article 6 of the CoC can be equivalent to the actions of manufacture, trade, exchange and giving out" in the Article 285 of CCV 2015. The conduct of 'making available of" or publishing the tools online is not included in the Article 285 of the CCV 2015. Also, Paragraph 1(b) of Article 6 creates the offence of possessing the harmful items but the mere possession of them is not a crime in the CCV 2015. Additionally, in terms of criminal object, while the Article 6 of the CoC includes all potential objects of this type of crime including 'a computer program', 'computer password', 'access code' or 'similar data', Article 285 of the CCV 2015 does not consider computer passwords, access codes as the objects of misusing device. Obviously, this loophole may result in the difficulties in prosecuting a person who trading in passwords or access codes that is used to commit cybercrime. From these analyses, it can be concluded that misuse of device has not been criminalized adequately by the CCV 2015.

C. Computer-related offences

Title 2 of the CoC includes types of "computer-related offences" where computers are tools to commit 'ordinary crimes' [25]. Under this title, two types of offences required by the Convention are "Computer-related forgery" (Article 7) and "Computer-related fraud" (Article 8).

1) Computer-related forgery

Article 7 requires each party to criminalize the activities of 'inputting, altering, deleting, and suppressing computer data' to create 'inauthentic data' so that it is 'considered or acted upon for legal purposes as if it were authentic". This provision is developed to construct a similar crime in cyberspace to the conventional forgery of documents which has been criminalized by many jurisdictions [25]. Although this untraditional type of forgery may not bring about tangible documents, it causes remarkable harm to the victims of the deception. The nature of the 'forgery' is identified based on 'the issuer of the data' rather than its the exactness [25].

In the CCV 2015, there are not any specific provisions on computer-related forgery. The fabrication of data is mentioned in the Article 289 of the CCV 2015 as follows**:**

> 'Any person who deliberately bypasses the warning, hacks the password or firewall, or uses the administrator's right of another person to infiltrate another person's computer network, telecommunications network, or electronic device in order to take control, interfere the operation of the electronic device; steal, change, destroy, fabricate data or illegally use services shall be liable to a fine of from VND 50,000,000 (US$2,500) to VND 300,000,000 (US$15,000) or face a penalty of 01 - 05 years' imprisonment'

But this article mainly criminalizes the activity of illegal access. Data fabrication is a part or a purpose of the crime of illegal access instead of an independent crime. As a result, the

© 2015-19, IJARCS All Rights Reserved

mere creation of inauthentic data without illegal access is not a crime covered by this Article. Only one type of data forgery mentioned in CCV 2015 is making counterfeit credit card that is criminalized by Article 290. According to this Article, any persons who make, store, trade, use and circular fake bank cards with the intent to appropriate money of the account holders or use them to pay for goods and services without right are considered as criminals. However, information related to bank account is only one type of computer data. It cannot replace all types of computer data covered by Article 7 of the CoC. Therefore, it can be concluded that the creation of inauthentic computer data has not been criminalized adequately by the CCV 2015.

2) Computer-related fraud

Article 8 of the CoC requires each party to criminalize the activities that cause a loss to victims' property by 'inputting, altering, deleting, suppressing the computer data, or interfering the functioning of the computer system'. These wrongdoings must be conducted without right and with intent to gain an economic benefit for perpetrators themselves or for another person. Compared to the Article 7, the list of conducts regulated by Article 8 is supplemented with the content "any interference with the functioning of a computer system". This supplement broadens the scope of activities to all potential activities to defraud victims including those had not appeared or could not be described exactly at the time the Convention was passed. "Loss of property" is explained as 'loss of money, tangibles and intangibles with an economic value' [25].

Computer-related fraud is not stipulated in a united provision in the CCV 2015. Literally, the conducts mentioned in the Article 8 of the Convention are regulated by Articles 286, 287, 289 and 290 of the CCV 2015. These articles embrace the conducts of interfering computer networks, telecommunications networks and electronic device to acquire economic benefits. For instances, in Articles 286 and 287, the actions of spreading harmful software or obstructing and disturbing 'a computer network, telecommunications network, or an electronic device' is a crime once offenders gain illegally profit worth 50 million VND or more. In Article 289, gaining economic benefit is not a compulsory part of the crime but it is the factor to identity a harsher punishment to an offender. For example, an offender who illegally access the computer network, telecommunications network, or electronic device shall be fined 50 to 300 million VND (US$2,5000-15,000) or sentenced to one to five years' in prison. However, if he gains an illegal benefit worth 200 million VND to 500 million VND (US$10,000-25,000), he will be fined 300 million VND to one billion VND (US$15,000-100,000) or sentenced to from three to seven years' imprisonment.

