Cybercrime in the Republic of Korea II:
Criminal Justice and International Cooperation for Cybercrime Prevention

Cybercrime Research Unit
Korean Institute of Criminology
FOREWORD

Over the past few decades, cybercrime has rapidly evolved from being an annoyance to a grave threat to individuals, businesses, countries and the international community that may overwhelm the benefits created by information technology. The importance of keeping track of the latest trends in cybercrime and continued research on global cybersecurity issues, therefore, cannot be overemphasized.

Shortly before Christmas in 2013, Target, one of the largest American retailing companies, fell victim to a massive security breach which resulted in over 70 million credit and debit accounts compromised nationwide. Only one month later, it was the Republic of Korea’s turn to experience a similar nightmare, as nearly half of the entire country’s population including high-profile figures had their credit card data stolen in yet another massive data breach. The full impact of these types of attacks cannot be identified immediately and is yet to be seen.

In this regard, the Korean Institute of Criminology (KIC), a member of the United Nations Crime Prevention and Criminal Justice Programme Network Institutes (UNPNI), has played a leading role in promoting the study of cybercrime, contributing to international endeavors in cybercrime prevention, as well as educating the general public.

In June 2013, the KIC hosted the First Regional Conference of the World Crime Forum, in a joint effort with the International Society for Criminology (ISC), under the theme of “Information Society and Cybercrime: Challenges for Criminology and Criminal Justice.” Twelve leading cybercrime experts in the Asia-Pacific region spoke at this conference, sharing their knowledge and views on some of the latest
and most relevant issues in cybercrime, such as cloud computing, cyber victimization and digital forensics.

The Virtual Forum against Cybercrime (VFAC), developed by the KIC under the auspices of the United Nations Office on Drugs and Crime (UNODC), aims to provide online training on cybercrime investigation techniques to law enforcement officers in Asian and African developing countries, while at the same time acting as a clearinghouse of latest news, trends, academic resources, legislations, experts, conferences and seminar information on cybercrime.

The Cybercrime Research Unit (CRU), established under the Economic and Commercial Crime Research Division, continues to dedicate its research efforts to cybercrime in close cooperation with government agencies and academic institutes worldwide. As part of these efforts, the CRU issued “Cybercrime in the Republic of Korea (I): Criminal Laws on Cybercrime” in 2012, as the first volume of a research report series on cybercrime. While the first volume dealt with Korean laws and practices in cybercrime control, this second volume has focused on cybercrime prevention efforts by the KIC, the Korean government and the international community at large.

It is hoped that scholars, practitioners, experts and students interested in the global efforts in the fight against cybercrime will find this volume both informative and helpful.

Sang Ok Park
President
Korean Institute of Criminology
# TABLE OF CONTENTS

**FOREWORD** ......................................................................................................................................................... i

**DEVELOPMENT AND ACHIEVEMENTS OF CYBERCRIME PREVENTION PROGRAMS OF THE KOREAN INSTITUTE OF CRIMINOLOGY: INTRODUCTION TO THE VIRTUAL FORUM AGAINST CYBERCRIME**

*(LEE, YOUNMI & LEE, SEUNGJIN)* ......................................................................................................................... 1

1. Introduction ......................................................................................................................................................... 1

2. Cybercrime Prevention Programs Developed by the Korean Institute of Criminology .......................... 4
   A. Research Projects and Programs on Cybercrime Prevention ................................................................. 4
   B. The Virtual Forum against Cybercrime .................................................................................................. 4

3. Achievements of the Virtual Forum against Cybercrime ........................................................................... 8
   A. Development and Launch of the Online Training Program ................................................................. 8
   B. Development and Launch of the Research Network ........................................................................... 16
   C. Management of the VFAC Website .................................................................................................... 19

4. Future Goals of KIC Cybercrime Prevention Programs ........................................................................... 22

5. Conclusion ......................................................................................................................................................... 23

**THE CURRENT STATE OF RESPONSE TO CYBERCRIME BY THE PUBLIC PROSECUTORS’ OFFICE OF THE REPUBLIC OF KOREA**

*(LEE, YOUNG JOO & KIM, YOUNG DAE)* ............................................................................................................ 25

1. Background ....................................................................................................................................................... 25

2. Organization of the Cybercrime Investigation Unit .................................................................................... 27

3. Primary Tasks of the Cybercrime Investigation Unit ................................................................................. 28
   A. Investigation Activities ........................................................................................................................... 28
   B. Enhancement of Investigation Competence in Cybercrime ................................................................. 29
   C. Empowerment of Digital Forensic Investigation ............................................................................... 29
   D. Promotion of International Cooperation and Assistance in Investigation among Related Organizations .......................................................................................................................... 31
IV. Examples of Major Cybercrime Investigations .................................................. 33
   A. DDoS Attack on the National Election Commission Website .................. 33
   B. Distribution of Digitally-manipulated Images of Celebrities .................. 34
   C. Database Leak from Chauffeur Service Companies .............................. 34
   D. Disclosure of Financial Fraud Organizations that Engaged in Voice Phishing ............................................................... 35
   E. Small-sum Fraud Exploiting the Loophole of WAP (Wireless Application Protocol) on Mobile Phones ........................................... 36
   F. Disclosure of Advertisement Companies using Illegal Keyboard Hooking Programs ............................................................. 36
   G. Collusion between Illegal Predatory Lenders and Mobile Communications Agencies ............................................................. 37
   H. Illegal Selection of Government-ordered Construction through Computer Hacking ................................................................. 38
   I. Korea-China-Japan International Smishing Fraud ........................................ 39

V. Conclusion ............................................................................................................. 39

RESPONSES TO CYBERCRIME BY THE KOREAN NATIONAL POLICE AGENCY (KIM, JAE WOON) ................................................................. 41

I. Introduction ............................................................................................................. 41

II. Development of Cybercrime Investigation Organizations ............................. 41
   A. Hacker Investigation Squad ........................................................................... 41
   B. Computer Crime Investigation Team .......................................................... 43
   C. Cyber Terror Response Center ...................................................................... 44

III. Recruitment of Cyber Police and Educational Training .............................. 45
   A. Size of Cyber Police Workforce .................................................................. 45
   B. Recruitment of Cyber Police ....................................................................... 46
   C. Educational Training of Cyber Police .......................................................... 47

IV. National Cyber Terror Response Activities ...................................................... 48

V. Cybercrime Investigation ....................................................................................... 49
   A. Receipt of Cybercrime Report and Counseling .......................................... 49
   B. Analysis by Types of Cybercrime ................................................................ 50
   C. Capacity Building for Digital Evidence Analysis ....................................... 52
   D. Establishment of Digital Evidence Physical Restoration Bureau ............... 52
   E. Supply of Digital Forensic Equipment .......................................................... 52

VI. Future Regional Directions ................................................................................ 53
THE CURRENT TRENDS OF VOICE PHISHING FRAUD:
LEGISLATION AND POLICY IMPLICATION
(YOON, HAE SUNG) ...................................................................................................... 133

I. Introduction ............................................................................................................. 133

II. Review of Amendment Direction on The Definition of Regulation for Voice Phishing Fraud Crime .............................................................. 134
   A. Understanding National and International Trends and Analysis of Types ................................................................................ 134
   B. Review of National and International Definition of Regulation .................................................. 136
   C. Seeking an Amendment Direction ........................................................................... 138

III. Review of Amendment Direction on the Definition of Penal Provisions on Voice Phishing Fraud Crime .................................................. 139
   A. Analysis of Types ................................................................................................ 139
   B. Punishment of Fraud Under the Criminal Code ................................................ 140
   C. Indirect Principle Offender of Fraud By Using Computer, etc. .................. 142
   D. International Trend ............................................................................................ 143
   E. Seeking an Amendment Direction ........................................................................ 147

IV. Conclusion .............................................................................................................. 150

CRIMINAL LAW AGAINST ELECTION CAMPAIGN ON SNS
(CHUN, HYUN WOOK) ...................................................................................................... 153

I. Introduction ............................................................................................................. 153

II. Non-Criminalization of Campaign Activities on the sns ........................................... 155
   A. Difficulties in Distinguishing Simple Expressions of Political Opinions and Campaign Activities on the SNS ......................................... 155
   B. Ambiguity of the Prerequisites in Paragraph 1, Article 93 of Election Law .................................................. 158
   C. Provisions that Allow Campaign Activities Using the SNS in Current Election Act ........................................................................... 161

III. Regulation of The Methods of Campaign Activities Using sns ................................. 162
   A. Whether SNS can be Included in the Campaign Activity Methods Allowed ................................................................................ 162
   B. Types of Still Prohibited SNS Election Campaign ........................................ 165

IV. Conclusion .............................................................................................................. 170
ANALYSIS AND IMPROVEMENT STRATEGIES FOR KOREA'S CYBER
SECURITY SYSTEMS REGULATIONS AND POLICIES
(SOUNG, JEA HYEN) ................................................................. 171

I. Introduction ......................................................................... 171

II. Korea's Cyber Security Laws and Policy Implementation .................. 172
    A. Status of Korea’s Cyber Security Management System ............... 173
    B. The National Cyber Security Strategy Council and the National
       Cyber Security Taskforce Committee .................................... 174
    C. National Cyber Security Center ............................................. 175
    D. Information Communications Infrastructure Protection Commission · 176
    E. The Private Information Conflict Mediation Commission ............ 176
    F. Industrial Technology Protection Committee ............................ 178
    G. Software Industry Conflict Mediation Committee ....................... 179

III. Problems and Improvements of Cyber Security Systems ................ 179

IV. Conclusion ......................................................................... 183
I. INTRODUCTION

People of today have taken advantage of technology as the information and communication technology (ICT) has transformed the societies all over the world. However, they have also abused and developed technology to commit criminal activities by creating new forms of high-tech-related crimes. These are so-called ‘cybercrime’ which includes penetration of the Internet security system, identity theft, fraud, defamation of character, illegal distribution of digital contents, etc. The rate of cybercrime has skyrocketed since the 1990s as the number of Internet users has dramatically increased. Thus, cybercrime is the fastest spreading and evolving crime in the 21st century.

The spread of the information and communication technologies has also created a digital divide between developed and developing countries. In order to narrow the digital gap and to become capable of handling and tackling cybercrimes, comprehensive information on trends and characteristics of cybercrime as well as methods to improve the skills to protect the countries against cybercrime should be provided in developing countries.

Under these circumstances, law enforcement officials and experts in cybercrime have carried out measures to respond to cybercrime. First, cybercrime-related issues were stipulated in national and international laws in order to prevent and combat such crimes. Since 2001, the European
Cybercrime in the Republic of Korea

Commission has tried to insert the provision on computer-related crimes to its proposals for the Council framework decision on attacks against information systems to make the Internet safer. Second, there have been efforts in cyberspace to combat cybercrime, such as strengthening online cooperation among law enforcement agencies, encouraging search and seizure of digital evidence in cyberspace, expanding jurisdiction over transnational cybercrime, and securing a sound cybercrime investigation procedure.

The Korean Institute of Criminology (KIC) has been actively involved in conducting research on cybercrime prevention since its establishment and has cooperated with the international community to combat cybercrime since 2005. With the United Nations Office on Drugs and Crime (UNODC), KIC successfully co-hosted a workshop on “Measures to Combat Computer-related Crime” during the 11th United Nations Congress on Crime Prevention and Criminal Justice. The declaration adopted by the Congress emphasized the need to enhance cooperation to prevent, investigate and prosecute high-technology and computer-related crime (A/RES/60/177, para.16).

It was also noted that a virtual forum or an online research network should be established to encourage communication among experts throughout the world on the issue of computer-related crime and the UNODC should provide technical assistance and training programs in order to address the lack of capacity and deal with the problems of such crimes (A/CONF.203/18, para.340(a)(b)). The declaration adopted in the workshop stated that the “Virtual Forum against Cybercrime (VFAC)” would be implemented for strengthening international cooperation in cybercrime prevention and control.

Against this backdrop, KIC and UNODC made joint efforts to establish the VFAC and convened five Expert Group Meetings and Steering Committee Meetings in Korea.1 Throughout those meetings, members of

the Steering Committee, International Consultant Group, and other participants from all regions exchanged their expertise and know-how in developing the project further.

The Virtual Forum against Cybercrime has two main goals: to offer technical assistance to developing countries by providing technical training on cybercrime investigation, and to provide a forum for communication and information-sharing among experts on cybercrime on its official website.

The VFAC website and the cybercrime training program are very unique in terms of representation and delivering methods. The VFAC homepage is a site for collecting information on cybercrime, a clearinghouse for cybercrime-related data. The cybercrime training program is an online-based training program providing basic knowledge of cybercrime as well as advanced technical skills of cybercrime investigation to law enforcement officers and judicial officials.

Since KIC officially launched the VFAC website on 16 October, 2009, and the online training program on 1 August, 2010, it has been providing practical information to law enforcement officers and research materials for scholars and researchers. The VFAC also provides comprehensive information and practical knowledge on cybercrime to the general public.

As modern society has rapidly shifted into the age of information and communication technology, high rate of cybercrime is inevitable. Cybercrime spreads quickly across borders and poses threats to individuals and social security. It is urgent that law enforcement officers fully understand what cybercrime is and have specific investigation skills. Proper training programs for law enforcement should be provided to control crimes, thereby protecting the general public both in cyberspace and in the real world.

In this respect, KIC has been involved in various efforts to develop training programs and conduct research on cybercrime control. VFAC will continue to support developing countries in their capacity-building efforts to combat cybercrime and establish effective criminal justice systems.
II. CYBERCRIME PREVENTION PROGRAMS DEVELOPED BY THE KOREAN INSTITUTE OF CRIMINOLOGY

A. KIC Research Projects and Programs on Cybercrime Prevention

KIC has been working on issues related to cybercrime since the late 1990s. First, KIC has been producing two to three research series on cybercrime prevention and related legislations every year, having published approximately 30 research papers so far. They cover almost every aspect of cybercrime, including juvenile crime in cyberspace, crime victimization in cyberspace, identity theft, defamation, illegal websites, cyber security, cyberterrorism and cloud computing.

In 2009, KIC published a separate volume entitled the “Study on the Internet Law” which covers cybercrime trends and various contemporary issues such as control in cyberspace versus freedom of speech, prevention of cyber violence, criminal law and civil law related to Internet matters, and introduction to the Information and Communication Network Act in Korea.

Second, from 2009 to 2011, KIC developed a series of law education programs targeting various groups in Korea such as elementary students, juvenile delinquents, released prisoners, international marriage migrant women, and adult and adolescent North Korean defectors.

In particular, the law education program for elementary students, developed in 2010, focused on cybercrime prevention. KIC also developed a manual for teachers, workbooks for students, and an ICT-based program (DVD). The researchers analyzed the most frequently committed cybercrimes among elementary students, narrowed down to the following list of cybercrimes: infringement of copyrights, cyber property crime, and cyber violence. This program was distributed to public elementary schools nationwide.

B. The Virtual Forum against Cybercrime

As cybercrime poses greater threat to our society, international and national bodies including the United Nations and various NGOs have made every effort to tackle cybercrime. The Republic of Korea has been actively participating in such multilateral efforts to counter cybercrime. To name a
few, KIC, Ministry of Justice, National Intelligence Service, National Police Agency, and other governmental and non-governmental organizations have created independent divisions or bureaus and have been engaging in providing criminal justice education and training programs on cybercrime prevention and investigation to developing countries in the Asia-Pacific region. This chapter will focus on the project undertaken by KIC under the auspices of the UNODC.

The idea of creating a virtual forum on cybercrime prevention first emanated from the 11th United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok, Thailand in 2005. In the Declaration adopted by the Congress and later endorsed by the United Nations General Assembly, the Congress noted that:

In the current period of globalization, information technology and the rapid development of new telecommunication and computer network systems have been accompanied by the abuse of those technologies for criminal purposes. We therefore welcome efforts to enhance and supplement existing cooperation to prevent, investigate, and prosecute high-technology and computer-related crime, including by developing partnerships with the private sector. We recognize the important contribution of the United Nations to regional and other international forums in the fight against cybercrime and invite the Commission on Crime Prevention and Criminal Justice, taking into account in that area under the aegis of the United Nations in partnership with other similarly focused organizations.²

At the same Congress, KIC organized a workshop on “Measures to Combat Computer-Related Crime” which highlighted the need to strengthen cooperation and measures against cybercrime, in which it was noted that:

[...] consideration should be given to the establishment of a virtual forum or online research network to encourage communication among experts throughout the world on the issue of computer-related crime (para.340(a)). Technical assistance and training should be provided by UNODC to States in order to address the lack of capacity and expertise to deal with the problems of computer-related crime. International cooperation should be developed in the areas of information exchange, research and analysis concerning computer-related crime.³

KIC presented the outcome of the Workshop at the 14th Session of the United Nations Commission on Crime Prevention and Criminal Justice in 2005. The Commission noted in its report that:

*The observer for the Korean Institute of Criminology made a presentation on the Workshop on Measures to Combat Computer-Related Crime. The outcome of the Workshop could be practically translated into a proposed technical assistance project on the prevention and control of cybercrime, the scope of which would be the development of a model training course for law enforcement personnel from developing countries with a rolling curriculum that included control and prevention. An expert group meeting was to be held in Seoul in 2006, with the participation of the institutes of the United Nations Crime Prevention and Criminal Justice Programme Network and the private sector, to develop the project to produce the model training course. The project would include a virtual expert forum under the auspices of UNODC to facilitate the exchange of information on new trends and approaches in the fight against cybercrime.*

Against this backdrop, KIC and UNODC agreed to establish the Virtual Forum against Cybercrime aiming to provide technical assistance and practical information to law enforcement officers and other relevant government officials through an online system.

To meet these goals, KIC convened the first expert group meeting in 2006, and organized five Expert Group Meetings and Steering Committee Meetings in Korea for the development of the Virtual Forum against Cybercrime. After years of preparation and through pilot tests and evaluation process, KIC officially launched the VFAC website and the online training program, in 2009 and 2010, respectively.

For research network, the VFAC website provides information on cybercrime trends and related materials including statistics, publications, list of organizations and experts worldwide to the public at large. It also acts as an informal international network of cybercrime experts, scholars and relevant practitioners.

---

The online training program is another part of the VFAC project, which provides online courses on cybercrime prevention for law enforcement personnel in developing countries. The courses are comprised of introductory and advanced seminar courses, lectured by world renowned experts and scholars in the field. The details of this project will be introduced in the following sections.

The development of this training and education program in criminal justice has gained considerable attention within the international community. During the Conference of the Parties to the United Nations Convention against Transnational Organized Crime held in Vienna, Austria, in October 2008, VFAC project was introduced by the UNODC as an exemplary model for providing technical assistance in partnership with relevant stakeholders (in this case, KIC) by providing assistance to criminal justice systems to address computer-related crime.\(^5\) In addition, in the Asia-Pacific Regional Preparatory Meeting of the 12\(^{th}\) UN Congress on Crime Prevention and Criminal Justice held in Bangkok, Thailand, in July 2009, it was recommended that centralized databases on cybercrime and training programs should be established to enhance the operational skills of law enforcement officers and other relevant agencies, in which regard the VFAC was introduced as a good example of training program to fight against cybercrime.\(^6\)

The efforts by the KIC, working in close cooperation with the UNODC to develop the Virtual Forum against Cybercrime not only serve as a role model in education and training programs in the international community but also provide technical and practical information on cybercrime investigation for law enforcement officers in developing countries.


III. EFFORTS AND ACHIEVEMENTS OF THE VIRTUAL FORUM AGAINST CYBERCRIME

A. Development and Launch of the Online Training Program

(1) Development of the Online Training Program

The Korean Institute of Criminology developed a pilot program in cooperation with the UNODC in 2008, targeting to law enforcement and police officers in Vietnam. With great success of launching a pilot program, KIC gave public notice of bidding for a program developer, and Sungkyunkwan University in Korea won the bid in 2009 and collaborated with KIC to develop the online training program.

KIC provided the lecture materials, such as syllabi, lecture contents, Q&A from lecturers for the University to develop animation characters based on the lecture contents. Images and voice-recording of the lectures were added to the video clip (Figure 2). Some lectures were selected to be posted on the VFAC website (Figure 1) to encourage website visitors to access them without having to log in.

(2) Curriculum and Certificates

The online training program is comprised of 130 lessons covering introductory and advanced courses. The introductory course has 35 lessons in Module 1 and 2, which were developed for judicial and law
enforcement officers in order to help them learn computer-related technologies and obtain general information on cybercrime trends and legislations.

