Journal of The Korea Society of Computer and Information
Vol. 21 No. 2, pp. 137-144, February 2016
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2016.21.2.137

Control of International Cyber Crime

Jong-Ryeol Park*, Sang-Ouk Noe**

Abstract

The followings are required to establish uniform principle of criminal jurisdiction for international cyber crime into customary international law; ① clear guideline of UN for promoting national practice ② formation of general practices based on these guidelines ③ these general practices should obtain legal confidence. International society is in close cooperation for investigating and controlling cyber threat. The US FBI has closed down the largest online crime space called 'Darkcode' and prosecuted related hackers based on joint investigation with 19 countries including England, Australia, Canada, Bosnia, Croatia, Israel, and Rumania.

More and more people in Korea are raising their voices for joining cyber crime treaty, 'Budapest Treaty.' Budapest Treaty is the first international treaty prosecuting cyber crime by setting out detailed regulations on internet criminal act. Member countries have installed hotline for cyber crime and they act together. Except European countries, America, Canada, and Japan have joined the treaty. In case of Korea, from few years before, it is reviewing joining with Ministry of Foreign affairs, Ministry of Justice and the National Police but haven't made any conclusion. Different from offline crime, cyber crime is planned in advance and happens regardless of border. Therefore, international cooperation based on position of punishing criminals and international standards. Joining of Budapest international cyber crime treaty shall be done as soon as possible for enhancing national competence.

▸ Keyword : Budapest International Convention of Cyber Crime, criminal jurisdiction for international criminals, cyber crime, customary international law

I. Introduction

With the advance of Smart era, prevailing forecast is that cyber crime and security threat will increase more and more. Even today, various cyber attacks such as malignant code, hacking, Distributed Denial of Service (DDoS), and Advanced Persistent Threat (APT) have become so aggressive that global governments, corporations, and security businesses are grappling with finding solutions.

It is not long since Korea had serious security incidents in financial field one after the other from DDoS attack and hacking which led to leakage of personal information and NH computer network failure, and social anxiety has increased. What is more, smartphone malignant code is increasing rapidly through Android. These security incidents such as malignant code, DDoS, and hacking have become global issues.

The malignant code is spreading quickly through worldwide personal computer, mobile devices, and internet users. DDoS attacks are passing through and abusing different servers in global countries, making it difficult to find its origin. Similar to 'attack from China' which has become an issue few years ago, attacks targeting Korea from other countries is happening frequently.

• First Author: Jong-Ryeol Park, Corresponding Author: Sang-Ouk Noe.
*Jong-Ryeol Park(park3822@kwu.ac.kr), Kwangju Women's University, Professor.
**Sang-Ouk Noe (nosang2424@daum.net), Joongbu University, Professor
• Received: 2016. 01. 11, Revised: 2016. 02. 07, Accepted: 2016. 02. 19.

Although cyber criminal is a Korean and they targeted website of Korean organizations and corporations, those criminals either attack from other countries or hide away from being caught by investigating agency. It was analyzed that 'Stuxnet,' emerged during second half of last year, concurrently affected many different countries, not only Iran but also China and Indonesia.

Recently, hacker groups, 'Anonymous,' 'Antisec.' and 'Lulzsec,' that have become well-known on Korea media are active all over the world regardless of country, government, and corporation. Due to this borderless feature of cyber crime, importance of 'international assistance and cooperation' is increasing gradually in terms of handling cyber threat and crime. Another issue is that what if there is a global cyber crime but place of crime and attacked country differs, which national law has to be applied to the criminal for punishment. This research first explains about concept, characteristics, and international trend, basic factors of cyber crime. Then, it looks into the most difficult point in settling global cyber crime today, problem related to criminal jurisdiction and one of typical cyber crime treaty, Budapest Treaty' and offers ways to deal with these issues.

II. Definition of Cyber Crime

1. Concept

Cyber crime is a general term for defining every criminal act taking place in cyber place, that is "a new communication space created by network of inter-connected computers'[1]. However, there are different opinions on its more specific definition.

Some categorize cyber crime and internet crime separately but under the consideration that internet is the only cyber place that exists, it is actually appropriate to count cyber crime and internet crime as the same concept[2].

Cyber crime is divided into two types. First is criminal act towards internet system. A good example of this crime is infiltration behavior into computer network, that is hacking. Second type is crime by the medium of internet, for instance, distribution of pornography and online gambling. The National Police Agency is classifying the former as cyber terror and the latter as general cyber crime.