Especially, the Article 290 of CCV 2015 focus on some popular conducts to appropriate victims' property. The list of criminalized activities consists of:

a)Using information about another organization's or individual's bank account or card;

b)Making, storing, trading, using fake bank cards to steal money of card holders or illegally pay for the offenders' purchases;

c)Illegally accessing the account of an organization or individual in order to appropriate their property;

d)Commit frauds in electronic commerce, electronic payment, online currency trading, online capital raising, online multi-level marketing, or online securities trading for the purpose of property appropriation;

e)Illegally establishing or providing telecommunications or Internet services for the purpose of property appropriation

The listing of conducts in the Article 290 is believed to facilitate Vietnam law enforcement agencies in identifying, verifying and prosecuting the conducts that have emerged in Vietnam in recent years. However, the such method of listing cannot cover all possible methods to appropriate property that have not been discovered by law enforcement agencies. The application of this method in the CCV 1999 resulted in the failure in prosecuting some new types of fraud. The conducts in the Article 8 of the CoC is described in a larger scope than the list of activities in the Article 290 of the CCV 2015.

Additionally, while generic computer data is the criminal objects of criminal conducts in Article 8 of the CoC, Article 290 of the CCV 2015 mainly focus on the bank account and card information. Although the bank account and card information are the vulnerable targets of cybercrimes, it cannot be denied that other types of computer data can be abused by fraudsters such as email accounts or social network account. In other words, bank account and card information cannot replace all types of computer data. Obviously, the criminal objects of Article 8 of the Convention are more accurate than that of the Article 290. The difference in terms of conducts and criminal objects show the difference between the Article 290 of the CCV 2015 and Article 8 of the Convention.

However, the criminal justice system of Vietnam still can apply Article 286, 287 or 289 to fill this gap. Therefore, it still can be concluded that computer-related fraud is criminalized sufficiently by the CCV 2015 even though it is not stipulated in a united provision in the CCV 2015 but different provisions,

D. Content-related offences

Content-related offences are covered by Article 9 of Title 3 of the CoC that emphasize the need for criminalization of offences related to child pornography which is a threat to the development of children. The harmful conducts mentioned in Article 9 consists of **'**producing, offering, making available, distributing, transmitting, procuring, and possessing child pornography'. The Article aims to enhance protection for children against sexual exploitation by criminalizing the use of computers to commit sexual offences against children. 'Child pornography' refers to pornographic materials that visually contain 'a minor' or 'a person appearing to be a minor' 'engaged in sexually explicit conduct' (Article 9). Although a 'minor' is a person under 18 years old, the Convention allow parties adopt a lower age-limit, but it is not less than 16 years old [25].

In Vietnam, neither CCV 2015 nor CCV 1999 have any particular articles on child pornography. Before the starting date of CCV 2015 (January 1st, 2018), all the conducts related to pornography were prosecuted in accordance with the Article 253 of the CCV 1999 (amended and supplemented in 2009) "Disseminating debauched cultural products" that set punishment for 'those who make, duplicate, circulate, transport, sell or purchase, stockpile decadent books, newspapers, pictures, photographs, films, music or other objects for the purpose of dissemination thereof, or commit other acts of disseminating debauched cultural'. Although the paragraph C of section 2 of Article 253 stipulates a higher punishment for the dissemination of pornography to juveniles, children are only in the role of audience instead of a part of pornography products as described in Article 9 of the

© 2015-19, IJARCS All Rights Reserved

Convention. Additionally, with the usage of the general term "debauched cultural products", the article does not differentiate between child pornography and adult pornography. Consequently, the seriousness of the dissemination of child pornography as well as the importance of child protection did not receive attention from Vietnamese society as well as law enforcement agencies. End Child Prostitution in Asian Tourism [27] commented that the lack of child pornography definition or prohibition in Vietnam make children in Vietnam face the risk of commercial sexual exploitation. During the last review on implementation of the *Optional Protocol on the sale of children, child prostitution and child pornography* in Vietnam, the Committee on the Rights of the Child of the United Nations called for a specific provision of child pornography with appropriate punishment for production, dissemination, offering and possession of child pornography. However, this requirement is not satisfied by the CCV 2015.