The introductory courses demonstrate basic knowledge and understanding of cybercrime, and explain the risks associated with cybercrime and global networks, trends in cybercrime and understanding the practical and evidentiary requirements in the seizure and protection of computer-related evidence.

The advanced course consists of Module 3 and 4, providing more advanced information on cybercrime investigation techniques, such as identifying and tracing computer-related crime; applying investigative tools and strategies; applying data recognition; seizure and preservation procedures; understanding major forms of forensic interrogation of computers and related devices; describing the evidentiary aspects of cybercrime; the role of existing conventions and bi-lateral/multi-lateral arrangements; understanding topical and emerging issues in the investigation and control of cybercrime; using methodologies for acquiring forensic images; understanding national and international legal and ethical protocols; recognizing and resolving technical issues; and producing analytical procedures and performing the role of an expert in investigations and in court.

A seminar course in Module 5, as a part of the advanced course has been especially developed for experts, researchers and students in the cybercrime area to discuss recent issues on cybercrime. The curriculum is scheduled to be updated on a regular basis. Registered students take introductory and advanced courses for two months and six months respectively, with additional one week for mid-term and final-term exams. After finishing each course, KIC, as the VFAC Secretariat provide students with certificates of completion.

Following tables below provide the complete list of lectures offered by the online training program of the Virtual Forum against cybercrime, covering both introductory and advanced courses.
## Table 1  Curriculum for the Introductory Course

<table>
<thead>
<tr>
<th>Module</th>
<th>Courses</th>
</tr>
</thead>
<tbody>
<tr>
<td>0. Introduction to the Training Course of the Virtual Forum against Cybercrime</td>
<td>0.1 Introduction to the Training Courses of the Virtual Forum against Cybercrime</td>
</tr>
<tr>
<td></td>
<td>0.2 Cybercrimes in the global village (I)</td>
</tr>
<tr>
<td></td>
<td>0.3 Cybercrimes in the global village (II)</td>
</tr>
<tr>
<td>1. Understanding Information and Communication Technology</td>
<td>1.1 Understanding emerging trends in ICT &amp; cybercrime in the information age</td>
</tr>
<tr>
<td></td>
<td>1.2 Structure of the internet &amp; digital divide</td>
</tr>
<tr>
<td></td>
<td>1.3 Vulnerabilities of ICT</td>
</tr>
<tr>
<td></td>
<td>1.4 ICT &amp; network security</td>
</tr>
<tr>
<td></td>
<td>1.5 Forms of intrusion &amp; hacking</td>
</tr>
<tr>
<td></td>
<td>1.6 E-commerce &amp; forms of electronic payment</td>
</tr>
<tr>
<td></td>
<td>1.7 Digital evidence &amp; digital forensics for non-forensic specialists</td>
</tr>
<tr>
<td>2. Understanding Cybercrime Laws</td>
<td>2.1 Criminality: Definitions of cybercrime</td>
</tr>
<tr>
<td></td>
<td>2.2 Judicial issues in cybercrimes (I)</td>
</tr>
<tr>
<td></td>
<td>2.3 Judicial issues in cybercrimes (II)</td>
</tr>
<tr>
<td></td>
<td>2.4 Types of Cybercrimes (I): Cyber-property crimes</td>
</tr>
<tr>
<td></td>
<td>2.5 Types of Cybercrimes (II): E-commerce &amp; e-banking crimes</td>
</tr>
<tr>
<td></td>
<td>2.6 Types of Cybercrimes (III): Cyber-terrorism</td>
</tr>
<tr>
<td></td>
<td>2.7 Jurisdiction: The roles of national &amp; international law enforcement</td>
</tr>
<tr>
<td></td>
<td>2.8 International cooperation in the control of cybercrime</td>
</tr>
<tr>
<td></td>
<td>2.9 Compatibility of international conventions on cybercrime with domestic laws</td>
</tr>
<tr>
<td></td>
<td>2.10 Mutual legal assistance: methods &amp; problems: Procedures &amp; practices of online cooperation for law enforcement agencies</td>
</tr>
<tr>
<td></td>
<td>2.11 Digital evidence, preservation &amp; presentation of evidence for non-forensic specialists</td>
</tr>
<tr>
<td>Module</td>
<td>Courses</td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
</tr>
</tbody>
</table>
[3.2] Computer investigation techniques(II)  
[3.3] Investigation systems of developed countries  
[3.4] Criminal procedure and digital evidence  
[3.8] Modus Operandi of cybercrime and investigation techniques(IV): Terrorist use of the Internet  
[3.9] Preservation and presentation of digital evidence  
[3.10] Potential threats of anonymous communication  
[3.11] Network security  
[3.12] Incident response teams  
[3.13] Investigative best practices: Case studies  
[3.14] Practicum: Project exercise |
[4.2] Acquiring forensic images and preservation of digital evidence  
[4.3] Computer Forensics Tools Testing (CFTT)  
[4.4] Analytical procedure and forensic techniques(I): Program analysis  
[4.5] Analytical procedure and forensic techniques(II): Network analysis  
[4.6] Analytical procedure and forensic techniques(III): Database analysis  
[4.7] Analytical procedure and forensic techniques(IV): Digital evidence analysis  
[4.8] Email investigation  
[4.9] Keyword analysis  
[4.10] Internet activity analysis  
[4.11] Encryption and stenography  
[4.12] Computer security risks and remedies |
[5.2] Obscenity and offensive/racist materials  
[5.3] Online game and gambling  
[5.4] Potential threats from wireless technology  
[5.5] ID theft and online fraud  
[5.6] The challenge of cybercrime  
[5.7] Special topics issued by participants: Open forum |

Table 2: Curriculum for the Advanced Course
(3) Translation

In order to reach a broader audience, the VFAC online training program was translated into Thai, Vietnamese and Korean. KIC selected those three languages based on the trainees' strong demands and the first targeted groups for implementing the online training program. The lecture contents were translated by one of Korea's major translation companies and reviewed by cybercrime experts from local organizations in Vietnam and Thailand, in close cooperation with KIC. The translation process took six months for each language. Before starting the online program, students can select a language among English, Korean, Thai and Vietnamese on the main screen.

(4) Selection of Lecturers

KIC made every effort to expand and secure the prominent national and international experts in order to provide a best qualified curriculum. KIC invited world class professors and experts as lecturers while keeping ratio of nationality and gender. After three times of screening process to select lectures, KIC contracted to a total number of 28 lecturers working in academia and in the field as professor, prosecutor, police, investigator and researcher of Australian National University, Australian Institute of Criminology, Cybercrime Research Institute in Germany, Manonmaniam Sundaranar University, UNAFEI, Center for Cyber Victim Counseling from countries, including Australia, Germany, Hong Kong, India, Japan, UK, US and Korea.

(5) Official Launch of VFAC Online Training Program

In August 2010, an official opening ceremony was held for the launch of the online training program. The ceremony included congratulatory remarks made by lecturers and was attended by the VFAC online training program developer from Sungkyunkwan University, financial and advisory partners for the project from NHN (one of Korea’s largest Internet services providers) and other experts, practitioners, professors and prosecutors in the field of cybercrime who had contributed to the development of the VFAC online training program.
(6) MOU Requirement

Organizations that wish to participate in the online training program are required to complete a memorandum of understanding with KIC, the process of which is described below.

a. Introduction between two organizations

KIC provides information on the VFAC, including VFAC brochure and, when requested, a video clip for a better understanding of the objective of the online training program, target students, and curriculum and descriptions of the online lectures. A partner organization briefly introduces itself to KIC, such as the name, role, and characteristics of the department in charge of the management of this online training program. In addition, the organization designates its single contact point and informs KIC.

b. Designation of contact points

The contact point of the partner organization provides information on the Internet environment to implement the online training program. The contact point cooperates with KIC to review the draft MOU prepared by KIC. When amendment of the MOU is necessary, both parties discuss the matter to reach an agreement.

c. Completion of MOU

When both parties agree on the contents of MOU, two copies of MOU are conveyed via air mail or a direct visit to the organization. In the case of air mail, one copy of MOU should be sent back to KIC after a signee of the partner organization signs the MOU. After signing the MOU, the contact point is required to provide the curriculum vitae of each trainee for his or her log-in account (personal ID and password) of the online training program.

d. Follow-up and implementation of the training program

Based on the curriculum vitae of the trainees, the Student Selection Committee of VFAC assigns each trainee into Introductory and Advanced Courses. Prior to initiation of the online training program, KIC offers a pilot lesson to the contact point of the partner organization to test its own Internet environment. When the Internet environment turns out to be
adequate to implement this program, KIC sends the trainee a student manual that explains how to operate the program. The trainees can then take the online lessons.

e. Feedback on the courses

KIC distributes a questionnaire to trainees for evaluation after completing the courses and makes a request to the contact person to submit the evaluation papers completed by trainees.

(7) Partner Organizations

KIC has signed MOU with several Asian and African countries as shown below in Table 3 to implement the VFAC online training program, provided the introductory courses, and offered certificates to the students who had completed the courses. Apart from this, KIC has given online training lectures under the title of ‘Challenges of Cybercrime’ and ‘Cybercrime Controlling System in Korea’ to several practitioners and experts from Asian and African countries who visited the Institute of Justice in Korea through the KOICA program.

<table>
<thead>
<tr>
<th>Name of Organization</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of the Attorney General, Kingdom of Thailand</td>
<td>July 1, 2011</td>
</tr>
<tr>
<td>Ministry of Justice, Ethiopia</td>
<td>May 9, 2011</td>
</tr>
<tr>
<td>Directorate of Public Prosecutions, Tanzania</td>
<td>April 15, 2011</td>
</tr>
<tr>
<td>Ministry of Justice, Thailand</td>
<td>October 10, 2010</td>
</tr>
<tr>
<td>Office of the Special Envoy on Transnational Crime, Republic of the Philippines</td>
<td>December 18, 2009</td>
</tr>
<tr>
<td>National Law Development Agency Ministry of Legal Affairs and Human Rights, Indonesia</td>
<td>December 8, 2009</td>
</tr>
<tr>
<td>CyberSecurity Malaysia, Malaysia</td>
<td>November 16, 2009</td>
</tr>
<tr>
<td>Institute for Crime Prevention, Ministry of Justice, People’s Republic of China</td>
<td>July 30, 2009</td>
</tr>
</tbody>
</table>

Table 3 List of Partner Organizations
(8) VFAC 2.0

In order to meet international demands, the contents of the VFAC online training program are expected to be modified and revised to cover the African and Latin American regions. KIC also considered of signing MOU with the Office of the Attorney General and Police in Brunei, Kenya and Malaysia. At the end of 2012, KIC produced CDs and DVDs in cooperation with the online training program developer, Sungkyunkwan University, and distributed them to the VFAC online training program partner organizations.
B. Development and Launch of the Research Network

(1) Development of the Research Network

Cyberspace has become a place not only for new types of activities, but also for communication channels. In particular, military forces are also covering cyberspace into a military activity areas, including territory, sea, aviation and space, which means cyberspace has been regarded as an important place for the military purpose. In a nutshell, cyberspace can be understood in different ways by each sector and can be used as different types of research topics by each academic researcher.

However, the problem is that the persons who are in charge of combating cybercrime are not familiar with cyberspace and inexperienced in cybercrime law, legislation and investigation technologies. If they have different levels of understanding on cybercrime, they will introduce different levels of measures to combat cybercrime. Practitioners like cybercrime-related legislators or law enforcement officers and scholars have already understood the existence of understanding gap; however, they are also aware of the difficulties of filling the gap. Furthermore, this understanding gap causes a variety of problems in combating cybercrimes, which is not limited to one country, but reaches far beyond all over the world where cybercrime issues are raised.

KIC established the website of the Virtual Forum against Cybercrime (VFAC), a Research Network, which is another pillar of VFAC project along with the online training program. The objective is to narrow the gap in countering cybercrime through discussions among experts at the international level. One of the benefits of the VFAC website is that it enables cybercrime experts and professionals to share information and expand their views. It also narrows the understanding gap of cybercrime not only between practitioners and scholars, but also between developed and developing countries.

For this project, KIC first sent an invitation letter to the world class experts to join the Network and they formed the International Consultant Group (ICG). In 2009, like the online training program, KIC opened a pilot website of VFAC and asked ICG to review the contents and provide their feedback. Based on the opinions of the experts, KIC enhanced the security of the website, improved its functions and checked the database.
on a regular basis. KIC conducted a successful opening ceremony in October 2009, which was prior to the launch of the online training program. After two times of website revision, the main page of website was completed as shown below [Picture 5]. To meet the international demand, KIC is also making VFAC website suitable for both PC and mobile phone.

(2) Contents of the Research Network

a. Objective

The objectives of the VFAC can be summarized into two: one is to provide a clearinghouse for research and database in relation to statistics, legislation, institution and world renowned experts; the other is to build a communication and knowledge network among scholars and practitioners. The functions of the VFAC based on two objectives are interrelated. In other words, research on cybercrime and knowledge-based network are established though the Research Network, and this process is included in the online training program and vice versa. To do this, KIC has continuously posted information on cybercrime trends and experts views on
the Research Network on its website. It cannot be emphasized enough that KIC continues to devise the method to effectively deliver useful information to relevant institutions, so that it will contribute to the research work, government policy making, and strong ties between scholars and practitioners.

![Figure 6](image-url) Correlation among Various Entities for Combating Cybercrime

**b. Main categories**

The Research Network includes information on current cybercrime trends and issues, statistics, experts and professionals, publications, cybercrime-related institutions, legislations, and seminars and conferences, as well as other research products. Persons who are interested in cybercrime can access the website without login. If you are registered as a member of ‘expert or professional’ of the secretariat, you can freely participate in the online discussion on cybercrime and utilize the information on the VFAC website.
C. Management of the Virtual Forum against Cybercrime Website

(1) Information Clearinghouse

VFAC website plays a key role as an information clearinghouse in providing cybercrime-related information to people interested in cybercrime. In other words, it functions as an online library in the field of cybercrime. In particular, the major contents posted on the website are the opinions or views of the cybercrime experts, which makes the website more reliable. The information uploaded on the website is as below and is updated on a regular basis.

- Computer crime (Unauthorized access, database theft, spam, phishing)
- Internet-related crimes such as online-fraud, ID theft, money laundering
- Cyber-stalking
- Child grooming, child pornography
- Online organized crime and international organized crime
- Botnet, Malware
- Security accidents and releasing security information
- Response of legal agencies relating to cybercrime
- Efforts to control cybercrime
- Research for advanced technology of information security

The total amount of information stored on the website is about 5,000 cases and articles on cybercrime. One thing to note is that KIC regularly conducts a screening of the contents to make sure that the contents are of good quality. Information posted on the website is arranged in the order that visitors can easily find the information they need. The Q&A service is also provided to visitors.

(2) Management of the Research Network

The Research Network is composed of four types of member groups: experts, practitioners, industry members, and external industry members. First, ‘experts’ are those who are professionals with extended knowledge of cybercrime and included in the experts category of the clearinghouse on the VFAC website. Visitors can find experts profiles on the website and ask for their advice. 75 experts are listed on the website. Second,
‘practitioners’ are those who are supporting the VFAC project in the field. The number of practitioners is approximately 20 and the number continues to increase. Third, industry members are those who have expertise and are working in the cybercrime-related area in a direct or an indirect way. 30 or more people are registered on the website. Lastly, external industry members are those who are not closely connected to and not involved in the VFAC project. They are potential members of VFAC experts, practitioners and industry members groups.

The Research Network is for building a strong tie between practitioners and experts working in the cybercrime field. After VFAC has extended its role to be a clearinghouse, VFAC’s Research Network is expected to provide a place for information sharing and communication channels. In this way, more trainees and participants will take advantage of the VFAC online training program and gain more opportunities to take the online lessons. In addition, activities like information sharing between members and notice of thesis promotion will support more research activities.

The number of cybercrime experts and professionals cannot outnumber the number of cybercrime cases all around the world and the types of crime continue to increase and develop. Therefore, it is necessary that the members of knowledge-based research network should be linked each other more closely to counter rapidly developing cybercrimes and techniques.

(3) VFAC Newsletter

The first issue of the VFAC Review (previously ‘VFAC Newsletter’) was published in June 2011. Its main contents include cybercrime trends and recent information posted on the website, and articles by the prominent cybercrime experts and scholars. Review plays a key role in promoting and introducing the Research Network nationally and internationally. In addition, it provides the research on cybercrime conducted by researchers in KIC.

VFAC Review is published monthly and distributed in the form of PDF file via email. PDF file is reader-friendly and readers can have access to the file regardless of the Internet operating system and devices. Furthermore, hyperlinks in the PDF file can easily guide readers to find relevant information directly.
Cybercrime Prevention Programs of the Korean Institute of Criminology

Figure 7  Layout Change of the VFAC Newsletter

Figure 8  VFAC-related Websites on Social Network Services
Social Network Service is newly regarded as a forum for information sharing and communication channels. SNS is very important considering the characteristics of VFAC and its role as an online communication channel worldwide. People who want to find information can have more possibilities to be informed about VFAC through a search engine uploaded in SNS. VFAC helps online users to be more connected each other and understand the current crime trends, concerns and countermeasures.

IV. FUTURE GOALS OF KIC CYBERCRIME PREVENTION PROGRAMS

The main purpose of developing the VFAC program was to reinforce international network to fight against the fast growing high-tech and computer-related crimes. KIC and the UNODC have acknowledged that these new forms of crimes are committed across the border. Resolutions at an international level are necessary to prevent such crimes. However, a significant digital gap between developed and developing countries exists.

The VFAC online training program and the Research Network, as well as the VFAC Review provide practical information to experts on cybercrime, scholars and law enforcement officers worldwide. In addition, the discussion group of the Research Network functions as a forum consisting of cybercrime experts worldwide to enhance cooperation and exchange information. The VFAC has achieved its purpose in this regard. However, the VFAC project still bears some tasks ahead.

First task is the revision of the online training program. As the forms of cybercrime evolve rapidly, the curriculum and contents of the online training program need to be continuously updated and revised. KIC has established a revising committee consisting of cybercrime experts in Korea and the secretariat of the VFAC7 to review the curriculum and its contents thoroughly, and the Committee submitted the outcome in 2011.

Based on the outcome of the Committee, KIC has set up an updated version of the curriculum in 2012. KIC has been working on developing the second version of VFAC program which will contain new contents of

7 KIC appointed Professor Jin-Hyuck Justin Choi of Daejun University as Chair of the Committee on the Revision of the VFAC Online Training Program, and Mr. Sanghoon Chung of KAIST Cybersecurity Research Center, Professor Won-Sang Lee of Chosun University and Ms. Younmi Lee of KIC as its members.
online courses and be operable on the new VFAC website. In the meantime, KIC is expanding its cooperation with relevant organizations in developing countries to provide the VFAC online training program.

Second task is the renewal of the VFAC website. More than six years have passed since KIC first developed the VFAC website. Considering rapidly developing information technology, it is necessary to upgrade the system and redesign the website. Thus, as of December 2013, KIC completed the renewal of the VFAC website, including the overall design of the website and replacement of the operating system into a latest version.

Third task of KIC is to expand the function of the discussion group in the Research Network. KIC is planning to host an offline forum to gather the members of the VFAC discussion group to discuss the recent cybercrime trends, issues and countermeasures in depth. The offline forum will be organized this year in Seoul, Korea.

V. CONCLUSION

According to a document produced by the UNODC in 2011, at least 2.3 billion people, equivalent to more than one-third of the world population, had access to the Internet. By 2017, it is estimated that 70 percent of the world population will subscribe to the mobile broadband. The number of network devices is expected to outnumber people by six to one, transforming the current concept of the Internet by 2020.8

As one might imagine, rapid development of the Internet and the electronic information technology has already become and will become a more crucial part of our daily lives. The issue on cyber security has also been raised at the national and international level.

This chapter emphasized the need to raise awareness on the risks of cybercrime and enhance public security in the criminal justice system. The VFAC functions as a good example of building close relationship among

---

organizations worldwide in establishing international criminal justice system for cybercrime prevention and investigation, and plays a significant role in education and training program.

As the only national institute in the field of crime prevention and criminal justice in Korea and the member institute of the United Nations Crime Prevention and Criminal Justice Programme Network, KIC will continue to dedicate to the fight against cybercrime and transnational organized crime by developing and providing practical resources and valuable materials to relevant international organizations. Furthermore, KIC will expand its efforts to become a hub of research on cybercrime and criminal justice.
I. BACKGROUND

South Korea has made remarkable development in the field of information and communications. By 2012, the number of Internet users had reached 84.1% of the entire Korean population, placing Korea on the 21st place among 211 countries. The average Internet speed as of the first quarter of 2013 was measured at 14.2Mbps, the fastest in the world. At the same time, however, cybercrime is increasing and its tactics are becoming highly specialized.