2. Difference with General International Crime

International crime before computerization revolution, it referred to criminal act with substantive significance involving human or physical movement across the border. General characteristics of international crime as follows; ① significant physical, psychological, and property damages are caused by criminal act. ② subjects of damages may involve individuals, objects, and psychological value. ③ in terms of crime tools, tangible and intangible weapons are used and may also include violent behavior as well as advanced intelligence. ④ criminals can be individuals, organized crime group, and national organizations. ⑤ criminals usually utilize physical tools such as weapon. ⑥ one may obtain obvious human, physical, circumstantial evidence on criminal act. ⑦ most of the time, place of crime committed and targeted areas are the same. Not much difference in time exists.

On the other hand, characteristics of international cyber crime that appeared along with development of info-communication technologies such as computer and internet as follows; ① criminal act is similar to illegal access to materials and leakage, falsification, elimination, and destruction of materials in cyber space. ② no loss of life but only damage occurs in cyber space. ③ no physical abilities are required but intellectual abilities of computer specialist or ones created through computer are needed for criminal act. ④ criminals are same as other international crime but every criminal has to be computer specialist. ⑤ no physical tools such as weapons are needed for criminals but only knowledge on computer is required. ⑥ as evidence on criminal act only exists in cyber space it is difficult to collect clear human and circumstantial evidence. ⑦ as crime is committed in cyber space, place of crime and targeted area may differ. Also, due to possibility of manipulation, time difference may also exist.

III. Problems of Suppressing International Cyber Crime

1. Principles of Criminal Jurisdiction Related to International Criminals

As I have mentioned earlier, cyber crime happens across the border and thus, original place of crime committed and damaged country may differ. For instance,

if person A having Philippine nationality spread virus in Philippines and this damaged B company in the US, there is a issue that according to which national law shall this A be punished.

The principles of criminal jurisdiction for international criminals are divided into territorial, active personal, passive personal, protectionism, and universalism. This study looks into each of those principles based on above example.

1.1 Territorial Principle

Territorial principle means applying national law to all the crime committed within the territory of a country, regardless of nationality of the criminals. According to territorial principle, as A committed crime in Philippines, jurisdiction of Philippines shall be applied. However, based on omnipresence principle, as crime was committed in America, the country may also have the jurisdiction. If Philippines has no legislation for punishing this crime, it is not considered as a crime in the country and thus, jurisdiction is not granted to Philippines.

1.2 Personal Principle

Active personal principle refers to, regardless of place of crime act, law of criminal's country is applied. According to active personal principle, although A's crime took place in America, as A is a Philippines nationality, only Philippines has the jurisdiction for this crime, not America. In case of Philippines having no legislation established for this crime, it is not considered as a crime and it ay lead to the issue of principle of legality.

1.3 Passive Personal Principle

Definition of passive personal principle is country of victim has the jurisdiction. In accordance to passive personal principle, country of victim B, which is America, has the jurisdiction but Philippines is not. However, passive personal principle is not internationally used and there are no treaties based this principle.

1.4 Protectionism

Protectionism means regardless of country of criminal and crime committed, law of country is applied to any criminal act violating rights of country or its nation. According to protectionism, as B company is based in America, criminal act of A infringing interests of B belongs to federal jurisdiction. However, crimes related to national Rechtsgut regulated under legislation of each country is subjected to protectionism. As this is the case, federal jurisdiction may or may not be granted.

1.5 Universalism

Universalism is a principle of applying country to a certain criminal act (piracy, war, etc) regardless of country of crime, criminal, and victim. Here, certain criminal act within universalism means piracy, war, and crime against humanity that are recognized by international practice. Thus, based on universalism, America has no jurisdiction for cyber crime.

2. Difficulties of Concluding Convention on Criminal Jurisdiction of International Cyber Crime

As I have mentioned before, if an international cyber crime occurs there may arise many issues regarding jurisdiction of the criminal. The most effective way to solve this problem is to establish a unique principle of jurisdiction regarding global cyber crime based on international law. However, still, it is not easy to make this principle by treaties.

As stated above, international cyber crime is one that takes place on cyber space irrespectively to space and time. Under this circumstance, even if an international treaty is concluded on criminal jurisdiction of international cyber crime, there is a higher possibility of treaty itself being a useless thing if all the countries do not participate. In case of international crime based on the movement of an individual and physical object, as they have to cross the border, once principle of criminal jurisdiction is established in treaty, all the participating countries can have an effective internal and external control of the crime based on the uniform principle. In contrast, as international cyber crime is committed in cyber space by the criminal, once crime happens in a country that did not join the treaty the country does not necessarily need to abide by criminal jurisdiction defined by treaty.