Like the CCV 1999 (amended and supplemented in 2009), the CCV 2015 does not put child pornography and adult pornography in separated provisions. All offenses related to pornography are handled basing on the Article 326 "Distributing pornographic materials" of the CCV 2015. Paragraph 1 of Article 326 reads

> "Any person who makes, duplicates, publishes, transports, deals in, or stores books, magazines, pictures, films, music, or other items that contain pornographic contents for the purpose of distributing them or distributes pornographic materials in any of the following cases shall be a fine of from VND 10,000,000 (US$500) to VND 100,000,000 (US$5,000) or face a penalty of up to three years' community sentence or between six and 36 months' imprisonment:
> a) The offence involves an amount of digital data from 01 GB to under 05 GB in size;
> b) The offence involves 50 - 100 physical books or magazines;
> c) The offence involves 100 - 200 physical pictures;
> d) Pornographic materials are distributed among 10 - 20 people;
> dd) The offender incurred an administrative penalty or has a previous conviction for the same offence which has not been expunged".

Although both Article 9 of the CoC and Article 326 of the CCV 2015 criminalized the offenses related to pornography materials, there are some differences between them. Firstly, the main purpose of Article 9 of the CoC is to protect children from the risk of being sexually abused while that of the Article 326 of CCV 2015 is to maintain Vietnam social order. The criminal object of the Article 326 of the CCV 2105 is the pornography materials in general that is believed to be harmful for the social order in Vietnam. That is also reason why this article is laid in section 4 "Offense against public order" of the Chapter XXI "Offences against Public Order and Public Safety" instead of Section 2 "Offense in the field of information Technology and Telecommunications Network" like other types of cybercrime. Obviously, the criminal justice system of Vietnam may still use Article 326 of the CCV 2015 to prosecute the distribution of child pornography, but the importance of protecting children is significantly underestimated.

Another noticeable loophole in the Article 326 of the CCV 2015 is that it does not criminalize mere possession, accessing or viewing child pornography online. The main conduct criminalized in this article is distributing pornography materials. All other actions such as making, duplicating, publishing, transporting, dealing in and storing *only can* be prosecuted if they are conducted with the purpose the purpose of distributing pornography material. This gap results in the difficulties in prosecuting people who merely possess child pornography in Vietnam although the criminalization of this harmful conduct is required by the Convention. From above analysis, it can be concluded that child pornography is not criminalized adequately by the CCV 2015.

E. Copyright infringement

The final category of cyber offences mentioned in Title 4 of the Convention is copyright infringement. Although this is traditionally a civil matter, the requirement for criminalization of this activity is made based on the fact that copyright infringements have been spreading rapidly all around the world [25]. The Article 10 of the CoC was built with the hope that copyright infringement may be prosecuted according to criminal laws, especially in the case of large scale or commercial infringement. Article 10 of the Convention requires parties to criminalize the infringement upon copyright 'on a commercial scale' via computers. However, these requirements are defined by reference to the commitments that member state has taken on under international laws such as the Berne Convention, the TRIPS agreement and the WIPO Copyright and Performances and Phonograms Treaties.

The infringement of copyright and relevant rights is criminalized by Article 225 in the Chapter XVIII "*Economic Offences*" of CCV 2015. Article 225 stipulates that:

> 'A person who, without the consent of the holders of copyrights and relevant rights, deliberately commits any of the following acts which infringe upon copyrights and relevant rights protected in Vietnam and earns an illegal profit of from VND 50,000,000 (US$2,500) to under VND 300,000,000 (US$15,000) or causes a loss of from VND 100,000,000 (US$5,000) to under VND 500,000,000 (US$25,000) to the holders of such copyrights and relevant rights, or with the violating goods assessed at from VND 100,000,000 (US$5,000) to under VND 500,000,000 (US$25,000) shall be liable to a fine of from VND 50,000,000 (US$2,500) to VND 300,000,000 (US$15,000) or face a penalty of up to three years' community sentence:
> a) Making copies of works, video recordings, audio recordings;
> b) Making the copies of works, video recordings, audio recordings publicly available.'