Generally speaking, there are two major types of cybercrime: *crime by use of cyberspace* and *crime specific to cyberspace*. The limits of existing regulations had manifested as traditional forms of crime extended into cyberspace, such as infringement of personal information, Internet fraud, cyber defamation, and cyber stalking. It is difficult to apply existing laws to new types of crime such as hacking, spreading of malicious codes, and DDoS attacks. Meanwhile, in January 2011, gangsters who run illegal gambling websites hired hackers to launch a series of distributed denial-of-service (DDoS) attacks on over 100 of its competing gambling sites. As such, cybercrime is becoming highly relevant in serious crimes, which makes professional

---

* This article is summarized from research outcome of scientific investigation conducted by the Prosecutor's Office, internal data of the Seoul Central District Prosecutors' Office's and press releases on cybercrime investigations.

** Prosecutor, Research Fellow, Korean Institute of Criminology

*** Prosecutor, Forensic Science Planning Officer, the Supreme Prosecutors’ Office

1 Sung Eun Yang, “Cybercrime Trends and Criminal Liability,” Internet & Security Focus (September 2013).

investigation and analysis techniques absolutely vital for cybercrime investigations.

In order to effectively combat organized cybercrime, building a specialized response system specific to cybercrime is essential. In November 2011, the South Korean prosecution established the Cybercrime Investigation Unit within the National Digital Forensics Center (NDFC) of the Supreme Prosecutor's Office, and the Cybercrime Investigation Center within High-tech Crime Department 2 of the Seoul Central District Prosecutors Office, each body exclusively dedicated to the investigation of cybercrime. The former collects cybercrime-related information with the aim of establishing a state-of-the-art investigation system for cybercrime that can respond effectively to the rapidly changing environment. The latter carries out investigations on cybercrime cases by directly applying information and intelligence obtained from the Supreme Prosecutor's Office.

In South Korea, investigation of cybercrime is conducted primarily by the police and the prosecution. The police is mainly involved in the investigation of cybercrime at the scene of the crime, and the prosecution investigates cases of major social concern but within a limited range. The Korean National Police Agency is known to have approximately 900 cybercrime investigators, and the prosecution approximately 50 professional investigators.

Cyber terrorism, has also frequently occurred in Korea, many cases of which are understood to have been launched by North Korea. Examples are DDoS attacks on the official website for Cheong Wa Dae, Korean presidential office, on July 7, 2009, another DDoS attack on the Ministry of Foreign Affairs and Trade website on March 4, 2011, and hacking into the databases of Korea's major banks, press and broadcasting outlets. Such acts of cyber terrorism are known to be Advanced Persistent Threat (APT) attacks, thoroughly planned for several months to destroy stored information at the time of the attack.

Cyber terrorism is controlled by the National Crisis Management Assessment Committee with Cheong Wa Dae as the control tower and participated by the National Intelligence Service, South Korea Internet and

---

3 Supreme Prosecutor's Office Directive No. 168, Regulations on the Establishment and Operation of the Cybercrime Investigation Center of the Supreme Prosecutor's Office
Security Agency (KISA), the Prosecutor’s Office, the National Police Agency and other major national authorities. In the case of cyber attacks or threats, they closely cooperate amongst themselves through exchanging information and forming joint response teams, for instance. In addition, cyber security companies and private institutions cooperate by sharing latest information on malicious codes and monitoring potential malware distributors. In order to prevent cyber terrorism, public-private cooperation is essential.

II. ORGANIZATION OF THE CYBERCRIME INVESTIGATION UNIT

Prior to the establishment of the Cybercrime Investigation Unit (CIU) at the Supreme Prosecutor's Office, cybercrime-related tasks were divided between the Internet Crime Investigation Center and the Cyber Control Team of the Digital Investigation Office. The Internet Crime Investigation Center was in charge of high tech crimes including cybercrime, and the Cyber Control Team supported cybercrime investigations by developing forensic techniques regarding collection and analysis of digital evidence.

By performing the roles previously divided between these two entities, the newly-established CIU has enabled efficient and expeditious investigation of cybercrime. As the importance of collecting and analyzing digital evidence becomes more evident in all areas of investigation by the prosecution, the scope of CIU's work encompasses strengthening investigation capacity and conducting research on various investigation techniques and tools.

Following the establishment of the Unit, the prosecution has further strengthened its human resources by hiring private security experts and white hat hackers as special investigators. Moreover, internal investigators and IT professionals undergo regular systematic training to strengthen their expertise in cybercrime investigation.
III. PRIMARY TASKS OF THE CYBERCRIME INVESTIGATION UNIT

A. Investigation Activities

Various types of crimes occur in the cyberspace, including Internet gambling sites, web hard companies, copyright infringement, identity theft, hiring hackers, Internet phishing, defamation and among others. The collection and analysis of cyber evidence are becoming more important in order to dismantle illegal websites. Likewise, this evidence is also essential in all investigations in the field that demands continuous and strengthened investigation of the Prosecutor's Office within the Supreme Prosecutor's Office in each area.

The Cybercrime Investigation Division transmits investigation data on crimes that occur in cyberspace, collected through criminal investigation and intelligence production, to the Supreme Prosecutor's Office. It meticulously analyses and gathers information. If necessary, the Supreme Prosecutor's Office sends investigators to the front-line support services or provides network analysis. In the future, cybercrime through personal blogs, Facebook, among other media will be expanded by systematic acquisition channels, National Internet Development Agency of Korea, and financial security researchers. By expanding cooperation with relevant organizations and interactions, cybercrime defense will be reinforced through collected information.

Malicious code analysis system is conducted electronically to handle malicious code extraction, analysis, tracking, and a series of criminal process electronically. In order to take firm legal action against the use of Smart phones, social media websites (e.g., Twitter, Facebook) and file-sharing websites in spreading of malicious code, the advance system of duplexing analysis system DB, expanding linkage analysis system and consisting memory forensics analysis environment, such as configuring, are required.

4 Some of the major cases will be introduced in Chapter 4.
B. Enhancement of Investigation Competence in Cybercrime

After the establishment of the Cyber Crime Division Prosecutor's Office, the Supreme Prosecutor's Office has appointed 61 prosecutors in 58 branch offices in the District Prosecutor's Offices to spread and share recent trends in cybercrime, investigation practices, analyze, disseminate know-how and techniques in exclusive national inspection workshops for cybercrime. Also education programs aimed at training experts by 2016 has been initiated according to its 5-year roadmap. In addition, IT experts such as Information Security Officers and hackers were invited to the Cyber Crime Investigation Forum which was established to discuss the latest technology trends and key issues. Auto-detect systems which were developed by the Cybercrime Division in the Supreme Prosecutor's Office were sent to major government agencies in order to help detect and analyze suspicious phishing websites.

Furthermore, the office plans to work on the maintenance of investigation infrastructure, such as by designing the Cyber Crime Profiling System, establishing a system for gathering and preserving digitalized cybercrime related evidence. Moreover, along with recruiting top class human resources specialized in malicious codes and information security, the office will continue to provide intensive and rigorous training.

C. Empowerment of Digital Forensic Investigation

An understanding of digital forensics is crucial in investigating cybercrime. Digital forensic analysis ability has become a prerequisite, not only for cybercrime investigations, but for any modern investigation due to the digitalization of individual and business activities. In the case of individual crime, it is necessary to check personal electronic devices because most data are saved on smartphones, tablet PCs, SNS, personal PCs or USBs (portable data storage device). In the case of corporate crime, it is necessary to check the ERP (Enterprise Resource Planning) system of the company, cloud systems, etc. which can be found in corporate computing systems.

Digital forensic is a process which includes: identifying electronic data that could be saved on computers or digital storage devices; identifying any electronic data which is sent through the network; gathering and analyzing
Recognizing the importance of these processes, the Korean prosecution established the administration office of digital forensic investigations in 2005, and also created digital forensic teams along with 7 other frontline digital teams within the Seoul Central District Prosecutors’ Office between 2007 and 2012. Six more digital foresics teams are expected to open soon. As individuals’ and corporations’ activities become more highly digitalized, requests for assistance related to digital forensic investigations are rapidly increasing each year.

<table>
<thead>
<tr>
<th>Year</th>
<th>No. of cases</th>
<th>Increase rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>1,409</td>
<td>170%</td>
</tr>
<tr>
<td>2010</td>
<td>2,633</td>
<td>187%</td>
</tr>
<tr>
<td>2011</td>
<td>3,979</td>
<td>151%</td>
</tr>
<tr>
<td>2012</td>
<td>6,301</td>
<td>158%</td>
</tr>
<tr>
<td>2013 (as of September)</td>
<td>4,909</td>
<td>-</td>
</tr>
</tbody>
</table>

**Table 1** Number of Cases with Investigation Support from CIU

The primary responsibilities include (i) computer forensics (targeting digital storage devices such as computers, laptops, external hard drives, PC tablets, etc. to collect and restore any suspicious facts related to digital evidences; in-depth analysis of the evidence; and giving testimony in court), (ii) crypto analysis (unlocking the passwords of digital evidences in any seized hard discs, USB memory sticks, and files through various methods for the investigation team during their search), (iii) database forensics (downloading DB forensics, financial information used by companies and organizations, emails, electronic liquidations, business databases, etc. from the information-based system of the corporations or institutions to analyze and transform these active data into files; restoring every type of financial data, electronic files and emails and providing these results to the investigation team; and when necessary, testifying at trial regarding the results or providing the investigation team with technical consultation), and (iv) mobile forensics (obtaining memory data of cell phones, such as smart phones and PC tablets, to analyze and restore any text messages, call logs, contact information, pictures, videos, etc.).
Regarding digital forensics, the most important issue is to train the experts. Hence, in 2001, the Supreme Prosecutors' Office opened the ‘Digital Forensics Specialist Training Courses.’ This training course provides in total six months of training which dedicates three months to learning related theories and another three months to practical training. Through these training programs, experts are trained to become qualified digital forensic investigators. The course also provides digital forensics expert training to the National Tax Service, the Ministry of National Defense and other related agencies. As of today, a total of 180 people have completed this training along with 146 prosecution investigation officers, 34 investigators of the National Tax Service, and many other experts from 17 related organizations.

In addition, the ‘Digital Forensic Institute’ was established in the Prosecutor's Office in August 2013 in response to the rapidly changing IT environment. This institute has a long-term development plan regarding digital forensic techniques and tools for systematic research on cybercrime.

D. Promotion of International Cooperation and Assistance in Investigation among Related Organizations

As it becomes increasingly necessary to reinforce cybercrime combating systems at the national level, the CIU held a conference in January 2012 with the participation of Ministry of Public Administration and Security, Department of Defense, the Korea Communications Commission, Finance Committee, the Korea Internet & Security Agency (KISA) and 10 other national organizations. The purpose of this conference was to have closer cooperation through increased coordination and policy planning in cybercrime, as well as development of related systems and research. In addition, the conference was aimed at practically and systematically responding to cybercrime through rapid evidence collection and information exchange, exchange of analytical strategies on malicious codes among related organizations and research development by raising awareness regarding cyberspace attacks and its response capabilities.

On February 10, 2012, the CIU brought forward detailed countermeasures as discussed in this previous conference, and held a follow-up conference with the consultative body composed of national organizations and practitioners of public institutions and private companies in order to devise
a response mechanism in case of an emergency. This conference consisted of cybercrime-related national organizations, such as the National Intelligence Service, the Ministry of Public Administration and Security and the Korea Communications Commission and 40 other press agencies, portals and vaccine manufacture-related organizations. It also organized regular meetings every quarter. For future reference, the division should try to involve other bodies, such as national organizations, IT businesses, and academic institutions of industry-academic cooperation to become its members, so that a broader range of experiences and best practices can be exchanged.

In addition, as the use of international servers becomes an increasingly common method of committing cybercrime, international cooperation is now key to conducting successful investigations. However, the traditional process of international cooperation in criminal justice through diplomatic channels takes a considerable amount of time; therefore, it is unsuitable for cybercrime which requires rapid preservation of evidence, log tracking and so on. Hence, the CIU takes responsibility as a national representative in the ‘High-tech crime 24/7 network’ by being the focal point for Korea. Also, its efforts continue in building cooperative systems with major partners in Asia, such as China and the Southeast Asian countries for to increase the effectiveness and speed of cooperation.

In October 2013, the Seoul Conference on Cyber Space 2013 launched its third international meeting in Seoul. The prosecution participated in agenda planning with the cooperation of the Ministry of Foreign Affairs and Korea Communications Commission. Out of its 6 discussion topics, the prosecution specifically presented on the cybercrime at the panel. Also it plans to take active part in the Internet consultative group meeting between China and Korea to discuss the prevention of cybercrime spreading from China.

In order to respond effectively to the advanced and trans-nationalized cybercrime and meet the global standard, it is necessary to join international agreements. The CIU is leading the reinforcement and development of the international regulations by organizing official national discussions regarding the ‘Council of Europe Convention on Cybercrime’ in

5 High-tech crime 24/7 Network was founded and is currently led by the G8 countries and 58 other countries to join in the activities and cooperation regarding cybercrime.
cooperation with the Ministry of Foreign Affairs, the National Intelligence Service, the Korea Communications Commission and other related organizations. Also they are pushing forward the development of related domestic regulations and policies.

IV. EXAMPLES OF MAJOR CYBERCRIME INVESTIGATIONS

A. DDoS Attack on the National Election Commission Website

In January 2012, the prosecution indicted seven people including ‘Gong’, chauffeur of Assemblyman, ‘Choi’ and ‘Cha’, employees of a gambling site operator, and ‘Kim’, protocol secretary of Chairman of the National Assembly, for allegedly taking part in the DDoS attacks which occurred on October 26, 2011 against the website of the National Election Commission.

This was considered to be the first election terror case in the history of constitutional government and it proceeded as follows: With the 17th National Assemblymen Election near at hand, Kim, the protocol secretary of the Chairman of the National Assembly, and Gong, chauffeur of Assemblyman, conspired to make an attack on the National Election Commission. When these two entrusted DDoS attacks on the National Election Commission website to Gang, an employee of an illegal gambling site operator, Gang then directed Kim to be in charge of the DDoS attacks. In the end, Kim committed the criminal act by launching the DDoS attacks. The police carried out their first investigation of the case, and as soon as it was handed over to the prosecution, the prosecution proceeded with a full-scale reinvestigation in the tracking of 547 financial accounts in total, the inquiry about details of phone calls regarding 353 phone numbers in total, the seizure and search of seven venues including the Assemblyman Hall, 111 cases of mobile and computer analysis and the examination on 44 testifiers including Assemblyman Choi.

6 The High-tech Criminal Investigation Part 2 of the Seoul Central District Prosecutors' Office is in charge of cybercrime investigation. Seoul Central District Prosecutors' Office has High-tech Criminal Investigation Department Part 1 with deals with industrial technology leakage related crime, and High-tech Criminal Investigation Department Part 2 which concerns investigation and processing of high-tech crime, maintenance-related information and data collection, information processing devices such as computers and telecommunications media and the evidence seized in the search and analysis of data.
In particular, the prosecution carried out recovery analysis of Kim’s desktop and Gong’s laptop, and secured the evidence to prove conspiracy of crime between Kim and Gong, as well as the remittance of honorarium through the restoration of SMS messages in smart phones, the wide-range analysis of phone call details, the comparison and analysis of records of access to the website of the National Election Commission before election day.

B. Distribution of Digitally-manipulated Images of Celebrities

In January 2012, the prosecution charged seven offenders for distributing digitally-manipulated images of celebrities, and among them, Moon was arrested and charged with the violation of the Promotion of Information and Communication Network Use and Protection of Information Act for intentionally spreading over 2,000 images of 157 female celebrities that had been digitally manipulated. Lee and four others were charged without detention and two teenagers were sent to Juvenile Court while removing all related images on various Internet portals (including U.S. websites) to prevent the images from spreading elsewhere.

The prosecution received an investigation request from the general public about the spread of obscene images of celebrities on an Internet community site. A widespread Internet monitoring revealed that the amount of images that had been distributed and the level of obscenity were far too serious. It was also revealed that the motivation for distributing such images was to earn web hard points and other economic benefits. Therefore, the prosecution launched an investigation right away. This is an example of declaring the prosecution's will to heavily punish offenders of defamation hiding behind anonymity allowed by the Internet.

C. Database Leak from Chauffeur Service Companies

In April 2012, the prosecution indicted a database seller, "N" (male, age 33), who had sold personal information of clients of chauffeur service companies after receiving the database from "K", a hacker residing in the Philippines. K then illegally hacked into the company websites using the administrator ID and password to obtain the database, a violation of the Information and Communications Network Act (hacking into an information and communications network). The prosecution also indicted
seven people without detention including "D" (age 53) who had purchased and used the database for the same crime.

This crime was committed by a professional hacker who had leaked personal information of half of the nation's car owners for the purpose of selling the personal information database. This database contained information relating to customers of chauffeur services companies which could be abused for various kinds of crime such as financial fraud by voice phishing.

The investigation revealed that personal information database is highly vulnerable in security, and these stolen personal information database are being traded illegally. Therefore, it is necessary to strengthen the security on personal information database sites with more protection and always be aware that these crimes of database leak may occur at any time through hacking attempts.

D. Disclosure of Financial Fraud Organizations that Engaged in Voice Phishing

In May 2012, the prosecution indicted with detention seven persons in total, including ‘K’ (male, 51 years old) on charge of fraud, who sent out loan advertisement messages on a mobile phone to those having difficulties in getting a loan from financial institutions, and swindled approximately 3.4 billion KRW from roughly 2,330 victims between November 2011 and April 2012.

The method employed in this case was the use of Internet phone which converted the outgoing phone calls automatically to representative phone numbers of legitimate financial institutions, which demonstrated how the methods of crime in voice phishing had become even more sophisticated and intelligent. This case raised public concerns over electronic telecommunications marketing and the public demanded that, in order to prevent damages caused by financial fraud via phone, mandatory technical measures be taken including the blocking of falsely-marked phone numbers.
E. Small-sum Fraud Exploiting the Loophole of WAP (Wireless Application Protocol) on Mobile Phones

In June 2012, the prosecution indicted with detention of one mobile phone operator who had swindled 287 million KRW from mobile phone users by charging them for services that they did not use by manipulating the automatic WAP (Wireless Application Protocol) system, and indicted without detention one accomplice, and directed an open search for another accomplice who had fled.

This case is a criminal act that exploited the loophole of WAP system. Under this system, some telecommunication operators and their payment gateways do not send any SMS message to mobile phone users with regard to the details of payment under the amount of 1,000 KRW. In this case, the accused had exploited this loophole of the WAP system. This case confirmed the need to change the current practices of some telecommunication operators, so that mobile phone users are always informed of any payment made via their phones, irrespective of the amount.

F. Disclosure of Advertisement Companies using Illegal Keyboard Hooking Programs

In August 2012, the prosecution disclosed illegal advertisement companies that had indiscriminately distributed a keyboard hooking program through the Internet and thereafter gained an income of approximately 2.4 billion advertisement fees for a year. The method used involved the user of a computer entering a search word in big portal sites such as ‘Naver’, followed by advertisements of advertisers recruited by them appearing as if they were advertisements provided by the portal site. The prosecution indicted without detention 9 persons (including 3 corporations) in total including operator “K” (male, 49).

This is a case of illegal advertisement on the Internet exploiting the

---

7 WAP (Wireless Application Protocol) method refers to the payment method that if the operator (CP) notifies the Payment Gateway (PG) with the details of service use, the CP or the PG sends the details of payment to users of mobile phone through SMS message.

8 The program that if the users of computer enter a search word (keyword) in the search box of big portal sites, snatches (i.e. hooking) a search word without the users of computer knowing and sends it to a server of suspects and confirms if there are any registered contents as that search word, and exposes the contents on the screen of users to display the result of search.
keyword hooking program that can expose the advertisements as if they were the advertisements provided in portal sites like 'Naver', without affecting the operation itself of portal sites. The keyword hooking program can be manufactured easily at low cost by anybody due to its very simple principle of operation while the gain of advertisement fees using the program is enormous, so the necessity to control the illegal advertisement in such way has been raised continuously because of its prevalence. However, big portal sites like 'Naver' failed to respond effectively due to technical problems and economic conditions. At this, the prosecution disclosed professional keyword-hooking advertisement companies and program development companies that developed and managed the program through an active investigation, such as the identification of actual conditions through the performance of Internet monitoring, seizure and search of offices and servers of illegal advertisement companies, etc.