That is, cyber crime is a borderless crime and to standardize criminal jurisdiction on this, worldwide law and regulations are required. International treaty based on

national voluntarism cannot guarantee participation of all the countries and thus, in reality, it is extremely difficult to control cyber crime through this.

IV. International Convention of Cyber Crime

1. Details and Features of Budapest Convention

'Budapest Treaty' is also referred to as 'international cyber crime treaty' and is the first international treaty created to deal with cyber crime. It was signed by about 40 different countries during international conference on cyber crime held in Budapest, Hungary, on the 23rd of November, 2001. Since then, it is named as 'Budapest Treaty.' This treaty includes detailed definition for all kinds of cyber crimes happing on the internet and their punishment.

It defines computer system, illegal access to data, infringement of intellectual property, development and dispersion of computer virus, and distribution of child pornography as a criminal act. It obliged joining countries to ban these crime by domestic law. All the treaty signed countries have standardized law and regulation to control cyber crime and established international cooperation system by building up a hotline.

2. Achievement of Budapest Convention [3]

2.1 Reformation of Law and Institution on Cyber Crime

The achievement of Budapest Treaty is that it has made a practical changes such as legislation or revolution of law on cyber crime. Especially, around year 2006, The Council of Europe has launched global project on cyber crime to reinforce internal stability based on Budapest Treaty. As a result, it has recommended legal and institutional revolution on cyber crime to about 120 different countries. Influenced by this, The United Nations general assembly has mentioned Budapest Treaty as a basis for developing law and institution for investigation and prosecution on cyber crime and suggested this to the countries. To conclude, they played a role of pioneer for standardizing Budapest Treaty and managing improvements.

2.2 Formation of Effective Cooperative System for Individual Country

Although Budapest Treaty is an agreement made by The Council of Europe, today, 55 countries in the world have joined it. Considering that 14 European countries haven't joined yet, this treaty has a potential to be developed into a global treaty, instead of a regional treaty in Europe.

Another advantage is that countries can effectively prevent cyber crime by participating in 'Cyber Cooperation Committee' based on this. Furthermore, its achievement, helping countries to obtain and promote overall technologies on international cyber crime is widely recognized.

2.3 Assistance of General Field in Increasing Reaction Ability of Cyber Crime

Legal and institutional revolution as well as establishment of effective cooperation with countries have led to accumulation of legal and institutional techniques on handling cyber crime. Thus, it is considered to give a positive effect in the perspective that they can assist non member countries. That is, having a meeting based on Budapest Treaty is similar to a catalyst accelerating development of technologies for managing cyber crime in each country.

Also, as one can see in Article 15 of Budapest Treaty, it is also functioning as a manual for preventing cyber crime and proper use of computer. Therefore, it not only protects privacy but also personal rights.

2.4 Other Achievements

Budapest Treaty serves as a momentum for increasing efficacy of already-existing treaties in each country (especially, Treaty on Mutual Legal Assistance, Extradition for the Execution of Punishment in Treaty, etc). Judical assistance for investigation, arrest, and prosecution of cyber crime based on Budapest Treaty is after all, possible in the point that it raises efficacy of other similar treaties.

Ⅴ. Control of International Cyber Crime

1. Problems with Criminal Jurisdiction of International Cyber Crime

1.1 Solving through Customary International Law

As explained above, it is difficult for international treaty based on national voluntarism to have a general binding in reality. Thus, it seems more appropriate to solve international cyber crime issues through customary international law than treaties. In terms of forming a customary international law requires no universality but once it is created, it includes general binding. Therefore, it is reasonable to establish uniform principle on criminal jurisdiction of international cyber crime through customary international law.

1.2 Requirements of Customary International Law

International customary law is mostly established on the basis of national customs but not all of them turn into customary law. For practices to become a customary law, they have to be "general practices" involving continuity, uniformity, and generality. Also, the country has to have legal confidence in those practices. Regarding North Sea Continental Shelf case, International Court of Justice (ICJ) has mentioned about requirements for establishment of customary international law.

In this ruling, ICJ has decided that the following conditions have to be satisfied for certain articles of treaty to be established as a customary international law; ① the article should have norm-creating feature ② participation of very wide and representative countries including countries of which interests are specially influenced by this ③ practice of the country is broad and actually consistent ④ these practices are executed under decision that they are legal duties.

What we need to focus here is the importance of "countries of which of their interests are specially influenced." For general practices to turn into customary international law, it has to be sustained for a certain period of time. However, there are no such fixed period of time for forming customs and thus, "broad and actually consistent" and general practices created by "countries having special influence" can become customary law in a short period.