In the CCV 1999, the crime of copyright infringement was stipulated in Article 131 "Infringement upon copyright" in Chapter XIII 'Crimes of Infringing Upon Citizen's Democratic Freedoms'. However, this important provision was removed from CCV 1999 when it was amended and supplemented in 2009. This change resulted in difficulties in dealing with all criminal cases related to copyrights in Vietnam because all violations related to copyright could only be fined or administratively sanctioned instead of attracting prosecution. According to the report of Vietnam Ministry of Science and Technology and Ministry of Public Security, there were very few cases related to infringement of copyright prosecuted since the enforcement of the CCV 1999. The criminalization of copyright infringement is a significant improvement in the CCV 2015 to confront the widespread of copyright infringement in Vietnam. This is also in line with many international agreements signed by Vietnam including the Paris Act 1971 revising the Bern Convention for the Protection

© 2015-19, IJARCS All Rights Reserved

of Literary and Artistic Works**,** the Agreement on Trade-Related Aspects of Intellectual Property Rights and the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention). However, Vietnam has not been a member of the World Intellectual Property Organization (WIPO) Copyright Treaty and the WIPO Performances and Phonograms Treaty.

Vietnam law makers do not only criminalize copyright infringement as the requirement of the CoC but also identity the detailed consequences of the infringement such as a loss of 100 million VND (US$5,000). This supplement aims to facilitate Vietnam law enforcement agencies in identifying exactly whether a violation is a crime or not. With all above analysis, it can be concluded that copyright infringement is criminalized adequately by the CCV 2015.

F. Corporate liability

Article 12 and Article 13 of the CoC require its party to make sure that legal persons can be sanctioned if they commit crimes stipulated in the CoC. In CCV 2015, corporate liability is stipulated at Article 76 "Scope of criminal responsibility of a corporate legal entity" that include a list of criminal offences that corporate legal entities have to take criminal responsibility such as 'smuggling', 'Illegal trafficking of goods or money across the border', and 'manufacture or trading of banned commodities'. However, among all these offences related cybercrime mentioned by the Convention, legal persons are only liable for copyright infringement (Article 225) and they do not have to bear criminal responsibility for offences in Articles 285 through 294**.**

G. Criminal conducts mentioned in the Additional protocol

The Additional Protocol of the CoC focus exclusively on 'acts of a racist and xenophobic nature committed through computer systems.' The Protocol aims at enhancing protection for human rights by deterring the activities of disseminating racist and xenophobic materials via computer systems [25]. 'Racist and xenophobic material' is explained by Article 2 of the Protocol as follows

> 'any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, color, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.'

The offences mentioned in the Protocol can be divided into two group: Group (I) including offences related to racist and xenophobic material such as disseminating (Article 3), threatening (Article 4) and insulting publicly (Article 5); Group (II) includes the activities of 'distributing or making available through a computer system material which denies, grossly minimizes, approves or justifies acts constituting genocide or crimes against humanity' (Article 6).

Offenses of the Group (I) is criminalized in the CCV 2015 with two following articles: Article 116 'Sabotaging implementation of solidarity policies' and Article 422 'Crimes against humanity'. Article 116 stipulates the activities of sowing divisions between the classes of people; causing discrimination among the ethnic communities of Vietnam; and cause separation 'between religion followers and non-followers, between religions, between religion followers and the government or socio-political organizations.' In Vietnam, discrimination between white people and people of color has not been widely known so far. However, there are 54 ethnics living in Vietnam with different languages and culture. There are also many religions in Vietnam such as Buddhism, Catholicism and Caodaism. Vietnam government always state its policy to foster the solidarity among ethnicities and religion followers. The Article 116 aims at dealing with any actions to initiate the discrimination against any minorities or religion followers. Although the activities related to racist and xenophobic material via computer systems contained in Articles 3 through 5 of the Protocol is not focused by this Article, any types of offences causing discrimination against any minorities or religion followers can be covered by it.

Group II of the Protocol include only Article 6 that pays attention to the dissemination or making available of materials which denies, grossly minimizes, approves or justifies acts constituting genocide or crimes against humanity. The article originates from the facts that many subjects expressed ideas or theories to deny, approve of justify the genocide during the second World War II that was condemned by international community (*Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, 2003). These activities have not been known in Vietnam so far. Additionally, the Protocol also allows its party not to apply this article wholly or partly. Thus, criminalization of such activities in CCV is unnecessary under current context.