In the future, too, it is required to make continuous efforts for the activation of legal Internet advertisement market by strengthening the monitoring activities of investigation agencies, and keeping the positive control over and taking a stern legal action against the crimes of illegal advertisement like the above through the connection to portal sites.

G. Collusion between Illegal Predatory Lenders and Mobile Communications Agencies

In November 2012, the prosecutors charged 16 people based on special criminal laws on specific crimes (fraud), and are still trying to arrest one person. They were accused of defrauding the telecommunications company (KT, SKT) billions by abusing bundle product system which is selling laptop in interest-free installment for the long-term use of WiBro service customers.

The defendants, in this case, swindle money out of laptop payment by simply signing up for WiBro service regardless of credit rating through making up such as small loans. The small loan applicants recruited through advertisements in the name of WiBro service subscriptions, and then applied for a laptop with installment. The laptop to be paid to the subscriber liquidate on low-cost to in a way that 'distributor owners - the middleman - the lower recruitment agent-subscribers' share a certain percentage of its profit.
Traditionally, mobile telecommunication company considered the laptop to be paid to the actual subscriber and the payment was made to the distributor if the retail store enters the serial number of the laptop on the computer system. By using this loophole, intermediary trade, company B misused by inputting the false serial numbers to the computer system when SKT connection service opened. Company A, the laptop distributor, entered the serial number using laptops have already sold through a shopping mall. When opening, a reseller checked subscribers’ ID, laptop's model, and contents of contract, after recording the information and guidance to subscribers, and gave them Egg (WiMAX receiver) and USIM delivered by courier to pretend to be a legal sale. In addition, when the mobile carrier doubts about false subscription due to non-use of Egg, a reseller triggered traffic of Egg and delivered it to subscribers, thereby continuing to intelligently commit crimes and conceal them.

H. Illegal Selection of Government-ordered Construction through Computer Hacking

In April 2013, the prosecution arrested malicious program developer, construction broker, and constructor as well as 10 concerned people on account of computer fraud and bid interference. They illegally bid the government-supplied construction ordered by a local government by manipulating lower limit of bid through computer hacking. 25 people have been indicted to date, and one broker who fled was put on the wanted list.

Malicious program developer “A” and others bid on construction by manipulating lower limit of bid for the government-supplied construction and delivering the fair value of the bid to construction company through construction broker, using a malicious program that performs hacking an estimated construction cost.

Construction broker “B” and others distributed a malicious program which A had developed without permission to PCs of finance secretary and construction company planning to participate in bidding, and delivered the bidding price estimated by A to the participating company. Constructor “C” and others participated in bidding with the bidding price received by B and others, awarded a construction, and paid A, B and others 6-7% of the winning bid as a commission.
This case is a new type of organized intellectual fraud that program development-manager, construction broker, and constructor shared their roles and conspired to award illegal bid by developing malicious program, figuring out the lower limit of bid, searching for a construction company wanting to be selected, and delivering possible bidding price as well as paying a commission.

I. Korea-China-Japan International Smishing Fraud

In September 2013, the prosecution found 5 offenders in ‘International Smishing Crime Group’ and indicted and arrested 4 persons including “A” on account of a violation of the law regarding the promotion of information and communication network use and protection of information. They hacked text message (authentication number) from smart phone user by producing and spreading malicious application and used illegally collected text message information in swindling money from small purchase on the cellphone and purchasing game money, which is so-called ‘smishing.’ They then exchanged proceeds of crime to gift voucher and exported to China.

Public Prosecutors’ Office investigated this case based on the intelligence of crime produced at ‘Cybercrime Investigation Center’ of the Supreme Prosecutors’ Office. The offenders used borrowed-name bank account and borrowed-name email account in order to conceal their trace of crime. The prosecution revealed smishing crime for the first time, and arrested the producer of the malicious application of a new type of crime ‘Smishing’ and organization in charge of exchanging and withdrawing proceeds of crime, by tracking payment ID's IP and reverse IP, compact DB analysis, call history, and accounts analysis via high-tech investigation.

The case revealed a loophole of current system that the electronic publishing system of gift voucher is used in illegal money laundering; thus, a system reform is planned ahead.

V. CONCLUSION

In sum, the current status of the prosecution's response on cybercrime in South Korea was examined. As mentioned earlier, the Cybercrime Investigation Center of the Supreme Prosecutors’ Office and internet
investigation center of Seoul Central District Prosecutor's Office are the major investigation agencies. In order to prevent cybercrime, trying to improve professionalism by training professional investigator and operating related organizations for sharing the cybercrime information as well as strengthening international cooperation to detect cybercrime cross-nationally occurred.

The patterns of cybercrime in Korea has developed in new forms, such as farming, smishing, memory hacking, etc. beyond existing DDoS attacks and hacking. As IT develops continuously, cybercrime has been in progress each day. Previously, cybercrime was committed at an individual and personal level; now, it is becoming bolder and more organized, such as digging holes in financial systems using Internet banking to achieve financial purposes.

In the face of this situation, cybercrime is out of prevention level by one intuition or individual. Sharing information of malicious code with a national organization and private institutions and detecting in advance required comprehensive and systematic response is urgently needed. Furthermore, it required more attention by at least installing a vaccine program, upgrading new version of vaccine, avoiding high-risk site visit, paying attention to early warning sign of cybercrime.

The risk of cybercrime in the future will be even higher. However, it is hard to tell cyber security is first priority policy in spite of several warnings and real situation arising. To overcome this kind of situation, International cooperation is critical in each country through such international cooperation on cyber security policy priorities put to urge action is needed first.

What is needed is to training professional for Cyber Security is responsible for the development. The Korean Government and the prosecution have made an effort, but still not nearly enough. Therefore, in the future cyber security or cybercrime investigation stresses the experts know how to take a training addition to the domestically international needs more work. Because cybercrime will be raged, it may be appeared to the most serious international crimes in near.
RESPONSES TO CYBERCRIME BY THE KOREAN NATIONAL POLICE AGENCY

Kim, Jae-Woon*

I. INTRODUCTION
Since the first personal computer, Altair 8800, was released worldwide in 1975, the information communication technology industry has made rapid progress, and modern people depend on computer devices for most of their daily lives (e.g., home shopping, home banking, e-learning, etc.). Accordingly, the scope of work of the police charged with the mission of stability of society and maintenance of order has changed from prevention of street crimes, including robbery, burglary, and crimes of violence, to prevention and investigation of cybercrimes, including cyber hacking and monitoring of illegal sites. This paper examines the responses to cybercrime by the Korean National Police Agency by discussing the following sub-topics: development of cybercrime investigation organizations, recruitment of cyber police and educational training, national cyber terror response activities, cybercrime investigation, cybercrime prevention, and international cyber police cooperation.

II. DEVELOPMENT OF CYBERCRIME INVESTIGATION ORGANIZATIONS

A. Hacker Investigation Squad
Since the spread of personal computer supply and commercialization of the Internet in the late 1980s, information communication technology (ICT) has rapidly developed in Korea. Accordingly, cybercrime, such as hacking using information communication technology, virus dissemination, and Internet

* Official of the Korean National Police Agency seconded to the Korean Institute of Criminology
frauds, has become a serious social problem. In 1992, acknowledging the seriousness of cybercrime and the necessity of cooperative investigation with the Interpol, the Korean National Policy Agency (KNPA) appointed a lieutenant executive with expertise in computer technology as the Head of the International Criminal Affairs Division and commenced its cyber police operations.

Late in 1994, the Head of the Division successfully handled an international hacking case involving high-speed data transmission, at the request of Interpol, by conducting research and analysis of international data and utilizing cybercrime investigation technologies. Against this backdrop, the Korean National Policy Agency launched the Hacker Investigation Squad within the International Criminal Affairs Division on October 16, 1995 with the aim of responding to increasing cybercrimes. The Squad is comprised of eight officers, including one professional technology researcher and three agents who make up the Analysis and Investigation Team. The Squad resolved several cases of cybercrime, including the invasion of computer networks of Daewoo Shipbuilding and Marine Engineering, one of the world's largest shipbuilders, by a high school student hacker; the invasion of computer networks of the Japanese Ministry of Foreign Affairs; and the destruction of computer files of


2 The criminal was a second-year high school student in Busan who had learned hacking methods from one of the latest cryptography programs. The YPC program was obtained from computer security organizations of the United Kingdom and the United States in October 1995. He broke into the computer networks of corporations and universities 272 times. He also penetrated the Internet service company Inet by using a HITEL mobile phone, acquired file storing user passwords, and illegally hacked into the computer systems in 15 universities nationwide. In particular, he was able to enter the Internet network of Daewoo Dockyard located in Geoje, Gyeongnam, and he looked into various pieces of confidential information, including ship design data, without due notice by manipulating password files. The Hacker Investigation Squad of the Korean National Police Agency arrested him and found out that he was a professional hacker who had been working on computers since he was in the fourth grade of elementary school. (Donga Ilbo, January 21, 1996, "A Second-Year High School Student Hacker Breaks into 17 Networks through the Internet," p. 31.)

3 The Hacker Investigation Squad of the Korean National Police Agency arrested a 21-year-old male who identified himself as Kim. On April 18, 1996, he penetrated the networks of 34 foreign and 53 national universities and research institutes, including Nippon Telegraph and Telephone. He managed to read documents, and took out password files. The criminal, a car mechanic, felt resentment toward ludicrous statements made by Japanese politicians, and he decided to retaliate by accessing the system of the Japanese Ministry of Foreign Affairs through the network of a U.S. university and the subsystem of Nippon Telegraph and Telephone. However, the hacker put aside his plan because he worried that inserting the phrase "Dokdo is Korean Land" on the homepage of the Japanese Ministry of Foreign Affairs would
Nowcom, a Korean IT company, which caused interruption of services for six hours.4

B. Computer Crime Investigation Team

To respond to increasing computer-related crimes and hacking more effectively, the Hacker Investigation Squad was expanded and reorganized as the Computer Crime Investigation Team in August 1997. The Computer Crime Investigation Team was reassigned from Foreign Affairs Division 3 to Intelligence Crime Investigation Division, which enabled the team to take charge of all types of cybercrime, including the sale and distribution of pornography through PC communications and hacking cases.

The Computer Crime Investigation Team is equipped with a 24-hour search, analysis, and investigation system for domestic and foreign computer communication networks. This team conducts direct investigations on professional and technical cases, such as hacking and virus infringement, whereas it orders regional police agencies to conduct investigations on general cases. For the later investigations, four computer crime investigators are assigned to each regional policy agency.

In December 1999, the Computer Crime Investigation Team was renamed the Cybercrime Investigation Team. The Cybercrime Investigation Team is comprised of three groups (investigation group, crime prevention group, and international cooperation group) with 16 permanent police officers with expertise on computer knowledge and four conscripted police officers who work around the clock building a real-time prompt response system. In February 2000, the Cybercrime Investigation Team was also established in regional police agencies in every city and province.

create diplomatic problems. While hacking, he regularly checked whether the system manager monitored the system and escaped as soon as he found out that the system manager was monitoring. He also utilized a high level of techniques and completely erased any traces of hacking after penetration. (Donga Ilbo, April 19, 1996, "Breaking into 92 networks worldwide, including the Japanese Ministry of Foreign Affairs/ First Arrest of a Global Hacker in His 20s," p. 39).

4 On May 9, 1997, the Hacker Investigation Squad of the Korean National Police Agency arrested and imprisoned a male who identified himself as Kim according to a report by Nowcom after a four-month chase. He was the vice-president of an Internet Club in Busan, Gyeongnam area. He accessed the Internet network of Nowcom through a PC, stole a file which stored the passwords of 24,000 members by using the hacking program UUTX, and destroyed a portion of the operating program. He ended up suspending Internet service for six hours. (Seoul Shinmun, May 10, 1997, "A University Student Hacks into Commercial Network and Destroys Program," p. 23).
C. Cyber Terror Response Center

On July 11, 2000, the Cybercrime Investigation Team of the Korean National Police Agency was expanded and reorganized to the Cyber Terror Response Center with the goal of establishing a comprehensive response system to cope with cybercrime and cyber terror that have accompanied the increasing number of the Internet users. The Cyber Terror Response Center is directed by a senior superintendent and comprised of four teams (collaborative operations team, report and alert team, investigation team, and technique development team) with 72 members in total and 27 civilian cyber specialists who are employed through a special employment program.

This team took full charge of developing cyber investigation techniques and investigating cyber terror, such as hacking and virus dissemination into government organizations, public institutions, or major information communication infrastructures. Cybercrime Investigation Teams affiliated with each regional police agency are responsible for suggestive cases that include hacking targeted at companies, DDoS attacks, distribution of pornography, and operations of gambling sites, as well as personal information leakages. In April 2006, the Cyber Investigation Team was established in each police station to conduct investigations on civil cases that occur on a daily basis, such as Internet fraud, cyber defamation, distribution of pornography, digital copyright infringement, etc.

Currently, the Cyber Terror Response Center is comprised of the following four teams: Management and Cooperation Team, Investigation Planning Team, Investigation Team, and Digital Forensic Team. The Management and Cooperation Teams is in charge of maintaining cooperation among domestic and foreign response teams against cybercrimes, operating expert training programs, and promoting public relations. The Investigation Planning Team receives 24-hour cybercrime reports, analyzes cybercrime trends, and issues alerts when cyber terror is detected. The Investigation Team is composed of three sub-units, patrols cyberspace 24 hours, and conducts direct investigations when major cybercrimes occur (e.g. hacking and virus dissemination). The Digital Forensic Team manages the collection, analysis, and preservation of data stored in crime-related computers, laptops, or mobile phones to procure evidence.
III. RECRUITMENT OF CYBER POLICE AND EDUCATIONAL TRAINING

A. Size of Cyber Police Workforce

Currently, the organization of the police that are affiliated with the Korean National Police Agency is composed of 16 regional police agencies and 250 police stations. The Korean National Police Agency retains 60 personnel, including 49 police officers within the Cyber Terror Response Center. These police are exclusively responsible for cybercrime cases. The Cybercrime Investigation Team of the regional police agencies located in each city and province consists of 187 personnel in total, including 39 in Seoul, 28 in Kyung-gi, and 14 in Busan. In addition, 790 personnel are in charge of investigating cybercrime cases within the Cyber Investigation Team of the police stations of the cities, towns, and districts.

<table>
<thead>
<tr>
<th>Total</th>
<th>Korean Police Agency</th>
<th>Regional Police Agency</th>
<th>Police Station</th>
</tr>
</thead>
<tbody>
<tr>
<td>267 (agencies)</td>
<td>1</td>
<td>16</td>
<td>250</td>
</tr>
<tr>
<td>1,037 (persons)</td>
<td>60</td>
<td>187</td>
<td>790</td>
</tr>
</tbody>
</table>

Source: Korean National Police Agency

Table 1: Size of Cyber Police Workforce
B. Recruitment of Cyber Police

Human resources required for cybercrime investigations are procured by selecting police officers who have expertise in information communication technologies and providing them with cybercrime investigation training. However, it is also important to secure civilian experts with professional skills and techniques because police officers dealing with patrol and investigation of street crimes may have difficulty in handling cybercrimes. For this reason, since 2000, the Korean National Police Agency have been recruiting approximately 20 civilian IT specialists every year as corporal-rank police officers through a special employment examination. As investigators with professional skills and techniques, civilian specialists work in the field of high-technology, including hacking investigations, malicious code analyses, data restoration, program source analyses, and code analyses, as well as wireless communications tracking.

In addition, the Korean National Police Agency has promoted the recruitment of disabled persons out of consideration for socially disadvantaged people. Since 2007, the Korean National Police Agency has recruited one to two disabled persons through a special employment examination. From 2000 to present, 270 police officers have been recruited as experts on cybercrime through a special recruitment process.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Persons</td>
<td>27</td>
<td>48</td>
<td>20</td>
<td>19</td>
<td>19</td>
<td>21</td>
<td>26</td>
<td>15</td>
<td>18</td>
<td>17</td>
<td>18</td>
<td>21</td>
</tr>
</tbody>
</table>

Source: Korean National Police Agency

Doctoral researchers and contract professionals have also been recruited to supplement unstable human resources due to frequent changes of personnel in the Korean National Police Agency. In response to growing demands for doctoral researchers in the field of high technology, such as hacking investigations, malicious code analyses, code analyses, and digital forensics, five doctoral researchers were first employed in 2007 with continuous increase and now consisting of 17 persons in total.5

---

C. Educational Training of Cyber Police

As cybercrime includes new types of crime involving high technology, education and research should be reinforced through close cooperation with academia, research institutes, and private companies related to information communications to allow cyber police to acquire expert knowledge on high technology.

Currently, education on cybercrime investigation is provided by the Korea Police Investigation Academy in the Korean National Police Agency. The cyber professional education consists of three courses, which include cybercrime investigation, digital evidence analyses, and hacking crime investigation. These courses are provided to approximately 50 personnel per year.

<table>
<thead>
<tr>
<th>Courses</th>
<th>Duration</th>
<th>Number of Trainees</th>
<th>Number of Courses</th>
<th>Total Number of Trainees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybercrime Investigation</td>
<td>4 weeks</td>
<td>30</td>
<td>3</td>
<td>90</td>
</tr>
<tr>
<td>Digital Evidence Analyses</td>
<td>4 weeks</td>
<td>20</td>
<td>2</td>
<td>40</td>
</tr>
<tr>
<td>Hacking Crime Investigation</td>
<td>4 weeks</td>
<td>20</td>
<td>1</td>
<td>20</td>
</tr>
</tbody>
</table>

Source: Korean National Police Agency

Table 3 Korea Police Investigation Academy Cyber-related Education Courses in 2013

The lectures within the cyber professional education program are given by expert investigators on cyber investigation and digital evidence analyses, IT experts, and criminal law professors. The courses provide elite education, including law, technique, theories, and experiences, and are also provided for the personnel in the Ministry of Defense, Ministry of Information and Communication, Korea Coast Guard, and Korea Customs Service. Moreover, to enhance the IT expert knowledge of cyber investigators, domestic and foreign educational institutes provide privately commissioned education on 15 fields of high technology, including hacking, malicious code, database, data restoration, and operation systems.6

6 In 2012, a customized Department of Digital Forensic for current cyber police officers was established in partnership with the Graduate School of Information Security of Korea University. Currently, 40 cyber police officers are enrolled.
IV. NATIONAL CYBER TERROR RESPONSE ACTIVITIES

Major tools in cyber terror include hacking and distribution of malicious codes. These tools are becoming serious threats to national cyber security.

Until now, there have been two major cybercrime cases in Korea: the so-called "January 25 Internet Crisis" in 2003 and the hacking of major government agencies in 2004. In particular, the latter case involved approximately 300 systems of over 10 government agency websites that were hacked by a global hacker, which caused harm of the largest scale at the national level. The Cyber Terror Response Center of the Korean National Police Agency was the first to recognize this hacking case and prevented the leak of state secrets in advance. The Center notified the National Intelligence Service to prepare ex post facto security measures.

In 2003, the Korean National Police Agency arrested a Brazilian hacker after six months of cooperation with the Japanese National Police Agency. The arrested hacker had hacked 1,038 websites worldwide, including 58 in Korea, and had made the initial screen page containing messages against the war in Iraq. In 2008, a Chinese hacker who had obtained personal information of over 10 million members of Auction, one of the largest e-commerce websites in Korea, was arrested through rapid international mutual assistance.

7 On a Saturday afternoon on January 25, 2003, the majority of Internet networks in Korea were disrupted for three hours. This crime started when the Slammer Worm virus (Worm.SQL.Slammer) penetrated the Microsoft SQL server without security patch; the Slammer Worm-infected PCs produced massive data, which increased the Internet traffic of the DNS server at the KT Hyehwa Telecommunications Office. When the KT Hyehwa Telecommunications Office became paralyzed, the Internet traffic nationwide took a detour to another backbone network and other DNS servers, which also became paralyzed in turn. This virus infected approximately 8,800 servers in Korea; netizens were unable to use Internet services, such as shopping, banking, and flight reservations. (Donga Ilbo, Jan. 27, 2003, "1․25 Internet Crisis/ IT Korea Collapsed by 35-Min Virus Attack," p. 3).