1.3 Provision of Guideline through UN and Establishment of Customary International Law

To establish customary international law on criminal jurisdiction of international cyber crime, there should exist constant national practices. In general, practices mean uniform and continuous act among countries. One of most effective ways to form these practices is to make a worldwide guideline in reflection to opinions of countries that have special interests in international cyber crime, yet no legal binding is valid.

It is considered appropriate to establish these guidelines through worldwide international organization called UN. For details of this guideline, under the circumstance that the damaged country shares the most interests, it is reasonable for affected countries to have criminal jurisdiction in accordance to territorial or passive personal principle.

The aforementioned guideline has possibility of being developed into customary international law for the following reasons; ① uniform principle of criminal jurisdiction for international cyber crime is that it basically has norm-creating feature ② damaged countries from international cyber crime belong to "ones with special interests" and participation of those countries are premised. If these practices are formed to ① be executed widely, practically, and uniformly and ②be done under legal confidence of participating countries, then the guideline will be established as customary international law.

2. Problems of Convention on International Cyber Crime

To effectively manage cyber war committed by group of people against building of nuclear generation station Korea needs to have strengthened international cooperation for cyber security with other countries including the US and China. At the same time, it should reinforce manpower and organizations for controlling cyber terror in Korea.

Starting from December last year, this group has been sustaining its cyber psychological warfare by making public of data one after the other, starting from one belonging to Korea Hydro & Nuclear Power, the Blue House, National Intelligence Service, and Ministry of National Defence. Korean government is not taking any actions other than positioning a security professional as special presidential security advisor. A 'special

presidential advisor' is a 'non-permanent' presidential assistance position with no any other operational manpower. Even National Intelligence Service, in charge of cyber terror is also suffering from political offence of suspected hacking.

While the Blue House and national security organizations not being able to control cyber warfare properly, this group of people have been frequently challenging cyber psychological warfare through global internet service, where Korean jurisdiction cannot be reached. What Joint Investigation Squad do is to block any websites loaded with this data including Twitter, in cooperation with FBI. Even this becomes difficult without acceptance from Twitter headquarter.

Expanding budget and strengthening of organization related to cyber security is an urgent matter. Last year, the US President Obama has announced establishment of 'E-Gov Cyber,' a general responsible department for cyber threat after hacking incident in Sony Pictures Entertainment Inc. 'E-Gov Cyber' set up under Office of Management and Budget (OBM) it not only lay down cyber regulations but also inspects and adjusts cyber strategies of different federal organizations. The President Obama has submitted budget plan of 'E-Gov Cyber' for year 2016 in the amount of 130 million US Dollar (about 120 billion Korean Won) to the Congress.

Last year, Israel has established a new competent department for national cyber security, so called 'national cyber protection organization.' National cyber protection organization is a main center for promoting mid to long-term cyber security policies. Along with national cyber bureau which governed policies for cyber security in national defence and public sectors and security bureau, it controls all the private sectors. It has assimilated role jobs of previous security competent department to strengthen cyber protection system in cooperation with other organizations and corporations. It is an organization which deals with crime, war, and terror in cyber space. International society is closely working together to investigate and control cyber threat. America FBI executed cooperative investigation with 19 different countries to shutdown world's largest online crime space 'Darkcode' and prosecuted related hackers. Among 19 countries. England, Australia, Canada, Bosnia, Croatia, Israel, and Rumania are included.

During SecuInside held in July, national security specialist of the Blue House, Jongin Lim, emphasized that "Korea is suffering from difficulties in investigating outflow of floor plan for nuclear generating plant of Korea Hydro & Nuclear Power due to insufficient international cooperation" and "to deal with borderless cyber crime, it shall have a global approach and prepare for international cooperation." [4]

Looking at the international cooperation system regarding international cyber crime, although there are treaties concluded and came into effect in the world such as cyber crime treaty of The Council of Europe (Budapest Treaty) and United Nations Convention against Transnational Organized Crime, Korea is not preparing to join not even one treaty.

The most important reason for Korea not to join international treaty is because according to Budapest Treaty, what needs to be done in prior to joining is that there should be a law in Korea subject to criminals and regulation of adjective law shall be done in a proper way.

These problems in substantial and adjective law involves professional issues that might go against national law system or legal emotion. Thus, for them to be accepted, sympathy of nation has to be developed [5].

At this point, political community should discuss, point out problems, and find what goes against national law in cooperation with academic community to revise law or legislate new law. However, no efforts are made, not even that of the government.

Also, there are strong opinions from academic community suggesting that Korea should actively review joining of the treaty but the government tried none but holding Seoul Cyber Space General Assembly on October 17th, 2013.