V. DISCUSSIONS AND CONCLUSIONS

From above analysis that, it can be concluded that there is disparity between CCV 2015 and the CoC in defining and using key terms related to cybercrime such as 'computer system' or 'computer network'. Also, legal persons are not held liable to majority of cybercrime in CCV 2015 although this is a requirement of the CoC. Additionally, although CCV 2015 has sufficiently criminalized many criminal acts stated in the CoC and its Additional Protocol including illegal access, illegal interception, system interference, computer-related fraud, copyright infringement and dissemination of racism materials, it has failed to criminalize properly other criminal acts including data interference, computer – related forgery, misuse of device, child pornography and corporate liability. This section will mainly present and discuss the findings, which will assist us in understanding the difference between CCV 2015 and the CoC. The discussions may also contribute to formulate a set of necessary and appropriate policy recommendations for Vietnam legislation.

The recent amendments and supplement of many articles in CCV 2015, along with including several other acts of cybercrime as recognized by international community, manifests the firm determination of Vietnamese government to improve their legal framework against fighting cybercrime. However, the process of amending and supplementing CCV was complex and conducted sluggishly. The progress of building CCV 2015 was directed by the Drafting Committee established by Standing Committee of National Assembly before submitting to the National Assembly. The Committee

© 2015-19, IJARCS All Rights Reserved

included members from leaders of 16 ministries and equivalent bodies, leaders of Supreme Court, Supreme Procuracy, Central Comittee of Vietnam Fatherland Front, Vietnam Lawyer Association and Vietnam Union of Lawyers. Drafting Committee is led by Minister of Justice. Criminal Code 2015 was drafted by many bodies in the Government such as Ministry of Public Security, Ministry of Defense, Ministry of Justice, Supreme Court and Supreme Procuracy. Each body is in charge of one or a few chapters of the Code. In terms of time, it took almost ten years to amend cybercrime related articles, despite which the amended articles have failed to appropriately deal with cybercrime in the beginning years of current 21st century. It also took another eight years to modify these provisions which came into force in 2018. Whereas, technology and cybercrime have been developing at an astonishing speed, Vietnam's legislative assembly has been too sluggish in implementing changes to prevent cybercrime.

The disparities between the Convention and CCV 2015 as presented in the findings part is an illustration for the dissimilar perspectives about the definition of cybercrime and its classification between Vietnamese law makers and their counterparts in the European Union. Some specific types of crime are considered as crimes using high technology by Vietnam criminal justice system but not mentioned in the Convention on Cybercrime. For instances, in the section on '*Offense against Regulations on information Technology and Telecommunications Network'* that include most types of crime using high technology, some types are not included the Convention such as "online currency trading, online capital raising, online multi-level marketing, or online securities trading for the purpose of property appropriation". Besides, recent report on cybercrime of Ministry of Public Security [19], the main actor in preventing and suppressing crimes using high technology in Vietnam, even include other types of hi-tech criminal conducts, which the Convention does not require its party to criminalize such as online gambling, using Facebook to dishonor state leaders. The criminalization of these types of cybercrime are a distinct feature of Vietnam criminal code. Obviously, there is a disparity in the understanding of the scope of the criminal conducts identified as cybercrime between the Convention and Vietnam lawyers and criminologists.

In terms of classification, the types of cybercrime that are included in the Convention are not clustered together in one part of CCV 2015 rather spread around in different sections. Vietnam law makers classify crimes in criminal codes based on criminal objects such as national security, public order or public safety where technical aspect of cybercrime is not a prioritized criterion in such classification. Therefore, many types of cybercrime are gathered in Section 2 "Offense against Regulations on information Technology and Telecommunications Network" in the Chapter XXI "Offences against Public Order and Public Safety" only because their criminal objects are regulations on information technology and telecommunications network. Meanwhile, other types such as pornography and copyright infringement are covered in other sections because of the perspective that they cause damages to other criminal objects like public order or economic law. This method of classification separates child pornography and copyright infringement from other cybercrimes although all these conducts are more or less related to computers and defined as cybercrime by the Convention. The difference in classification may result in the difficulties on conducting researches on cybercrime as well as participation in international framework on anti-cybercrime. It also leads to the distraction in efforts to deal with cybercrime of Vietnam law enforcement agencies.