8 In 2004, a global hacker broke into 10 computer networks of government and public organizations, as well as private companies (i.e. the National Assembly of the Republic of Korea, Korean Institute for Defense Analysis, Agency for Defense Development, Air University, Korean Atomic Energy Research Institute, and Korea Coast Guard). He used malicious variant programs, types of Trojan Horse programs called the variant Peep and the variant Revace, and hacked approximately 300 computers. The hacker made the hacking program penetrate computers and steal data when users opened their e-mails or attached files on the bulletin board. The National Intelligence Service announced that this hacking case was a crime that involved a large-scale criminal organization that threatened not only private parties, but also national security. (Donga Ilbo, July 14, 2004, "10 Organizations Hacked, a Serious Menace to National Security," p. 1).
In 2009, the so-called "July 7 DDoS Cyber Terror" paralyzed the websites of major government agencies, including the Blue House and the Ministry of Defense, by infecting thousands of personal computers with malicious codes, turning them into "zombie computers," and increasing the traffic (number of access) of the websites. The Cyber Terror Response Center played the most important role in identifying the cause of this attack by conducting an extensive investigation on approximately 60 domestic and international servers and zombie PCs for six months. The Center concluded that the source of the attack was the IP of the North Korean Communications Office. A similar cyber attack called the "March 4 DDoS Cyber Terror" occurred in 2011. The Cyber Terror Response Center of the Korean National Police Agency conducted joint investigations with foreign national police agencies from 40 countries and confirmed that the program used for the attack was identified as the same one used for the July 7 attack, concluding that North Korea was also the source of the March 4 DDoS Cyber Terror.

V. CYBERCRIME INVESTIGATION

A. Receipt of Cybercrime Report and Counseling

Victims of cybercrime can file a damage report by logging onto the homepage of the Cyber Terror Response Center of the Korean National Police Agency (www.netan.go.kr). Registered cases are processed at the headquarters of the police station according to type of case by the same means as the investigation procedure of ordinary cases. In the past, the majority of cases involved game fraud and account hacking, whereas the number of civil complaints of e-commerce fraud and cyber violence has increased.

9 This DDoS attack occurred from July 7-9, 2009, when the hacker targeted 435 servers of 61 countries and attacked 35 major Korean-American websites, including national government organizations, parties, portal sites, the press, financial institutions, vaccine businesses, and homepages operated by the American government. The attack was suspended when the zombie PC used for the attack was destroyed at midnight on July 10. The Korean National Police Agency conducted an investigation on the servers that passed through Korea and foreign countries and found out that the hacking attack source was the North Korean Regional Communications Office. (Internal document of the Korean National Police Agency).

10 This cyber terror was a crime that DDoS-attacked 40 national main sites, including Blue House and the National Assembly, by using 746 servers of 70 countries from March 3-5, 2011. Based on the homogeneity of the DDoS attack system and the designing method of the malicious code, as well as the foreign attack order server, the Korean National Police Agency specified that the attack source was North Korea. (Internal document of Korean National Police Agency).
increased. In addition, professional consultants with extensive knowledge in IT technology and law are arranged around the clock at the Cybercrime Report-Call Center (+82-2-393-9112) by the Cyber Terror Response Center of the Korean National Police Agency. These professionals provide emergency reports and counseling services.

B. Analysis by Types of Cybercrime

(1) Hacking and Malicious Code

Crime using hacking or malignant code has been increasing since the dissemination of the Internet. In the beginning, these crimes were committed by computer-related professional technicians, whereas today, anyone who desires can commit such crime by procuring hacking tools or malicious programs through the Internet. In addition, the degree of cybercrime is becoming more serious and has evolved from ostentation of one's hacking skills or simple curiosity to illegal acquisition of others' personal information from websites, abuse of obtained information for telemarketing, or hacking of government agency websites.

In particular, in 2011, a secretary to a member of the National Assembly was arrested for launching a DDoS attack on the homepage of the Korean National Election Commission with a zombie PC to make voters unable to find voting stations. This crime had dramatic implications for society and led to serious political conflict.

(2) Invasion of Personal Information

Currently, people are concerned about the protection of their personal information due to recent personal information leakage cases. Damage caused by such information leakage (e.g., using personal information of a particular person, procured by phishing or pharming, accessing other

11 On October 26, 2011, when the Mayor of Seoul by-election was held, the homepage of a candidate, Park Won-Soon, was paralyzed for about two hours. The Korean National Police Agency investigated and arrested a secretary of the member of the National Assembly of the ruling party, who identified himself as Kong, and two accomplices. They attacked the homepage of the National Election Commission by bringing a heavy increase in connections number in a moment by using approximately 200 zombie PCs from six a.m. on the 26th, the day of election; therefore, they paralyzed the site for two hours and 17 minutes beginning at 6:15 a.m. (Donga Ilbo, Dec. 3, 2011, "10-26 DDoS Attack on the Homepage of the National Election Commission and that of Park Won-Soon, the Criminal Turned Out to be the Secretary of the Member of the National Assembly, Choi Koo-Shik," p. 1.).
people's accounts, stealing secret contents or game items, or sending spam messages for profit-making purposes) is becoming more severe.

The Korean National Police Agency investigated the private information leakage of 35 million SK Communications (owner of popular Korean portals Nate and Cyworld) members in 2011. The investigation revealed that the server of a popular Korean public program distribution company was hacked, and files were modified, infecting 62 PCs of SK Communications and leaking out massive amounts of personal information to China. This case demonstrated the scope of danger that can be caused by malicious codes and the importance of detecting and blocking zombie PCs.

(3) Internet Fraud (Small-sum Fraud in Cyberspace)

According to the analysis of the National Statistical Office, the volume of cyber shopping and transactions has increased by 19.2% since last year and has become a 34 trillion KRW market with continued growth of online shopping, "open markets," and direct transactions. Also, Internet fraud using advance payment and deferred delivery methods of e-commerce are increasing sharply. The majority of criminals use more and more intelligent and sly methods, such as illegal use of others' banking accounts or mobile phones. Furthermore, the police now monitor fraud cases because of the recent increase in small-sum settlement fraud using game accounts.

(4) Illegal Sites for Pornography and Gambling

Although the number of pornography sites are decreasing, it is presumed that pornography is now distributed through file sharing sites that are accessible to everyone, irrespective of age or gender. The police punished a file-sharing site for the first time in Korea on account of illegal possession of child pornography. In addition, the police are cracking down on illegal gambling sites, including cyber gambling, private horse racing, and private Sportstoto using the Internet and smartphones.

12 An unidentified hacker penetrated the Internal network through the computer of a SK Communications employee from July 26-27, 2011. The hacker then released the 34 million cases of membership information through the database server of Nate and Cyworld operated by SK Communications. The Korean National Police Agency identified that the attack was committed by an IP assigned to China. (Internal document of the Korean National Police Agency).

13 See www.hikostat.kr/2068
C. Capacity Building for Digital Evidence Analysis

(1) Digital Evidence Analysis Bodies

As digital media become an important tool in investigations, the Korean National Police Agency created the Digital Evidence Analysis Center in 2004 and built a nationwide investigation support system by establishing a Digital Evidence Analysis Team at regional police agencies in May 2006. With the establishment of the organization and arrangement of human resource, the number of digital evidence analyses has steadily increased.

With the introduction of the court hearing-based trial and jury trial, when it comes to judging the admissibility of evidence, not only the results of the analysis, but also the professionalism of the analyst (e.g. his or her degree or certificate) are controversial issues. Therefore, professional education programs to acquire the "International Certificate of Digital Forensic" were initiated for evidence analysts of the Korean National Police Agency, regional police agencies, and 50 cyber investigators.

D. Establishment of Digital Evidence Physical Restoration Bureau

Lately, there has been a tendency that the suspect willfully damages digital media, such as a hard disk or USB, to destroy evidence. Therefore, the clean room-like Digital Evidence Physical Restoration Bureau was established to restore damaged media acquired by the Korean National Police Agency and the majority of regional police agencies. This bureau enabled the national Cyber Police to receive site support and respond to the changing judicial environment (i.e. court hearing-based trial).

E. Supply of Digital Forensic Equipment

The field digital evidence collection tool was developed and distributed to the cyber investigators nationwide to enable those without computer expertise to collect digital evidence stored in a PC. Other equipment, such as removable hard disks, were supplied for storing and securing collected evidence. Furthermore, as cyber terror is becoming a realistic threat to national security and public order, and attacking techniques are becoming increasingly intelligent and sophisticated, equipment for zombie PC detection and reproduction, as well as malignant code analyses were supplied to enhance DDoS investigation capacity building at the regional police agencies.
VI. FUTURE REGIONAL DIRECTIONS

With the Asian region taking account for the world’s most populated land masses, diverse languages and well defined national identities, there is always going to be major functional differences within jurisdictions. This is underpinned by a variety of philosophies and religions, Indigenous, colonised and mixed populations and legal support or restrictions placed on human rights and democratic processes. Most importantly for ordinary people wishing to own their crime, for those want to make things rights and for those wanting to share their story of their fear and harm, many regional governments and services are beginning to listen. The future does hold hope for restorative encounters and free-flowing conversations facilitated between harm doers and those most harmed, in a willingness to ensure that harmony prevails. The how, where and when we can all see restorative justice providing the region’s people with a safer way to live without fear of crime, is with us now. We are all empowered to take control of crime, work towards healing its impact and restoring good relationships. This should always lead to a greater understanding, compassion and fairness among families and communities. Restorative justice can come into its own once freed from the all-encompassing criminal justice systems, as it deals with the most crucial relationships between the victim of crime and the perpetrator.
THE COUNCIL OF EUROPE CONVENTION
ON CYBERCRIME:
ITS MAJOR SHORTCOMINGS AND THE ROAD AHEAD

Lee, Angela Changjin*

I. INTRODUCTION

Information communications technology (ICT) has developed at an incredible speed over the past several decades. Computers now affect almost every aspect of our daily lives, from emails and online banking, to medical treatment and public security. The Internet allows us to communicate with others, anytime and anywhere as well as to gain access to a wealth of information and resources that can be used for both personal and professional purposes. At the same time, however, expansion of Internet use has generated new kinds of crimes, additional means to commit existing crimes, and increased complexities of prosecuting crimes.1

Cybercrime has significantly profound consequences, reaching much farther than traditional methods of crime because cybercrime is not restricted by physical borders, thereby affecting all individuals and all countries worldwide with great political, social and economic implications. There is no universally agreed definition of what constitutes cybercrime2 but there is broad acceptance that cybercrime involves traditional crimes committed in a new environment using new methods as well as new crimes made possible in the new environment.3

* Researcher, International Center for Criminal Justice, Korean Institute of Criminology

2 See Ian Walden, Computer Crimes and Digital Investigations, (New York: Oxford University Press, 2007) 19 (introducing the debate on defining what constitutes cybercrime, quoting David Wall’s phrase of ‘new wine, no bottles’ to describe not only cyberspace but also the new types of criminal behavior he saw emerging, and Peter Grabosky’s ‘old wine in new bottles’ to suggest that crimes were fundamentally similar.)
3 Id.
Considering the borderless nature of cybercrime, combined with the rapid development of globalization, a very high proportion of cybercrime now involves an international element, especially so when compared with more traditional crimes. The international element arises not only in terms of determining which country has jurisdiction over cybercrime for the purpose of criminal prosecution which would require establishing whether a certain conduct constitutes an offence, but also in respect of obtaining evidence in the forensic investigation of cybercrime. Scholars and policymakers around the world have been concerned with improving the scope, speed and efficiency of international cooperation in criminal procedures, in recognition that cybercrime can only be solved on a global level, which would be impossible if the law did not reflect the fast moving environment in which cybercrime operates.

In this regard, governments have recognized the need to ensure that international standards are developed for the harmonization of national legal frameworks. Various attempts have been made by several international organizations and regional institutions, such as the European Union (EU), the Group of Eight (G8) and the Association of Southeast Asian Nations (ASEAN), to achieve a harmonized approach against cybercrime, the most significant outcome of which has been the Council of Europe Convention on Cybercrime (hereinafter, the Convention on Cybercrime or the Budapest Convention). Opened for signature in Budapest in November 2001 and entering into force in July 2004, the Convention on Cybercrime is considered the most important international instrument to combat cybercrime.

However, ten years since the Convention on Cybercrime came into force, the international community still faces many challenges in reaching a global consensus on ways to address cybercrime. Compared to the speed at which cybercrime has evolves, international law, criminal justice systems and the level of international cooperation have lagged behind, rendering various concerted efforts on regional and international levels far less effective. One

5 Supra note 2, 351.
of the main reasons is that the magnitude and the complexity of the problem of cybercrime becomes evidently intense when it is elevated from a national to an international level, particularly when countries with less developed cybercrime legislations are involved for whom fighting cybercrime is not one of the highest national priorities. As such, harmonization of national legislations and existing international legal instruments has been and remains difficult, despite the Convention on Cybercrime being in force.

Section II of this article will provide a brief overview of various international legal instruments that have been developed to combat cybercrime, including the Budapest Convention. Sections III and IV will review detailed provisions of the Convention, discussing both the positive features and the shortcomings of the Convention.

II. INTERNATIONAL LEGAL INSTRUMENTS ON CYBERCRIME

Over the past few decades, there have been various efforts by a number of international and regional organizations to develop legal solutions for cybercrime. The United Nations Office on Drugs and Crime (UNODC) drafted the Comprehensive Study on Cybercrime in 2013, which identifies five possible 'clusters' of instruments: (i) instruments developed in the context of, or inspired by, the Council of Europe or the European Union; (ii) instruments developed in the context of the Commonwealth of Independent States or the Shanghai Cooperation Organization; (iii) instruments developed in the African context; (iv) instruments developed by the League of Arab States, and (v) instruments developed under the auspices of, or associated with, United Nations entities. These clusters are not absolute and one group of instruments have had involvement in the development of other group of instruments, but based on their legal status, they may be categorized as the following.

9 Id.
<table>
<thead>
<tr>
<th>Binding</th>
<th>Non-binding</th>
</tr>
</thead>
<tbody>
<tr>
<td>· Council of Europe Convention on Protection of Children against</td>
<td></td>
</tr>
<tr>
<td>Sexual Exploitation and Sexual Abuse (2007)</td>
<td></td>
</tr>
<tr>
<td>· EU legislation including on e-Commerce, on Combating Fraud</td>
<td></td>
</tr>
<tr>
<td>and Counterfeiting of Non-Cash Means of Payment, on Personal Data</td>
<td></td>
</tr>
<tr>
<td>(as amended), on Attacks against Information Systems, and on Child</td>
<td></td>
</tr>
<tr>
<td>Pornography</td>
<td></td>
</tr>
<tr>
<td>· Commonwealth of Independent States (CIS) Agreement on Cooperation</td>
<td></td>
</tr>
<tr>
<td>in Combating Computer Information-related Offences (2001)</td>
<td></td>
</tr>
<tr>
<td>· Shanghai Cooperation Organization Agreement on Cooperation in the</td>
<td></td>
</tr>
<tr>
<td>Field of International Information Security (2009)</td>
<td></td>
</tr>
<tr>
<td>· (Draft) Economic Community of West African States (ECOWAS) Directive</td>
<td></td>
</tr>
<tr>
<td>on Fighting Cybercrime (2009)</td>
<td></td>
</tr>
<tr>
<td>· (Draft) African Union Convention on the Establishment of a Legal</td>
<td></td>
</tr>
<tr>
<td>Framework Conducive to Cybersecurity in Africa (2012)</td>
<td></td>
</tr>
<tr>
<td>· League of Arab States Convention on Combating Information Technology</td>
<td></td>
</tr>
<tr>
<td>Offences (2010)</td>
<td></td>
</tr>
<tr>
<td>· Optional Protocol to the United Nations Convention on the Rights of</td>
<td></td>
</tr>
<tr>
<td>the Child on the Sale of Children, Child Prostitution and Child</td>
<td></td>
</tr>
<tr>
<td>Pornography (2000)</td>
<td></td>
</tr>
<tr>
<td>· International Telecommunication Union (ITU)/Caribbean Community</td>
<td></td>
</tr>
<tr>
<td>(CARICOM)/Caribbean Telecommunications Union (CTU) Model Legislative</td>
<td></td>
</tr>
<tr>
<td>· International Telecommunication Union (ITU)/Secretariat of the</td>
<td></td>
</tr>
<tr>
<td>Pacific Community Model Law on Cybercrime (2011)</td>
<td></td>
</tr>
</tbody>
</table>

*Source: UNODC, Comprehensive Study on Cybercrime*

| Table 1 | Binding and Non-binding Instruments on Cybercrime |
As of 2013, 82 countries have signed and/or ratified one of following four legally binding cybercrime instruments: Council of Europe Convention on Cybercrime, League of Arab States Convention, Commonwealth of Independent States Agreement, and Shanghai Cooperation Organization Agreement. However, not a single one of these instruments have been signed or ratified with global geographic reach nor with equal geographical representation.

Of all the international or regional instruments, none of them seeks to create a global law enforcement agency to handle cybercrime on an international level. The assumption is that cybercrime is best handled by individual countries in cooperation with and with the assistance of other countries, all of which have adopted laws that allow them to investigate cybercrime and to apprehend and prosecute criminals. The underlying assumption is that the best approach to combating cybercrime is the approach we currently use for general crime.

In this regard, the Council of Europe Convention on Cybercrime may appear to be the most promising tool in combating cybercrime, given that

---

10 Id., 67.
among some of the major legally binding instruments on cybercrime, it is the most used multilateral instrument for the development of a global cybercrime legislation and, as its proponents argue, it is the most substantive and broadly subscribed treaty on cybercrime in existence. The following text will provide an overview of the history and the organization of the Convention on Cybercrime, followed by an analysis of its shortcomings.

III. THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME

A. Historical Background

Over the past few decades, there have been various efforts by several international and regional organizations to develop legal solutions for cybercrime, beginning in Europe. The Organization for Economic Cooperation and Development (OECD) issued a report in 1986, an outcome of a two-year study on the legal issues posed by cybercrime, which surveyed existing cybercrime laws and recommended a set of offences that should be criminalized in all countries in order to combat transnational cybercrime.12 A similar approach was taken by the Council of Europe in 1989 when it initiated its own study and published a set of recommendations addressing the need to establish new substantive laws criminalizing crime committed via computer networks.13 A second study followed in 1995, going beyond the identification of substantive offence categories and addressing the inadequacy of criminal procedural law. It explored various criminal law procedural issues, including search and seizure, technical surveillance, obligation to cooperate with investigating authorities, electronic evidence, use of encryption and international cooperation, emphasizing the need to minimize intrusion of privacy in criminal procedures.14 Building on these two reports, the Council of Europe appointed the Committee of Experts on Crime in Cyberspace (“PC-CY”) in 1997 to draft a binding convention upon identifying new

14 Supra note 7, 334. For the full report, see Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology (1995).
crimes, jurisdictional rights and criminal liabilities related to Internet communications, the final report of which became the master blueprint for the Council of Europe Convention on Cybercrime.15

Preceded by over twelve years of preparatory work, the Council of Europe Convention on Cybercrime became the first international treaty aimed at providing an effective legal framework for combating cybercrime. It opened for signature in Budapest, Hungary, in November 2001 and entered into force on July 1, 2004. Since then, it has been signed by 49 states and ratified by 40 states (as of October 2013), four of which are non-Member States of the Council of Europe, respectively.16 As set out in the Preamble, the main objective of the Convention is to “pursue […] a common criminal policy aimed at the protection of society against cybercrime […] especially by adopting appropriate legislation and fostering international cooperation.”17

B. Structure of the Convention

First international treaty on crimes committed via the Internet and other computer networks, the Convention on Cybercrime aims principally at harmonizing cybercriminal offences qualification, providing for laws empowering law enforcement and setting up an effective regime of international cooperation.18 The Convention consists of 48 articles, divided among four chapters: (1) “User of terms”; (2) Measures to be taken at the national level”; (3) “International cooperation”; and (4) “Final provisions.” Apart from Chapter I, the Convention has three principal parts.

Chapter 2 addresses the substantive cybercrime offences required of ratifying states to adopt in their national laws, drawing a distinction among offences against the confidentiality, integrity and availability of computer data systems19, computer-related offences20, content-related offences21, and

---

15 Id.
16 For the full list, see http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (last visited October 28, 2013).
offences related to infringements of copyright and related rights. Chapter 3 deals with the investigative procedures the states are required to implement, and Chapter 4 concerns the mechanisms to promote international cooperation in combating cybercrime.