Regardless of any types of international cooperation system including Budapest Treaty which have been growing strong in participation of major countries, if effective for controlling and removing cyber crime, Korea should also consider in more details and immediately.

Ⅵ. Conclusions

It is truth that information revolution through computer and internet made a large contribution to human progress, no one can actually deny this fact. As movement of information across the border has become possible, human, material, cultural, and diplomatic exchanges are taking place actively across the border and it has

solidified frame of international cooperation under a new paradigm called globalization.

However, similar to borderless information exchange and interaction, it also has become easy for cyber crime to jump across the control of border. Different from developed countries, the largest beneficiary of information revolution, legal system of developing countries having relatively less benefit is falling behind the technical development. Thus, they are laid in a situation where they can hardly deal with a new crime called international cyber crime.

As a result, cyber crime causing astronomical financial damage has happened across the globe but humanity failed to have effective control every time. Yet, our humanity is experiencing innovative development and progress of information and technology and scale of international crime abusing this will increase day by day. International society is still behind the preparation of uniform standard on criminal jurisdiction, the key factor in controlling this cyber crime.

There is no uniform principle on criminal jurisdiction regarding international cyber crime and this will preclude effective control of the crime. What is more, it will lead to an argument among countries if any crime happens. Therefore, solution to this is urgently required. Under the consideration that cyber crime takes place regardless of time and space, uniform principle on criminal jurisdiction must cover worldwide. It is determined that solution through customary international law based on universalism is more effective than that of treaty based on national voluntarism.

The followings are required to establish uniform principle of criminal jurisdiction for international cyber crime into customary international law; ① clear guideline of UN for promoting national practice ② formation of general practices based on these guidelines ③ these general practices should obtain legal confidence.

International society is in close cooperation for investigating and controlling cyber threat. The US FBI has closed down the largest online crime space called 'Darkcode' and prosecuted related hackers based on joint investigation with 19 countries including England, Australia, Canada, Bosnia, Croatia, Israel, and Rumania.

More and more people in Korea are raising their voices for joining cyber crime treaty, 'Budapest Treaty.' Budapest Treaty is the first international treaty prosecuting cyber crime by setting out detailed regulations on internet criminal act.

Member countries have installed hotline for cyber crime and they act together. Except European countries, America, Canada, and Japan have joined the treaty. In case of Korea, from few years before, it is reviewing joining with Ministry of Foreign affairs, Ministry of Justice and the National Police but haven't made any conclusion.

Different from offline crime, cyber crime is planned in advance and happens regardless of border. Therefore, international cooperation based on position of punishing criminals and international standards. Joining of Budapest international cyber crime treaty shall be done as soon as possible for enhancing national competence.

REFERENCES

[1] Gyuseok Moon, "Research on cyber crime on international law" 『The Korean Journal of International Law』, Vol. 89, 2001, pp.81

[2] Younghwan Kim, "Theological implication of establishing national control system on cyber crime" 『Korea Computer Information Conference Journal』, Vol.14, 2009, pp.165-171.

[3] Jaejoon Jeong, "Counterplan for international cyber crime" 『New trend in criminal code』, Vol. 39 2013,6 pp.125-127.

[4] "Helpless cyber crime, international cooperation is urgent for controlling cyber war" electronic newspaper paper 3 column 2 2015.8.4.

[5] Jeongil Jang, "International counterplan for cyber crime" 『Guard security research』, Vol. 10, 2005, pp.350.

[6] Taegye Kim, "Institutional problem and solution regarding counterplan for cyber terror crime" 『Law and political research』, Vol. 14 No. 3, 2014, pp.1373.

Authors

Jong-Ryeol Park received the Ph.D. degress in Laws and Civil Law from Chosun University, Korea, in 2001, 2006 respectively.

Dr. Park joined National Communication Ombudsman District Prosecutors' Office in Gwangju in 2009 and was a member of Metropolitan Police Agency Administrative Disposition of a Driver's Licence Review Committee in Gwangju in 2010. Also he was Policy Advisers in Gwangju.Jeonnam Regional Military Manpower Administration. He is currently a professor in the Dept. of Police & Law at Kwangju Women's University. He is interested in Civil Special Act and Registration of Real Estate Act.

Sang-Ouk Noe received the Ph.D. degress in Police Studies from Wonkwang University, Korea, in 2015.

Voluntarily resigned from human resources department of Posco Gwangyang steel mill in 2008 and worked as professor for industry-academy cooperation in Gangneung Wonju National University and Cheonnam National University, trying to promote employment and field practices. Since 2015, I have been working as an assistant professor in Police Law Department of Joongbu University.

Furthermore, I was designated as a professional member of Korea Industry Commercialization Association in 2014.