The dissimilarities between the CCV 2015 and the CoC can be explained by the difference in their politics, economics, society, culture, and especially the law system. It is obvious that Vietnam and European countries are developmentally different. Law systems or legal tradition in Vietnam also differs from many European countries. While Vietnam legal system is a socialist law system where decisions of courts only rely on written laws rather than precedence or court judgement, many countries in Europe use common laws in which court may convict based on precedence. Moreover, CCV 2015 is created to deal with crime within the jurisdiction of Vietnam territory. It is influenced by dominant ideology in Vietnam society as well as the situation of crime in general, thus has its own principles as well as distinctive features. For instances, some types of crime in Vietnam might not be a crime in other countries such as dissemination adult pornography, prostitution, and gambling. For these reasons, the difference in all laws built by two sides is unavoidable especially when Vietnam has not participated in the Convention and it is not to be obligated to fulfil its requirements. Besides, there have not been any international conference on legal framework against cybercrime organized in Vietnam up to now and thus, Vietnam legislators have not had opportunities to exchange their views with counterparts all around the world.

Notwithstanding, it is noticed that Vietnam legislature body underestimates some serious crimes that have been condemned in global scope although they have been emerging threats in Vietnam in recent years. These crimes are child pornography and copyright infringement. It is evident that child pornography has a close correlation with child sexual abuse. In Vietnam, there were 6,686 cases of child abuse, with 8,146 child victims over the past five years (2012 - 2016) [28, 29]. Leader of Vietnam police force states that crimes against children, especially child sexual abuse, are on the rise with diverse modus operandi [30]. Notably, a number of cases of child sexual abuse have caused extremely serious consequences for the young victims that may last for their whole life. The mixture of adult pornography and child pornography in a provision of CCV 2015 (Article 326) may result in the underestimation for the seriousness of child pornography and the lack of protection for children before child abusers. Moreover, along with technological advancements and increased use of smartphones in present era, the average age of smartphone users has decrease in Vietnam in recent years. It is lot easier for youngsters to watch immoral products on the internet and acquire degenerate thoughts from them and then turn into crime in practice. Also, youngsters *per se* or persons under the age of 16 unknowingly or unintentionally may facilitate child pornography that might be related to them or not. Neither the CoC nor CCV 2015 have any provisions to address this problem. This loophole reminds us that fact that Vietnamese law is struggling to keep pace with dynamic socio-technological change.

Together with this, copyright infringement in Vietnam has become a major concern of Vietnam government and international organization as Vietnam is one of the countries with highest copyright infringement rates in the world [19]. Copyright infringement is spreading in many fields such as

© 2015-19, IJARCS All Rights Reserved

piracy of computer software or illegal downloading music, films, book from the Internet. In the last few years, Vietnamese Government has made a great effort to enforce copyright protection such as conducting inspection against use of illegal computer software in a large number of enterprises and conducting propaganda for copyright protection, but hitherto have not been as successful in preventing the crimes related to copyright infringement.

VI. RECOMMENDATIONS

The central objectives of this research were (1) to identify whether the criminalization of cybercrime in CCV 2015 would satisfy the requirements of the Convention and (2) to propose recommendations to improve criminal law in the future. The above comparative analysis between CCV 2015 and the CoC has revealed that there are still gaps between the CCV 2015 and the CoC. Although the CCV 2015 has sufficiently criminalized the acts of illegal access, illegal interception, system interference, computer-related fraud, copyright infringement and dissemination of racism materials, other forms of cybercrime as per the Convention have not been criminalized adequately in Vietnam Criminal Code 2015 which includes data interference, computer – related forgery, misuse of device and child pornography. It can be concluded that the two central research questions 'Are cybercrimes objectively stated in the European Convention on Cybercrime also criminalized in the Vietnam Criminal Code?' and 'How are these crimes stated in the Vietnam Criminal Code?' have been answered.