Chapter 2, Section 1 of the Convention requires ratifying States to "adopt legislative and other measures [...] to establish as criminal offences under its domestic law, when committed intentionally and without right" nine offences defined as the following grouped into four categories:

19 Offences against the confidentiality, integrity and availability of computer data systems include illegal access, illegal interception, data interference and misuse of devices.
20 Computer-related offences include computer-related forgery and fraud.
21 Content-related offences include child pornography.
22 Supra note 18, 166.
23 Supra note 17, Chapter 2, Section 1
The Council of Europe Convention on Cybercrime

Computer-related offences

- Computer-related forgery: Input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible
- Computer-related fraud: Causing of a loss of property to another person by (i) any input, alteration, deletion or suppression of computer data, or (ii) any interference with the functioning of a computer system with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person

Content-related offences

- Offences related to child pornography: (i) producing child pornography for the purpose of its distribution through a computer system; (ii) offering or making available child pornography through a computer system; (iii) distributing or transmitting child pornography through a computer system; (iv) procuring child pornography through a computer system for oneself or for another person; (v) possessing child pornography in a computer system or on a computer-data storage medium

Offences related to infringements of copyright and related rights

- Offences related to infringements of copyright and related rights: Infringement of copyright, as defined under the law of [the ratifying] Party

Chapter 2, Section 2 of the Convention addresses a broader range of offences than those defined in Section 1 outlined above, including any criminal offence committed by means of a computer system or the collection of evidence in electronic form.24 As a threshold matter, it provides for the common conditions and safeguards applicable to all procedural powers in the chapter, which include expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, and interception of content data.25 Traditional application of search and seizure is provided for within the competent authorities of each ratifying

24 Id. Article 14 (Scope of procedural provision)
25 Supra note 7, 337.
state for stored computer data as well as other procedural options such as real-time collection of traffic data and interception of content data. Chapter 2 ends in Article 22 which loosely provides a set of rules by which states can establish jurisdiction over any offence established in the Convention.

Chapter 3 establishes a framework on international cooperation and mutual legal assistance for the investigation and prosecution of cybercrime, providing principles relating to extradition, procedures regarding mutual legal assistance requests in the absence of applicable international agreements, mutual legal assistance regarding investigative powers and a 24/7 network. As will be address in further detail in the following sections, the Convention explicitly rejects dual criminality as a prerequisite for mutual assistance for expedited preservation of stored computer data, although the Convention does grant states the right to refuse mutual assistance request for preservation of stored data in the case where the state “has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.” Chapter 4 includes all other miscellaneous provisions including signature and entry into force, territorial application, and amendments.

IV. MAJOR SHORTCOMINGS OF THE CONVENTION

The Council of Europe Convention on Cybercrime, coming into effect in July 2004, offered the prospect of establishing an international treaty for the investigation and prosecution of cybercrime. It has been considered by and large a sound model for international cooperation and harmonization of domestic legislations. It has also been drawn on by many non-ratifying states in the framing of their own national laws, one example being Thailand.

In 2012, Alexander Seger summarized key achievements of the Budapest Convention since its adoption in November 2001 as follows:

26 Id.
27 Supra note 17, Chapter 3, Section 2, Article 29
 Reinforcement of legislative reform worldwide: The Convention on Cybercrime has served as a guideline to most countries, at least 120 of which are undertaking legislative reforms.

 Reach beyond Europe: Of the 55 countries that had ratified or signed the Convention or had been invited to accede, 14 states were non-European countries. The Council of Europe also engaged with at least 55 other states in technical cooperation on the basis of the Convention.

 Increase in police-to-police and judicial cooperation: All ratifying states of the Convention now have functioning 24/7 contact points in line with Article 35 of the Convention. The considerable cooperation among law enforcement and judicial agencies is attributed to the ratification of the Convention by the United States in 2006.

 Increase in multi-stakeholder cooperation for Internet governance: There has been a particular increase in public-private cooperation. Practical outcome of such cooperation includes the establishment of the guidelines on law enforcement-service provider cooperation in the investigation of cybercrime of 2008.

 Given such an assessment of its achievements, however, the Convention on Cybercrime has been controversial less for what it does or has done than for what it does not do or has not done. 30

  A. Definitions

 As discussed earlier, Chapter 1 of the Convention identifies key definitions, including *computer system*, *computer data* and *service provider*, which are vital to interpreting the provisions under the Convention. It was agreed by the drafters of the Convention that parties need not incorporate verbatim the particular definitions as provided under the Convention, provided that such concepts are covered by each party’s domestic laws in a manner “consistent with the principles of the convention and [that each party] offer an

The key definitions provided under the Convention are as follows:

- **Computer system:** Any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data
- **Computer data:** Any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function
- **Service provider:** (i) Any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service
- **Traffic data:** Any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service

Proponents of the Convention argue that the technology-neutral language used in the Convention keeps it still most relevant after ten years since its adoption. Provided that the language used should not be so narrow as to disable the Convention’s adaptability to various technological changes and that statutory definitions are an obvious disadvantage as rapid technological developments may render such politically negotiated definitions unsuitable, concerns still remain as to whether these definitions are not too broad. The Convention’s definition of a *service provider*, for instance, is a very broad category of persons and/or entities that provide users with services for communication by means of a computer system. According to the Council of Europe Convention on Cybercrime Explanatory Report, the term *service provider* includes both public and private entities that provide the ability to communicate with one another, which means it could possibly include any Internet user who maintains a website, thus potentially

32 Supra note 17, Article 1
33 Supra note 31, ¶ 30.
imposing huge cost and labor burden on a large group of Internet users.\(^\text{34}\) Furthermore, it is unclear whether the definition of *traffic data* includes hyperlinks and http requests, in which case the definition may be far more invasive than the drafters of the Convention had intended.\(^\text{35}\) Also, it is unclear whether the term *communication* used in the definition of *traffic data* includes surfing the Internet – e.g., reading e-mails on a web mail provider by connecting through an ISP – which is traditionally considered both a communication and a transaction.\(^\text{36}\)

**B. Jurisdiction, Extradition and Mutual Assistance**

Article 22 of the Convention on Cybercrime requires parties to establish criminal jurisdiction over those offences defined in the Convention when committed “in its territory,”\(^\text{37}\) grounded upon the principle of territoriality. The Convention also provides that each party establish jurisdictional principles for offences committed by one of the party’s nationals, if the offence is punishable under criminal law where it is committed, or if the offence is committed outside the territorial jurisdiction of any state.\(^\text{38}\) Accordingly, if a national were to commit an offence abroad, the party of which the criminal is a national must be able to prosecute the criminal, even if the conduct is also an offence under the law of the country in which it was committed. However, the Convention does not resolve the extraterritorial jurisdictional issue because it ultimately fails to establish a common set of crimes, while it is further hampered by the lack of universal participation.

Moreover, the Convention does not resolve the major jurisdictional dilemma where more than one country has a “jurisdictional claim” to a case.\(^\text{39}\) Regarding Article 22 (5), the Council of Europe Explanatory Report explains:\(^\text{40}\)


\(^{35}\) *Id.* *citing* David Banisar and Gus Hosein, “A Commentary on the Council of Europe Cybercrime Convention” (2000).

\(^{36}\) *Id.*

\(^{37}\) *Supra* note 17, Article 22.1.a.

\(^{38}\) *Id.* Article 22.1.d.

\(^{39}\) *Supra* note 7, 347.

\(^{40}\) Article 22(5): When more than one Party claims jurisdiction over an alleged offence established
In the case of crimes committed by use of computer systems, there will be occasions in which more than one Party has jurisdiction over some or all of the participants in the crime. For example, many virus attacks, frauds and copyright violations committed through use of the Internet target victims located in many States. In order to avoid duplication of effort, unnecessary inconvenience for witnesses, or competition among law enforcement officials of the States concerned, or to otherwise facilitate the efficiency or fairness of the proceedings, the affected Parties are to consult in order to determine the proper venue for prosecution. In some cases, it will be most effective for the States concerned to choose a single venue for prosecution; in others, it may be best for one State to prosecute some participants, while one or more other States pursue others. Either result is permitted under this paragraph. Finally, the obligation to consult is not absolute, but is to take place "where appropriate." Thus, for example, if one of the Parties knows that consultation is not necessary (e.g., it has received confirmation that the other Party is not planning to take action), or if a Party is of the view that consultation may impair its investigation or proceeding, it may delay or decline consultation.\(^{41}\)

Given that jurisdictional matters involving the investigation and prosecution of cybercrime must be accompanied by international cooperation and mutual support, the Convention provides in Chapter 3 various means of cooperation, including extradition and mutual assistance, requiring parties to cooperate “to the widest extent possible.”\(^{42}\) According to the CoE Explanatory Report, the drafters of the Convention rejected the creation of a separate regime of mutual assistance that would be applied in lieu of other applicable pre-existing mutual legal assistance treaties (MLATs) and other instruments already in effect, agreeing that it would be more practical in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

\(^{41}\) Supra note 31, ¶ 239.

\(^{42}\) Convention on Cybercrime, Article 23: The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
to rely on those pre-existing instruments so as to avoid any confusion that may arise from the establishment of new, competing regimes.\footnote{Supra note 31, ¶ 262.} Accordingly, parties to the Convention that already have bilateral MLATs or other multilateral instruments governing mutual assistance in criminal cases are required to apply the terms thereof, given that computer- or computer-related crime-specific mechanisms provided in Chapter 3 of the Convention are supplemented, unless the relevant parties agree to apply any or all of the provisions in Article 24 (Extradition) of the Convention in lieu thereof.\footnote{Supra note 31, ¶ 263.}

The operative provisions of MLATs, however, often have the effect, whether intended or not, of limiting international enforcement efforts, as many such agreements require “dual criminality” — \textit{i.e.}, that the crime for which information is being sought by a requesting country also constitute a criminal offence in the country being requested to provide such information.\footnote{Convention on Cybercrime, Article 29(4): A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.; Supra note 7, 349.} Fortunately, the Convention on Cybercrime explicitly rejects dual criminality as a prerequisite for mutual assistance regarding the expedited preservation of stored computer data, an innovation widely lauded for allowing flexibility in mutual assistance among countries.\footnote{Convention on Cybercrime, Article 29(3): Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.} However, Article 29(4) of the Convention contains an electable reservation, allowing room for the toleration of dual criminality requirement.\footnote{Supra note 13, 434.} Furthermore, in the absence of an agreement on what elements constitute a certain criminal conduct, criminals may evade punishment, for no country has the right to interfere with the privacy of another country’s national to investigate a crime, an element of which is not required to constitute a criminal conduct in another country. The problem of reservations, mitigating the effect of controversial provisions will also be discussed in the following section. Finally, Article 24 (Extradition) of the Convention does not provide any
mechanism to implement or expedite extradition when a request is made by a party, rather providing that “extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the Party may refuse extradition.”

C. Reservations

Throughout the Convention, parties are allowed to selectively elect reservations from certain provisions. The Council of Europe Explanatory Report explains that such “reservation possibilities aim at enabling the largest number of States to become Parties to the Convention, while permitting such States to maintain certain approaches and concepts consistent with their domestic law.” Reservations, however, act as loopholes for states whereby they may become a member of the Convention while reserving what may be some of the most important parts of it, rendering the treaty fundamentally insufficient to harmonize cybercrime laws among its prospective members. The United States, for instance, signed the Convention subject to several reservations. The Explanatory Report also states that the drafters of the Convention

48 Convention on Cybercrime, Article 24; Supra note 7, 347.
49 See, for instance, Article 9 (Offences related to child pornography) which requires parties to establish as criminal offences under their domestic laws the conduct of (a) producing child pornography for the purpose of its distribution through a computer system; (b) offering or making available child pornography through a computer system; (c) distributing or transmitting child pornography through a computer system; (d) procuring child pornography through a computer system for oneself or for another person; or (e) possessing child pornography in a computer system or on a computer-data storage medium, but allows them to reserve from applying (d) and (e). Similarly, the term child pornography is defined as pornographic materials that visibly depicts (a) a minor engaged in sexually explicit conduct; (b) a person appearing to be a minor engaged in sexually explicit conduct; or (c) realistic images representing a minor engaged in sexually explicit conduct, but parties may choose not to apply (b) and (c) to their domestic laws. Article 22 (Jurisdiction) requires parties to establish jurisdiction over any offence established under the Convention when committed (a) in its territory; (b) on board a ship flying the flag of that party; (c) on board an aircraft registered under the laws of that party; or (d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State, but parties are given the right not to apply subparagraphs (b), (c) and (d).
50 Supra note 31, ¶ 320.
51 Supra note 7, 353 (referring to Letter Of Submittal To President Bush From Secretary Of State Colin Powell, United States Department of State, reprinted in Convention on Cybercrime, 108th Congress, 1st Session, Treaty Doc.108-11 (2003) at vi, noting that reservations allow for variations between the Convention and domestic laws allowing parties to “modify or derogate from specified Convention obligations.”)
“endeavored to restrict the possibilities for making reservations in order to secure to the largest possible extent the uniform application of the Convention by the parties. Thus, no other reservations may be made than those enumerated.”52 The available reservations, however, “highlight the areas of disagreement between the parties” and “emphasize, by their absence, areas of consensus.”53

Furthermore, given the many provisions that parties are permitted to reserve, the overall effectiveness of the Convention may be affected. In the course of initiating and conducting extraterritorial investigations on certain cases, both requesting and requested states will need to determine which specific reservations have been made by their counterpart in order to decide the level of assistance that may be provided and obtained.

**D. Concerns regarding Personal Privacy and Civil Liberties**

Advocates for personal privacy and civil liberties have noted their concern for the imbalance between law enforcement powers and protection of personal privacy. The Convention requires parties to establish the powers and procedures at the national level for law enforcement authorities to conduct certain types of criminal investigations or proceedings specific to cybercrime offences. Such procedural powers include preservation of stored data,54 expedited preservation and partial disclosure of traffic data,55 production orders,56 search and seizure of computer data,57 real-time collection of traffic data,58 and interception of content data.59

52 Id.
53 supra note 13, 440.
54 Convention on Cybercrime, Article 16 (Expedited preservation of stored computer data) Parties are obliged to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
55 Convention on Cybercrime, Article 17 (Expedited preservation and partial disclosure of traffic data) Parties are obliged to ensure that expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication.
56 Convention on Cybercrime, Article 18 (Production orders) An appropriate legal basis is established for the release of stored computer data or traffic data from third parties to competent authorities of parties to the Convention.
57 Convention on Cybercrime, Article 19 (Search and seizure of stored computer data) Parties are obliged to enable competent authorities to search or similarly secure stored computer data.
58 Convention on Cybercrime, Article 20 (Real-time collection of traffic data) Parties are obliged to empower competent authorities to collect or record, or compel a service provider to collect or record, traffic data to the extent that such activity is within their technical capabilities.
Given that such powers and procedures are subject to the conditions and safeguards provided under Article 15\textsuperscript{60} of the Convention, it has been criticized for not addressing the issue of privacy protection beyond this general statement. Consider the perspective offered by one of such advocacy groups, the Center for Democracy and Technology:

The treaty is fundamentally imbalanced: it includes very detailed and sweeping powers of computer search and seizure and government surveillance of voice, email and data communications, but no correspondingly detailed standards to protect privacy and limit government use of such powers, despite the fact that privacy is the #1 concern of Internet users worldwide who see an increase, not a decrease, in the surveillance capabilities of governments brought on by the digital revolution.

While the treaty’s express terms do not require companies to modify their equipment or business practices, the treaty must be viewed as part of the ongoing government efforts nationally and internationally to require telephone companies, Internet service providers, website operators and computer hardware and software manufacturers to design their systems, their record-keeping procedures and their very business models to guarantee the practical effectiveness of such surveillance authorities.\textsuperscript{61}

\textsuperscript{59} Convention on Cybercrime, Article 21 (Interception of content data) Parties are obliged to empower competent authorities to collect or record, or compel a service provider to collect or record, content data to the extent that such activity is within their technical capabilities.

\textsuperscript{60} Convention on Cybercrime, Article 15 (Conditions and safeguards):

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, \textit{inter alia}, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.
While such authority extended to the parties is critical for law enforcement efforts in deterring and combating cybercrime, especially as cybercrime becomes increasingly inseparable from the global fight against terrorism, they may be misused constituting grave violations of personal privacy and civil liberties. Although the Convention refers to multiple international legal instruments in its Preamble, for instance the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (1950) and the United Nations International Covenant on Civil and Political Rights (1966), it may be reasonable to analyze whether the powers and authority allowed to law enforcement for the purpose of protecting privacy are enough considering the speed at which electronic communications technology has developed over the recent years. If necessary, proposals should be considered so as to regain a balance by supplementing both domestic laws and international instruments.62

E. Further Concerns

Besides some of the major shortcomings of the Convention on Cybercrime, there are still some further concerns. First, the Convention, based on conduct of cybercrime in the late 1990s, does not cover new methods of conduct in cyberspace, such as botnets, phishing, identity theft and terrorist use of the Internet. Many countries have adopted or are preparing for new laws covering some of those conducts. In addition, the terminology included in the Convention is a 1990s terminology, not necessarily suitable for the 2010s. Against this backdrop, the EastWest Institute63 established a Cybercrime Legal Working Group64 in June 2010 with the purpose of developing a set of recommendations for potential new legal mechanisms to combat cybersecurity and cybercrime. At the 2012 Worldwide Cybersecurity Summit held in New Delhi, India, the Working

63 See http://www.ewi.info
64 This group, consisting of independent, non-governmental global experts from Norway, India, Russia, the United Kingdom, the United States, France, Switzerland, Sri Lanka, Italy and Belgium, was created to examine existing legal measures against cybercrime and to advance consideration of new legal measures on cybersecurity and cybercrime. The group works toward developing recommendations for harmonized legal frameworks to combat cybercrime through international cooperation.
Group suggested the preliminary draft of a new global treaty based on a set of principles. First, the group proposed that a set of definitions of key terms such as “computer,” “computer system,” “computer data,” “spam” and “identity theft” should be agreed upon so that they are both proper and compatible with existing international approaches. Second, the new treaty should include the existing procedural instruments that are already in place and applied by several states, which include expedited preservation of stored computer data, production order, lawful collection of traffic data and lawful interception of content data, with optional provision regarding the use of remote forensic software and sophisticated technical instruments with the possibility to limit their use only to certain types of serious crime. Finally, in the area of jurisdiction and international cooperation, the group proposes that the treaty build on existing regulations on jurisdiction so as to enable the establishment of a sufficient link to claim the jurisdiction for cyber offences, such as the location of data, the existence of any/certain effects in the prosecuting country and the intention of the perpetrator to affect a certain country.

Another obvious shortcoming is that the Convention is still far from universal ratification. While a good number of European countries have ratified the Convention, not a single Asian or African nation nor many of the major players still have not - most conspicuously, Russia and China, which have been considered the source of many of the most serious cyberattacks in recent years, some of which have been suspected to be state-sponsored or, at least, state-tolerated.

Finally, the Convention does not address the particular concerns that may be in connection with cyberattacks that may constitute acts of espionage or the use of force under the laws of war, as it does not take into consideration any military and intelligence-related matters. Other

66 Id. The group proposes that the set of standards should cover the most common types of cybercrime (e.g., illegal access to a computer system, data interference, misuse of devices, computer-related forgery/fraud, offences related to child pornography) in a matter compatible with existing international approaches.
67 Id.
69 Id.
shortcomings pointed out by nations include the lack of any enforcement or reporting mechanism by which countries that do not receive the requested cooperation from other parties may seek redress.

V. CONCLUSION

Cybercrime is a multi-faceted and complex topic that requires countries to act domestically and cooperate internationally, in which respect the importance of harmonization among existing legal instruments dealing with cybercrime has been emphasized. The Council of Europe Convention on Cybercrime was adopted in response to this very need for harmonization and international cooperation. While it is certainly a welcome and necessary advance in international criminal laws, for now, it is largely an "aspirational" effort for the numerous shortcomings that have been discussed in this article.

Despite the flaws, however, the Convention is definitely a starting point and it can be improved in a number of ways. As noted earlier, the lack of an enforcement mechanism by which states denied cooperation for its requested assistance may seek redress is a major area that can be improved. Moreover, a reporting mechanism could be added by which denials of cooperation requests can be reported to a certain body, so that records of such denials can be kept and shared among the ratifying states. Such additions may be made by making amendments of the Convention's current dispute resolution mechanism. This, too, will be an enduring process but a necessary one that will affect the overall effectiveness of the Convention.

Ultimately, the true value of the Convention may lie in attracting more countries to become signatories and ratifying members. Considering the Convention's value as a relevant tool to encourage harmonization amongst member states and force the same with parties outside the Convention, attracting more members is an important task that remains. In order to commence the true process of harmonization, however, the current parties must act more collectively and assert their powers more strongly so as to encourage non-member states to align their domestic cybercrime legislations with the paradigm set forth by the Convention.