Based on the above analysis, some following recommendations are made to improve Vietnam legal framework on cybercrime in the future. Firstly, it is recommended for Vietnam lawmakers to give clear definitions of computer data, computer system and computer network so that following legal visions are uniformed and applied accordingly. Also, Vietnam law makers need to consider computer data is a criminal object of cybercrime as it has been recognized by the CoC. As then only the provisions related to computer data such as data interference, illegal interception, computer – related forgery can be criminalized properly in the next stage of amendment for the CCV 2015.

Secondly, the author suggests that child pornography should be criminalized by an independent article in Vietnam Criminal law as Article 9 of the CoC require its parties. Such provision will separate child pornography from adult pornography and impose harsher punishment to show the seriousness of this type of crime. This suggestion was also given by the Committee on the Rights of the Child of the United Nations in the past but has not been acted on to date. So, such provision manifests the determination of Vietnam to protect children like its commitment with international community. It also will promote moral values in the society and play an importance role in combating child sexual abuse that has been threatening lives of many Vietnam children in recent years. The Vietnamese legislature should also consider criminalizing the activity of soliciting children for sexual purposes via computer or 'grooming'. Many countries such as the US, the UK and Australia consider this harmful conduct as an offence. Although 'grooming' has not been known widely in Vietnam, it can happen in the future, especially with the development of social media.

Thirdly, the author strongly recommends the Vietnam Government to ratify the European Convention on Cybercrime. It is evident that there are still gaps between Vietnam criminal laws and the international standard set by the CoC. Also, as Vietnam is not a party of the CoC, law enforcement agencies of Vietnam have missed out great opportunities to cooperate closely with their counterparts of a large number of member states of the Convention. The ratification of the CoC will contribute significantly to the development of Vietnam national laws as well as international cooperation. For instances, Vietnam laws may borrow some provisions from the Convention which have not been criminalized sufficiently in the CCV 2015. Additionally, Joining the Convention will ultimately promote information exchange and joint investigation on cybercrime between Vietnam police force and many law enforcement agencies in the world via the channel set by the Convention. Fourthly, it is recommended that Vietnam legislature should consolidate all types of cybercrime within the Code into a separate section or even make a specific law on cybercrime. Such innovations will lead to a more concentrated effort to rigorously define and purse cybercrimes. Since then, more research on cybercrime legislation in Vietnam will be carried out properly in the future.

Finally, further research with overall pictures on legal framework on cybercrime should be supported in the next time. The CCV 2015 has been enforced for a short time and its efficiency in practice need to be evaluated by further research in the future so that it can be amended and supplemented to adapt to rapid changes of cybercrime.

VII. REFERENCE

[1] Clough, J., Cybercrime. Commonwealth Law Bulletin, 2011. **37**(4): p. 671-680.

[2] Broadhurst, R. and L. Chang, Cybercrime in Asia: Trends and Challenges, in Handbook of Asian Criminology, J. Liu, B. Hebenton, and S. Jou, Editors. 2012, Springer: New York. p. 49-63.

[3] Clough, J., A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation. Monash University Law Review, 2013. **40**(3): p. 698-736.

[4] Chang, L., Cybercrime and Cyber Security in ASEAN, in Comparative Criminology in Asia, J. Liu, M. Travers, and L. Chang, Editors. 2017, Springer, Cham. p. 135-148.

[5] United Nations Conference on Trade and Development, Cybercrime Legislation Worldwide, United Nations, Editor. 2018, United Nations Publication: New York.

[6] Yilma, K., Developments in Cybercrime Law and Practice in Ethiopia. Computer Law & Security Review, 2014. **30**(6): p. 720-735.

[7] Sauliunas, D., Legislation on Cybercrime in Lithuania: Development and Legal Gaps in Comparision with the Convention of Cybercrime. Jurisprudence, 2010. **4**(122): p. 203-219.

[8] Moise, A., Modernization of Romanian Legislation on Preventing and Combating Cybercrime and Implementation gap at European level. . Revista de Stiinte Politice, 2015(45): p. 186-199.

[9] Wang, Q., A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe. , in School of Law. 2016, Erasmus University Rotterdam: Rotterdam, the Netherland.

© 2015-19, IJARCS All Rights Reserved

[10] Anuar, A., ASEAN's Digital Economy: Development, Division, Disruption, in Commentary, RSIS, Editor. 2019, S.Rajaratnam School of International Studies (RSIS): Singapore.

[11] Chua, S. and H. Venkataramani ASEAN in the Digital Age: Quo Vadis? Digital, 2018.