70 Supra note 1, 110.
REFERENCES


THE EQUIVALENCE OF KOREAN SUBSTANTIVE CYBERCRIME LAW TO THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME

Joyce, Michael*

I. INTRODUCTION

The borderless nature of cybercrime presents a great challenge to law enforcement agencies and the digital investigators.¹ Law enforcement is generally restricted by territorial jurisdictions based on geographical delineations that are not apparent or limiting in cyberspace.² Consequently, criminal justice responses to cybercrime must be effective across state borders, and to be truly effective be globally oriented. This requires cooperation between the justice agencies of different states if the mitigation of cybercrime is to be achieved.³ Despite the obvious benefits of international cooperation in reducing the harm caused globally by cybercrime the practical difficulties of implementing close cooperation on a global scale are great. Dealing with problems related to criminal law harmonization, mutual assistance, logistical and practical barriers in a global environment with a myriad of legislative, political, societal differences makes transnational cybercrime investigations a daunting task.⁴

* Researcher, Korean Institute of Criminology


II. INTERNATIONAL EFFORTS

Work to resolve issues regarding the international aspect of cybercrime has been underway for more than thirty-five years. This has resulted in a number of international organizations working to harmonize cybercrime efforts. Despite this lengthy period of development there is still no clear international instrument allowing for cooperation between all investigators in all countries. Nonetheless, some success has been achieved in creating transnational efforts to combat transnational cybercrime. The Mutual Legal Assistance (MLA) treaties resulting from these organizations and their related agreements are a powerful legal tool, but in practice police investigators use them charily because of their slow response relative to the speed required for online investigations. Attribution of offences in the online environment is particularly time sensitive, not only for the preservation of evidence but it also is critical for the selection of an appropriate responder. Formal cooperation is unfortunately a slow process, with responses to requests for assistance often taking months. Informal cooperation differs from formal channels as it often takes the form of a direct contact between investigators, generally from the police or a law enforcement organization allowing for low latency or real-time communication. Due to this direct nature and the lack of bureaucratic requirements it is generally a faster method of initiating transnational collaboration and often precedes cooperation through formal channels.

8 (UNODC 2013)
11 (Urbas 2012)
12 (UNODC 2013)
13 Ibid.
Informal modes of cooperation also make possible the continuation of investigations across borders where international instruments do not exist. Despite the clear advantages of and preference for informal cooperation in rapidly advancing an investigation it seems to be relatively underutilized compared to formal cooperation mechanisms.14

III. ENHANCING INTERNATIONAL COOPERATION

Measures to enhance informal cooperation between countries by international groups such as the group of eight (G8) have resulted in 24/7 available access points within the cybercrime department of the relevant justice body in each state.15 This is an important and useful measure to improve the level of international cooperation as it creates a potential link between investigative organizations where an existing relationship does not exist and provides a rapid and reliable channel of communication between countries also overcoming the problems related to the time differential between states. However, the provision of contact details does little to overcome the barriers presented by legal, cultural and language differences between states.16 Completely solving the issues caused by legal differences between states is a problem that will require a great deal of time to resolve, if the current rate of progress is any guide17. At any rate, international organizations have identified the harmonization of laws as a goal and despite the development of competing regional frameworks the efforts suggest that governments and law-makers are working to address this issue.18 The cultural and language problem is something that has largely been left to the professionals involved with the practical execution of multinational cybercrime investigations. The success stories of

14 Ibid.
15 (Schjolberg 2008)
16 See (Smith 2004).
17 Even the most successful international agreements such as the Council of Europe Convention on Cybercrime which was developed in 2001 and entered into force in 2004 at the 16th of October 2013 was still not ratified by eleven of the signing parties. See http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG
international operations against cybercrime suggest that law enforcement have been making progress on these issues.\textsuperscript{19} However, law enforcement organizations are by their nature geared towards domestic action and do not generally possess the form of resources required to efficiently affect cross-cultural communication and negotiations on a global scale.

We suggest that the practical benefit of the current level of international cybercrime law harmonization could be increased through the provision of communication tools to assist with overcoming cultural and language barriers. One form of tool that could assist in the bridging the communication gap would be an understanding of existent equivalencies in substantive law. Transforming legislative harmony into successful international cooperation requires that it be understood by those wishing to exploit it. For example, a required element of transnational legislative harmony is dual criminality. This is a core requirement for a successful outcome in a transnational investigation.\textsuperscript{20} Dual criminality is required for extradition and is a concept around which many forms of mutual legal assistance are based.\textsuperscript{21} For obvious reasons, it is not practical for a law enforcement agency to start a criminal investigation without information pertaining to a suspected criminal act (i.e. Investigating legal activities is not the role of law enforcement). International cybercrime conventions such as the Council of Europe (CoE) Convention on Cybercrime were designed to create equivalency in legislation between countries to ensure dual criminality between member states but it also communicates an understanding of transnational to those nations.\textsuperscript{22} The Convention on Cybercrime, despite its success is still a predominantly a regional instrument and consequently falls short of providing the required global solution to this problem.\textsuperscript{23}


\textsuperscript{20} (UNODC 2013)

\textsuperscript{21} Ibid.

IV. A COMMON UNDERSTANDING

The episteme that resulted in the convention is based on practical issues related to crime concerning computers and cyberspace that are universal due to the technological commonalities worldwide. The substantive law elements of the CoE Convention on Cybercrime classify crime as being either crimes against (or targeting) computers, computer-related offenses or content-related offenses. The classification of computer crime into those acts targeting computers and computer related acts is the result of a practical problem. The taxonomy arose around twenty years ago out of a need to assist investigators during criminal investigations when drafting applications for search warrants, to ensure that a search of the computer was included and executed to the necessary extent. This classification included a third category for offences where the computer was incidental to the offence. However, as a computer is not inherent in this type criminal offence the classification is not as useful for the development of cybercrime specific law. The growing value of content in our information society, and the resulting classification of illegal forms of content has resulted in informational contraband that can be stored and trafficked through information and communication technology. A classification of content crimes provides a demarcation of these offences related to such content. These classifications of cybercrimes are based on the practical requirements of computer crime investigators and the technological realities of the modern world. It is therefore reasonable to assume that they are relevant wherever investigators seek to gather appropriate evidence related to computer crime. It is also reasonable to assume that where cybercrime legislation is developed in response to a common method of crime it may contain similarities. It follows then, that the understanding of cybercrime that forms the foundation of the Convention on Cybercrime may be more universal than the convention itself and could be apparent in cybercrime legislation globally. Consequently, nations that have developed cybercrime legislation without ratifying the Convention on Cybercrime may have defined and criminalized the same or similar offenses. Based on this

23 See (Clough, 2013)  
24 Council of Europe n.d.  
26 Ibid.  
28 Ibid.
understanding, the taxonomy of defined in the CoE Convention on Cybercrime may provide a useful system for exposing, understanding and communicating latent harmonization in existing cybercrime legislation worldwide.

V. DEVELOPING A COMMON LANGUAGE FOR CYBERCRIME COOPERATION

The Convention on Cybercrime could be used as a comparative tool for determining and communicating the commonalities in substantive law in states that have developed legislative instruments for cybercrime.

An understanding of the existence of comparative legal instruments in nations outside of existing regional groups could help form a basis for communication. In order to progress investigations that require international cooperation investigators may be required to make requests in an unfamiliar language to a country with an unfamiliar criminal justice system. It is therefore possible that a legitimate request that satisfies the dual criminality requirement could be lost in translation. A request based of a common or commonly understood form of crime is conceivably more likely to be handled with confidence should each party be able to easily explain the act and consequently the illegality of the act in their respective jurisdiction. The categorization of cybercrime legislation into loose classifications for the purposes of aiding communication may permit cooperation that would have otherwise been stalled due to language or other differences.

To illustrate the possibility of classifying cybercrime legislation using of the Convention on Cybercrime as a basis for comparison we selected have the Republic of Korea (Hereinafter referred to as “Korea”) to serve as an example. Korea was not a party to the development of the CoE Convention on Cybercrime and has consequently not ratified it. However, Korea has a highly developed system of legislation and law enforcement systems to combat cybercrime and encourages international cooperation. Language differences between Korea and other countries and the

30 Jang n.d.
complexity of cybercrime legislation in Korea could potentially form a barrier to international cooperation. Korea is therefore a good example of a nation where a communication tool for defining the compatibility of legal instruments could improve international cooperation by providing a foundation for interaction.

By classifying Korean substantive cybercrime law using cybercrime definitions from the CoE Convention on Cybercrime we can determine a level of potential harmony between the provisions in Korean criminal law for cybercrime and those of countries that have either ratified the convention or have developed similar legal instruments. An understanding of this existing level of harmony and the corresponding taxonomical terminology may then serve as a basis for more confident and improved international cooperation between Korea and other nations through both informal and formal channels.

VI. CYBERCRIME LEGISLATION IN KOREA

Cybercrime legislation in Korea is complex and reflects the nature of its development as a response to a rapidly developing domestic information and communications technology environment. Korea’s commitment to information technology has resulted in a similar dedication to the creation and preservation of a secure online environment. The need to ensure a safe environment for persons, particularly children, their privacy and unhampered use of ICT as well as the protection of businesses, particularly online businesses has resulted in a number of laws that relate computers and cyberspace. Listed in table 1 below are some of the legislative acts enacted into law in Korea as part of the effort to combat cybercrime.
<table>
<thead>
<tr>
<th>Legislative Act</th>
<th>Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal Act^{31}</td>
<td>Manipulating or Impairment of Records, Computer Fraud, Computer Interference,</td>
</tr>
<tr>
<td>Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc.^{32}</td>
<td>Unauthorized Access, Transmitting Malware, DDoS, Online Pornography, Cyber Stalking, Online Defamation, SPAM</td>
</tr>
<tr>
<td>Act on the Protection of Information and Communications Infrastructure^{33}</td>
<td>Critical Infrastructure.</td>
</tr>
<tr>
<td>The Framework Act on Electronic Commerce^{34}</td>
<td>e-commerce</td>
</tr>
<tr>
<td>Digital Signature Act^{35}</td>
<td>e-commerce</td>
</tr>
<tr>
<td>The Act on the Punishment of Sexual Crimes and Protection of the Victims Thereof^{36}</td>
<td>cyber-sexual harassment</td>
</tr>
<tr>
<td>Act on the Protection of Children and Juveniles From Sexual Abuse^{37}</td>
<td>child pornography</td>
</tr>
<tr>
<td>Copyright Act^{38}</td>
<td>on-line copyright infringement</td>
</tr>
<tr>
<td>Computer Programs Protection Act^{39}</td>
<td>on-line copyright infringement</td>
</tr>
<tr>
<td>Game Industry Promotion Act^{40}</td>
<td>on-line games</td>
</tr>
<tr>
<td>Protection of Communications Secrets Act^{41}</td>
<td>Wiretapping or censoring private communications</td>
</tr>
<tr>
<td>Telecommunications Business Act^{42}</td>
<td>Communication Confidentiality</td>
</tr>
<tr>
<td>Personal Information Privacy Act^{43}</td>
<td>Personal Privacy and Data Protection</td>
</tr>
<tr>
<td>Law on the protection and use of location information^{44}</td>
<td>Location Privacy</td>
</tr>
<tr>
<td>Internet Multimedia Broadcasting Business Act^{45}</td>
<td>User Data Privacy</td>
</tr>
</tbody>
</table>

**Table 1**  
Korean Cyber-Law

---

31 Criminal Act (Korea) 1953 [Ministry of Government Legislation (Korea) trans.  

32 Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc. (Korea) 2001 [Korean Legislation Research Institute trans.  

33 Act on the Protection of Information and Communications Infrastructure (Korea) 2001 [Korean Legislation Research Institute trans.  

http://www.moleg.go.kr/lawinfo/engLawInfo?pstSeq=52442&searchCondition=AllForEngLaw&searchKeyword=%EC%A0%84%EC%9E%90]

35 Digital Signature Act (Korea) 2009 [Ministry of Government Legislation (Korea) trans.  
http://www.moleg.go.kr/lawinfo/engLawInfo?pstSeq=52443&searchCondition=AllForEngLaw&searchKeyword=%EC%A0%84%EC%9E%90]

36 Act On The Prevention Of Sexual Assault And Protection, Etc. Of Victims Thereof (Korea) 2011  
[Ministry of Government Legislation (Korea) trans.  
http://www.moleg.go.kr/lawinfo/engLawInfo?pstSeq=58519&searchCondition=AllForEngLaw&searchKeyword=%EC%84%B1%ED%8F%AD%EB%A0%A5]
VII. EQUIVALENCE TO THE COE CONVENTION ON CYBERCRIME

The following is a classification of Korean law as compared to the CoE Convention on Cybercrime. It is intended to provide a description of a relevant Korean law for each of the cybercrimes classified by the CoE in order to illustrate the degree of harmony already existing between the convention and the cybercrime legislation of Korea and provide a reference tool to promote communication between Korean investigators and other cybercrime investigators internationally. It should be noted that Korean law requires criminal intent for all offences for them to be punishable. Article 13 of the Criminal Act of Korea (1953) provides that:

[An] act performed through ignorance of the facts which comprise the constituent elements of a crime shall not be punishable, except as otherwise provided by [the] Act.46

The general provisions of the Criminal Act of Korea apply to all criminal acts, including those defined in special acts and consequently it is a requirement that all offences be committed with intent to be punishable as criminal acts.47 The Act also provides an exception for the case of negligent action in Article 14 which states that:

46 Criminal Act (Korea) 1953 art 13
47 Dr. Hyun-wook Chun, Personal Communication, 2013 October 8
[An] Act performed through ignorance of the facts which comprise the constituents of a crime by neglect of normal attention, shall be punishable only when prescribed so by [the] Act.48

Therefore, all acts of cybercrime where performed with intent shall be punishable, with the exception of where the law specifically defines negligent acts also punishable.

A. Definitions

The Convention on Cybercrime defines a ‘computer system’ as a “device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data”.49 This definition intends to include a device consisting of hardware and software (i.e. a set of stored instructions) that allows the processing data either with or without direct human intervention either alone or as part of a network.50

Korean legislation does not specifically define a ‘computer system’. However, the ‘Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc.’ (Hereinafter referred to as “PICNUIP”) defines an information and communications network as an “information and communications system for collecting, processing, storing, searching, transmitting or receiving information by means of telecommunications facilities”.51 In a practical sense, nearly all modern computers are connected to a telecommunications network and those that are not conform to a reasonable person’s understanding of a computer, making the distinction between the terms minor.

The Convention on Cybercrime defines ‘computer data’ as “any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function”.52 The Korean PICNUIP act defines the term ‘electronic document’ as “data prepared and transmitted,
received, or stored electronically in a standardized form of document by a device capable of processing information, such as a computer”. These terms of ‘computer data’ and ‘electronic document’ are very similar in definition and in practical application could be considered identical.

Under its CoE definition, a ‘service provider’ is both “any public or private entity that provides to users of its service the ability to communicate by means of a computer system” and “any other entity that processes or stores computer data on behalf of such communication service or users of such service”. The PICNUIP Act of Korea defines a service provider as either a traditional (telephony) telecommunications service provider or those who “provide information or intermediate the provision of information for profit by utilizing services rendered by a telecommunications business operator”. The Korean definition differentiates between the infrastructure provider and the business of providing access to such. However as both are combined in this definition of a service provider it is equivalent to the CoE but also includes those business that provide services online as well as the those providing access to the Internet.

The Convention on Cybercrime defines ‘traffic data’ as any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service. Korean law does not define traffic data separately from an electronic document. However, as the use of the term in limited to the criminal procedure section of the Convention on Cybercrime it is not relevant to this study.

There are differences between the definitions of the Convention on Cybercrime and those of Korean cybercrime legislation. However, in a practical sense these should not present a barrier to international cooperation as the Korean definitions do not contradict the definitions

53 Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc. (Korea) 2001 art 2.5
54 Convention on Cybercrime (Council of Europe) 2001 art. 1.c.i
55 Ibid.
56 Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc. (Korea) 2001 art 2.3
57 Convention on Cybercrime (Council of Europe) 2001 art. 1.d.
listed in the CoE Convention on Cybercrime.

**B. Against the Machine**

Section two of the CoE Convention on Cybercrime provides measures for offences against the confidentiality, integrity and availability of computer data and systems. These offences are categorized as illegal access, illegal interception, data interference, system interference, or misuse of devices.  

**1) Illegal access**

Article two of the Council of Europe Budapest Convention on Cybercrime provides a measure for the illegal access to a system:

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.  

Importantly, this defines the “access to whole or part of a computer system without right” as that which is to be regarded a criminal offence.  

Korean legislation as contained in PICNUIP Article 48 that provides for the Prohibition of Intrusive and Similar Acts on an Information and Communications Network provides similarly for the intrusion on a system without right for access. The article states as follows:

> (1) No one shall intrude on an information and communications network without a rightful authority for access or beyond a permitted authority for access.

---

58 Council of Europe n.d.)[35]
59 Convention on Cybercrime (Council of Europe) 2001. Art. 2
60 Ibid.
61 Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc. (Korea) 2001 art 48
62 Ibid. art 48.1
Penal provisions for such behavior are provided under article 72.1.1 of the same act that provides punitive measures of imprisonment with prison labor for not more than three years or a fine not exceeding 30 million won for a person who intrudes on an information and communications network in violation of Article 48.1 of the Act.63

The Korean legislation matches the Council of Europe provisions and provides additional detail regarding the exceeding of permission by users. The cybercrime legislation of Korea and the Budapest Convention on Cybercrime could be considered to be in harmony with respect to the act of unauthorized access to a computer system.

(2) Illegal interception

Article three of the CoE Convention on Cybercrime provides a measure for the illegal interception of communications as follows:

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.64

This element requires parties to the convention make illegal the interception of private (non-public) transmissions of computer data without right by technical means.65 The Korean PICNUIP Act defines as criminal the infringing, misappropriation or divulging of a person’s secret (private information) stored processed or transmitted through an information and communications network.66 Article 49 of the Act related to the ‘Protection of Secrets’ is as follows:

63 Ibid. art 72.1.1
64 Convention on Cybercrime (Council of Europe) 2001. art. 3
65 (Council of Europe n.d.)
66 Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc. (Korea) 2001 art 49
No one shall mutilate another person’s information processed, stored, or transmitted through an information and communications network, nor shall infringe, misappropriate, or divulge another person’s secret.67

Penal provisions for perpetration of this deed are provided under article 71.11 of the same act which prescribes a punitive measure of imprisonment with prison labor for not more than five years or by fine not exceeding 50 million won to a person who mutilates another person’s information or who infringes, misappropriates, or divulges another person’s secret in violation of Article 49 of the Act.68

The Korean measures match the requirements of the Convention on Cybercrime provisions for illegal interception and as such could be considered as harmonious.

(3) Data Interference

Article four of the CoE Convention on Cybercrime defines measures for the act of data interference as follows:

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.69

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.70

This article identifies the intentional damage, deletion, deterioration, alteration or suppression of computer data without right. This provision aims to provide protection to computer programs and data against damage similar to that of corporeal objects.71 Specifically, the protection against the damage to data and programs as constituted by data; including the destruction of the data, the negative alteration of the data, a change to the content of the data such as the insertion of additional code in the case of

67 Ibid.
68 Ibid. 72.1.1
69 Convention on Cybercrime (Council of Europe) 2001. art. 4.1
70 Ibid. 4.2
71 (Council of Europe n.d.)
a Trojan program, or the prevention of data availability.\textsuperscript{72}

The Korean Criminal Act provides data and programs the same protections as corporeal objects by referring to them both in the same provision. Article 366 of the Criminal Act of Korea, referring to the Destruction and damage of property, etc. states:

\begin{quote}
A person who, by destroying, damaging, or concealing another’s property, document or special media records, such as electromagnetic records, etc., or by any other means, reduces their utility, shall be punished by imprisonment for not more than three years or by a fine not exceeding seven million won.\textsuperscript{73}
\end{quote}

This provides the same protection to special media records, which includes computer data and consequently computer programs constituted of data as that afforded to corporeal objects. It defines the destruction, damage, concealment or reduction in utility of data as an illegal act. This matches the illegal acts of “damage, deletion, deterioration, alteration or suppression” against data as defined in the Convention on Cybercrime.\textsuperscript{74} Note that heavier penalties apply where the data affected is that of a public office, as dictated in article 141 of the Criminal Act of Korea, referring to the’ Destruction of Public Goods’ that provides:

\begin{quote}
A person who damages or conceals documents or other goods, or special media records, such as electromagnetic records, etc. used by a public office or spoils its utility by other methods, shall be punished by imprisonment for not more than seven years or by a fine not exceeding ten million won.\textsuperscript{75}
\end{quote}

In certain circumstances other parts of the criminal act could also be relevant where the alteration of data was performed with the intent of destroying a business,\textsuperscript{76} producing an error in the processing of documents pertaining to a right, duty or certification of fact of another person\textsuperscript{77} or where a public document was altered to disrupt business.\textsuperscript{78}

\textsuperscript{72} Ibid.
\textsuperscript{73} Criminal Act (Korea) 1953 art 366
\textsuperscript{74} Convention on Cybercrime (Council of Europe) 2001. art. 4.1
\textsuperscript{75} Criminal Act (Korea) 1953 art 141
\textsuperscript{76} See Criminal Act (Korea) 1953 art 314.2 ’Interference with Business’
\textsuperscript{77} See Criminal Act (Korea) 1953 art 232 ‘Falsification or Alteration of Private Electromagnetic Records’
\textsuperscript{78} See Criminal Act (Korea) 1953 art 227.22 ‘False Preparation or Alteration of Public Electromagnetic
The Korean legislation as noted in the Criminal Act can be seen to match the provisions of the CoE Convention on Cybercrime for data interference. The Korean substantive criminal law for data interference is therefore in harmony with those countries that have ratified the European Convention on Cybercrime or have matched it with their legislation.