[12] Lin, L. and J. Nomikos, Cybercrime in East and Southeast Asia: The Case of Taiwan, in Asia-Pacific Security Challenges: Managing Black Swans and Persistent Threats, A. Masys and L. Lin, Editors. 2018, Springer: New York. p. 65-84.

[13] Candice, D.T., Cybersecurity Governance Framework in Vietnam: State of Play, Progress and Future Prospects. Asian Research Policy, 2017. **8**(1): p. 86-97.

[14] Anh, N.N., Vietnam Law on Cybercrime, in Conference on Theoretical and Technical Problems on Counter-Cybercrime in Vietnam, X.N. Yem, Editor. 2014, The People's Police Academy of Vietnam: Hanoi, Vietnam [Vietnamese language].

[15] National Assembly of Vietnam, Law on Information Technology of Vietnam, in No. 67/2006/QH11, N. Assembly, Editor. 2006, National Assembly of Vietnam: Hanoi, Vietnam.

[16] Duc, M.N., Characteristics of cybercrime and Solutions to Enhance Effectiveness of Cybercrime Prevention and Suppression, in Conference on Theoretical and Technical Problems on Counter-Cybercrime in Vietnam, X.N. Yem, Editor. 2014, The People's Police Academy of Vietnam: Hanoi, Vietnam [Vietnamese language].

[17] Giam, M.B., Discussion on Necessary Traits, Ability and Skills of Anti-Cybercrime Police Officers, in Conference on Theoretical and Technical Problems on Counter-Cybercrime in Vietnam, X.N. Yem, Editor. 2014, The People's Police Academy of Vietnam: Hanoi, Vietnam [Vietnamese language].

[18] Nghia, Q.P. and H.P. Binh, eds. Principles and Provisions to Prevent and Combat High-Tech Crimes. 2014, The People's Police Academy of Vietnam: Hanoi, Vietnam [Vietnamese language].

[19] DCPCHC, Annual Report on Cyber Crime in Vietnam 2018 [Vietnamese language]. 2019, Department on Cybersecurity and Prevention and Combat High-Tech Crime (DCPCHC): Hanoi, Vietnam

[20] Van Hoecke, M., Methodology of comparative legal research. Law and Method, 2015: p. 1-35.

[21] Saleilles, R., The Individualization of Punishment (translated from the second French edition by Rachel Szold Jastrow, London. 1911, William Heineman.

[22] Wilson, G., Comparative legal scholarship. Research methods for law, 2007: p. 87-103.

[23] Sepec, M., Slovenian Criminal Code and Modern Criminal Law Approach to Computer-related Fraud: A Comparative Legal Analysis. International Journal of Cyber Criminology, 2012. **6**(2): p. 984.

[24] Markopoulou, P., The convention on cybercrime. Intellectum, 2008.

[25] European Commission, Convention on Cybercrime. 2001: Budapest, Romani.

[26] Jaishankar, K., Cyber Criminology: Evolving a Novel Discipline with a New Journal. International Journal of Cyber Criminology, 2007. **1**(1): p. 1-6.

[27] ECAPT, Protecting Children from Online Sexual Exploitation: A Guide to Action for Religious Leaders and Communities. 2016, End Children Prostitution and Trafficking (ECPAT): Bangkok, Thailand.

[28] VACR and ECAPT, Sexual Exploitation of Children in Vietnam for the Universal Periodic Review of the Human Rights Situation in Vietnam to the Human Rights Council 32th Session (January-February 2019) UPR Third Cycle 2017 – 2021. 2018, Vietnam Association for Protection of Child's Rights (VACR) and End Children Prostitution and Trafficking (ECPAT): Hanoi, Vietnam.

[29] ECAPT, Regional Overview: Sexual Exploitation of Children in Southeast Asia. 2017, End Children Prostitution and Trafficking (ECAPT): Bangkok, Thailand.

[30] Vietnam Association for Protection of Child's Rights and ECPAT Int, Sexual Exploitation of Children in Vietnam, in the Universal Periodic Review of the Human Right Situation in Viet Nam. 2018.

© 2015-19, IJARCS All Rights Reserved

Copyright of International Journal of Advanced Research in Computer Science is the property of International Journal of Advanced Research in Computer Science and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.