(4) System Interference

The CoE Convention on Cybercrime article five on system interference provides the following:

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.79

This provision is intended to criminalize those acts considered as computer or communications system sabotage committed by methods not requiring a type of access that would be considered unauthorized. This would include the engineering of a large amount of data traffic to a system that reduces the ability of that system to function, as in the case of a denial of service attack.80

Article 12.3 of the Act on the Protection of Information and Communications Infrastructure of Korea provides that no one commit an act of:

Abruptly sending large amounts of signals with the purpose of obstructing the operation of main information and communications infrastructure, or causing a fallacy in information processing by inducing the processing of a wrong order, etc.81

This article also targets an act of computer network sabotage that does not require illegal access, such as a denial of service attack. The noted purpose of the attack as obstructing the operation of an information and communications infrastructure is analogous to the Convention on Cybercrime specification of

---

79 Convention on Cybercrime (Council of Europe) 2001 art 5
80 (Council of Europe n.d.)
81 Act on the Protection of Information and Communications Infrastructure (Korea) 2001 art 12.3
an intentional hindering of computer system function. However, this article is intended for large scale attacks that affect the main information and communications network of the country, as is reflected by the stiff penalties attached to this act in the accompanying penal provisions. These are stated in chapter 7, article 28 of the same act as:

(1) Anyone who disturbs, paralyzes or destroys main information and communications infrastructure, in violation of Article 12, shall be punished by imprisonment for not more than ten years or by a fine not exceeding 100 million won.

(2) Any person who attempts a crime under paragraph (1) shall be subject to punishment.82

Provisions for a similar act against a network of a smaller scale are contained in article 48.3 of the PICNUIP Act which states that:

(3) No one shall cause a trouble to an information and communications network purposely to interfere with stable operation of the information and communications network by sending a large amount of signals or data, letting the network process an illegitimate, order etc.83

This provision also clearly spells out the illegality of a denial of service attack by noting the method of purposely interfering with the stable operation of an information and communications network by the sending of a large amount of signals or data. An act with the effect of interfering with the stable operation of a communications network is similar to the intentional hindering of a computer system indicated in the CoE Convention on Cybercrime. This act carries a penalty of imprisonment with prison labor for not more than five years or a fine not exceeding 50 million Korean won.84

The Korean legislation as noted in the Act on the Protection of Information and Communications Infrastructure and the PICNUIP Act can be seen to match

82 See the Act on the Protection of Information and Communications Infrastructure (Korea) 2001 art 28. Note that the translation for article 28.2 has been altered by the author for ease of legibility from the official English translation which reads “(2) Any person who is attempted a crime under paragraph (1) shall be subject to punishment”.
83 Act on the Protection of Information and Communications Infrastructure (Korea) 2001. art 43.3
84 Ibid art 71.10
the provisions of the Council of Europe’s Convention on Cybercrime for systems interference. The Korean law does however differentiate between an attack that affects the main information and communication network and an attack that affects a lesser network. Nonetheless, the Korean substantive criminal law for system interference could be considered as being in harmony with those countries that have ratified the European Convention on Cybercrime or have matched it with their legislation.

(5) Misuse of Devices

Article six of the Council of Europe Convention on Cybercrime defines measures for the misuse of devices as follows:

1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

   a) the production, sale, procurement for use, import, distribution or otherwise making available of:

      i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

      ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

   b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2) This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2
through 5 of this Convention, such as for the authorized testing or protection of a computer system.

3) Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.85

The misuse of devices provisions was intended to provide for the development and making available of tools for the commission of crimes in order to combat the creation of a black market for criminal devices and prevent the subsequent facilitation of offenses.86

These markets for malicious software do exist, and individuals do create and make available malicious programs online for reputational and economic benefit.87 The prices set for these programs can range from tens of thousands to just tens of dollars, however newly developed and professionally maintained programs such as the Zeus, “Hand of Thief” or the KINS banking Trojan are offered for sale online for $3,000 - $5,000 U.S. Dollars.88

Despite the apparent need to combat a black market facilitating crime, this part of the CoE Convention on Cybercrime is potentially problematic as it includes for the possession of malicious programs, which could be argued as an inhibitor to the research and development of information security solutions.89

85 Convention on Cybercrime (Council of Europe) 2001 art. 6
86 (Council of Europe n.d.)
Information security researchers and investigators often capture samples of malicious programs (malware) that spread across the Internet in order to analyze them.\(^90\) This analysis forms the basis for not only greater understanding of malware but also allows the development of security countermeasures. Furthermore, security researchers often develop programs to test hypothesized security weaknesses in information and communications systems and technology with the intent that the verification of these weaknesses will lead to enhancements in those systems and technologies.\(^91\)

The provisions in the CoE Convention on Cybercrime provide that the device be designed or adapted for the primary purpose of committing an offence or in the case of data that provides access, with the intent that it be used in the commission of an offence.\(^92\) In order to provide protection to researchers, or developers of devices that could possibly be subverted, the possession of a device is not an offence in itself, where there is no intent to commit an offence.\(^93\) Despite this, it is still possible that the intent to use such a device be argued as implicit in the possession of such a thing and as such this provision of the Convention on Cybercrime is considered contentious by some.\(^94\)

The Korean provisions designed to combat the online market for malware does not criminalize the possession or procurement of malware and as such does not present the same issue to security researchers as the EoC Convention on Cybercrime, and as such avoids this criticism. Korean PICNUIP Act Article 48.2 on the ‘Prohibition on Intrusive Acts, etc. on Information and Communications Networks’ provides a measure to combat the conveyance and circulation of malware as follows:

(2) No one shall, without justifiable grounds, transmit or disseminate a program (hereinafter referred to as a “malicious program”) capable of causing the damage, destruction, forgery, or modification of data, programs, etc., or interfering with the functioning of information and communications system.\(^95\)

\(^90\) Aquilina, James; Casey, Eoghan; Malin, Cameron; Rose, Curtis “Malware Forensics: Investigating and Analyzing Malicious Code”. Syngress Publishing Burlington, 2008


\(^92\) (Council of Europe n.d.)

\(^93\) Ibid.

\(^94\) (S. Brenner 2006)
The penal provisions for this offence are provided under article 71.9 of the same act prescribe a punishment of imprisonment with prison labor for not more than five years or by fine not exceeding 50 million won for a person who conveys or circulates a malicious program in violation of article 48.2.96

The PICNUIP act reduces the sale, distribution or otherwise making available of malware to simply the transmission or dissemination of malware which includes all of these acts without precluding other forms of software dissemination and deployment. The acts of malware production, import, procurement for use are omitted, a measure which provides additional confidence to security researchers and information security developers. For the purposes of international cooperation, this omission is irrelevant as it is required that malware that is either produced, imported or procured for use in Korea to then be transmitted or distributed to an offender or victim residing in another jurisdiction before it is a source of harm at that location.

We would consider that Korean cybercrime legislation be effectively harmonious with the CoE Convention on Cybercrime for the purposes of combatting the international black market for malicious programs.

C. Computer Related Offences

The creation of measures for computer related offenses reflect the increased volume and value of information that is now stored, processed

95 See Act on the Protection of Information and Communications Infrastructure (Korea) 2001. Art 43.3. Note that this translation has been altered by the author. The official English translation for this article reads “No one shall mutilate, destroy, alter, or forge an information and communications system, data, program, or similar without a justifiable grounds, nor shall convey or spread a program that is likely to interrupt operation of such system, data, program, or similar (hereinafter referred to as “malicious program”).” However, this translation creates confusion as the act and the instrument performing the act are separated. This legislation was not intended to provide for the act against the data, program or system separate to that performed by a malicious program, as is clear from the accompanying penal provisions in Article 71.9 of the same act that only provide for the acts of conveying or circulating a malicious program. For reference, the original Korean text of the Act on the Protection of Information and Communications Infrastructure (Korea) 2001 Art 48.2 is as follows:

② 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 "악성프로그램"이라 한다)을 전달 또는 유포하여서는 아니 된다.

96 Act on the Protection of Information and Communications Infrastructure (Korea) 2001 art 71.9
and represented by information processing technology.\textsuperscript{97} Computer-related Offenses as defined in the Council of Europe Convention on Cybercrime are those offenses such as fraud and forgery committed through a computer system.\textsuperscript{98} The broad range of these offenses are an extension of ordinary crime though the use of a computer system. As such, cybercrime specific legislation pertaining to these offenses may not be necessary where the existing law is sufficiently broad, or is broadened to include the use of computer systems. The Convention on Cybercrime provides for acts of computer related forgery and fraud.

(1) Computer-related forgery

Article seven of the CoE Convention on Cybercrime provides for computer related forgery as follows:

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.\textsuperscript{99}

The CoE Convention on Cybercrime provisions for computer-related forgery are to ensure that actions that involve the fraudulent use of a computer system, data or processes with the purpose of generating inauthentic data of legal import.\textsuperscript{100} The need for legislation pertaining to this act is to ensure that the changes in the manner of creating, validating, processing and articulating information brought about through the advancement of information processing technology have not resulted in a gap between legislation designed for conventional forgery offenses and those new possibilities for committing these offenses.

\textsuperscript{97} (Council of Europe n.d.)
\textsuperscript{98} Ibid.
\textsuperscript{99} Convention on Cybercrime (Council of Europe) 2001 art 7
\textsuperscript{100} (Council of Europe n.d.)
The Korean criminal law pertaining to forgery under the criminal act draws a distinction between offenses concerning official documents, i.e. those documents prepared by a public official or office and documents prepared by private individuals or for private purposes. In the case of public documents, article 227.2 of the Korean Criminal Act titled ‘False Preparation or Alteration of Public Electromagnetic Records’ provides that:

A person with the intention of disrupting business forges or alters electromagnetic documents of public official or public office shall be punished by imprisonment not more than ten years. 101

The creation of false record or the alteration of and existing records or a public office for the purpose of disrupting business is defined as illegal in this measure. The similar treatment of private documents is provided for in article 232.2 ‘Falsification or Alteration of Private Electromagnetic Records’ which dictates that:

Any person who forges or alters, with the intention of making any error in the management of affairs, any special media records, such as another person’s electromagnetic records which pertains to a right, duty, or a certification of fact, shall be punished by imprisonment for not more than five years, or a fine not exceeding ten million won. 102

Note that the intention of disrupting business or the management of affairs, and the limitation on the types of record involved in the case distinguish this act from that of data interference as described in articles 141.103 and 366104 of the same act.

101 See Criminal Act (Korea) 1953 art 227.2. Note that this translation has been altered by the author. The word “forges” replaces the word ‘falsely’ as used in the English translation provided by the Korean Ministry of government legislation (MoLeg) on the understanding that forge more adequately expresses the meaning of 위작 as an adjunct to 변작하다 so that together they express both the creation of an inauthentic duplicate and the alteration of an existing element to present false meaning. The MoLeg version is available at http://www.moleg.go.kr/english/korLawEng?pstSeq=52670

102 See Criminal Act (Korea) 1953 art 232.2. The translation of this article has been modified from the version provided by the Korean Ministry of government legislation (http://www.moleg.go.kr/english/korLawEng?pstSeq=52670) to enhance the intelligibility of the article. For clarity refer to the Korean language version of the Criminal act, as available at http://www.law.go.kr , which states: 제232조의2(사전자기록위작・변작) 사무처리를 그르치게 할 목적으로 권리・의무 또는 사실증명에 관한 타인의 전자기록등 특수매체기록을 위작 또는 변작한 자는 5년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

103 Criminal Act (Korea) 1953 art 141

104 Ibid. Art 366
The CoE Convention on Cybercrime provides a broader range of acts (i.e. the input, alteration, deletion, or suppression of computer data) which could result in inauthentic data. The Korean provisions specify only the creation of inauthentic data and the alteration of an existing record. Deletion could be interpreted as a form of alteration, as the process of deletion involves the alteration of either information allowing the access to stored data, or the alteration of digital patterns to remove the stored meaning. The suppression of data for the purposes of making an error in the management of affairs is not provided for under Korean laws pertaining to electronic forgery; however such an act would be encompassed by other provisions pertaining to interference with systems. The Korean provisions for computer related forgery could then be considered as being generally in harmony with the Convention on Cybercrime.

(2) Computer-related fraud

Article eight of the CoE Convention on Cybercrime provides for computer related fraud as follows:

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a) any input, alteration, deletion or suppression of computer data,
b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

This provision aims to criminalize undue manipulations in the course of data processing with the intended effect of an illegal transfer of property. The article provides for a broad range of possible manipulations of data; nominally any input, alteration, deletion or suppression of computer data or any interference with the functioning of a computer system that could result in economic or possessory loss. It also stipulates that the action should be conducted intentionally and without

---

105 Convention on Cybercrime (Council of Europe) 2001 art 7
106 See Section 2.1.4 of this document titled ‘System Interference’ for more details.
107 Convention on Cybercrime (Council of Europe) 2001 art 8
108 (Council of Europe n.d.)
right and that the procurement of benefit is also intentional and without right. The article is designed to include a broad range of actions that could be used to affect fraud but exclude commercial practices which could similarly cause economic gain to one or loss to another.109

Korean criminal law similarly provides a broad range of activities involving computer systems or data that lead to either the benefit of one or the loss of another. The offenses are separated by outcome in two distinct articles of criminal law. Article 347.2 of the Korean Criminal Act titled ‘Fraud by means of computers’ provides for offenses that result in the benefit of the offender or a third person.110 Alternatively, offenses that result in loss are provided for in article 314.2 of the same Act.111

Article 347.2 of the Criminal Act provides that:

Any person who acquires any benefits to property or has a third person acquire them, by making any data processed after inputting a false information or improper order, or inputting the data without any authority into the data processor, such as a computer, etc., shall be punished by imprisonment for not more than ten years or a fine not exceeding twenty million won.112

The input of false data, the alteration of data or the processing of data or the entry of data without authority into a computer system for benefit is defined as an illegal act by this article. The terminology used to define the acts is sufficiently broad so as to include the addition, modification or deletion of data or program code to produce false output, or in the case of data entry without authorization provide inappropriate data.

Article 314 of the Korean Criminal Act provides that:

(1) A person who interferes with the business of another by the method of Article 313113 or by the threat of force, shall be

109 Ibid.
110 Criminal Act (Korea) 1953 art 347.2
111 Ibid. art 314.2
112 Ibid. art 347.2
113 Criminal Act (Korea) 1953 Art 14.1 is included as the sentencing requirements for Criminal Act (Korea) 1953 art 314.2 are listed in this article. Criminal Act (Korea) 1953 art 313 refers to general crimes against credit and states: “A person who injures the credit of another by circulating false facts or through fraudulent means, shall be punished by imprisonment for not more than five
punished by imprisonment for not more than five years or by a fine not exceeding fifteen million won.

(2) Any person who interferes with another person’s business by damaging or destroying any data processor, such as a computer, or special media records, such as electromagnetic records, or inputting false information or improper order into the data processor, or making any impediment in processing any data by other way, shall also be subject to the same punishment as referred to in paragraph (1)\textsuperscript{114}

A very broad definition of acts that could interfere with the business of another are defined in article 314.2 of this Act including the damage or destruction of a data processor such as a computer system, the damage or destruction of data, the entry of false information into a data processor, the modification or addition of programming code to process data improperly, or any form of data processing impediment.\textsuperscript{115}

The Korean law provides similar measures to the conditions of the Council of Europe Convention on Cybercrime article concerning computer fraud and additionally provides utility in cases where the action causes a detriment to the business of another and the procurement of benefit is difficult to ascertain. The Korean legislative provisions for computer fraud could be considered as meeting the measures outlined in the Convention on Cybercrime.

**D. Content-Related Offences**

Content-related offences are those crimes that involve the storage, trade and distribution of contraband content via information and communication technology.\textsuperscript{116} The Convention on Cybercrime in particular seeks to combat the sexual abuse of children for the purposes of producing pornographic material by outlawing all activities related to such material.\textsuperscript{117} It also seeks to reduce the abuse of authors and neighboring rights made abundant by the ease of duplicating and transmitting content on the Internet.\textsuperscript{118}

\textsuperscript{114} Criminal Act (Korea) 1953 art 314
\textsuperscript{115} Ibid. art 314.2
\textsuperscript{116} (Wall 2007)P50
\textsuperscript{117} (Council of Europe n.d.)
\textsuperscript{118} Ibid.
(1) Offences related to child pornography

Article nine of the Council of Europe Convention on Cybercrime provides measures concerning offences related to child pornography. This article states that:

1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
   a) producing child pornography for the purpose of its distribution through a computer system;
   b) offering or making available child pornography through a computer system;
   c) distributing or transmitting child pornography through a computer system;
   d) procuring child pornography through a computer system for oneself or for another person;
   e) possessing child pornography in a computer system or on a computer-data storage medium.

2) For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:
   a) a minor engaged in sexually explicit conduct;
   b) a person appearing to be a minor engaged in sexually explicit conduct;
   c) realistic images representing a minor engaged in sexually explicit conduct.

3) For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4) Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c. 119

Article nine of the Convention on Cybercrime attempts to strengthen protective measures for children through the modernization of criminal law to encompass the use of computer system in sexual offenses against children.

119 Convention on Cybercrime (Council of Europe) 2001 art 9
children. The provisions seek to criminalize the various forms of electronic production, possession and distribution of child pornography; nominally the production, offering, making available, distribution, transmission, procurement, or position of child pornography. Child pornography is defined as a visual depiction of either a minor (i.e. a person under eighteen years of age), person appearing to be a minor or realistic images representing a minor engaged in sexually explicit conduct.

The definition of pornography is governed by national standards related to the classification and the right to freedom of expression therefore material having an artistic, medical, scientific or similar merit may not be considered as being pornographic. Sexually explicit conduct encompasses the real or simulated practice of:

- All forms of sexual intercourse including genital-genital, oral-genital, anal-genital or oral-anal contact, between minors, or between an adult and a minor regardless of sex;
- Bestiality,
- Masturbation,
- Sadistic or masochistic abuse in a sexual context, or
- Lascivious exhibition of the genitals or the pubic area of a minor.

The measures intend for these acts to be criminalized where they are conducted intentionally and without right.

The Korean Act On The Protection Of Children And Juveniles From Sexual Abuse provides measures that are sufficiently broad so as to include the use of an electronic medium. In particular, various forms of production, possession and distribution of child pornography are included in article eight of this Act on the Production, Distribution, etc. of Child or Juvenile Pornography that states that:

(1) Any person who produces, imports or exports child or juvenile pornography shall be punished by imprisonment for a limited term of not less than five years.

120 (Council of Europe n.d.)
121 Ibid.
122 Ibid. [100]
123 Act on the Protection of Children and Juveniles From Sexual Abuse (Korea) 2009
(2) Any person who sells, lends or distributes child or juvenile pornography for commercial purposes, or possesses or transports child or juvenile pornography for the said purposes, or publicly exhibits or shows child or juvenile pornography shall be punished by imprisonment with prison labor for not more than seven years.

(3) Any person who distributes, publicly exhibits or shows child or juvenile pornography shall be punished by imprisonment with prison labor for not more than three years or by a fine not exceeding 20 million won.

(4) Any person who possesses child or juvenile pornography shall be punished by a fine not exceeding 20 million won.

(5) Any person who recruits a child or juvenile for a child or juvenile pornography producer, knowing that they are to be used for producing child or juvenile pornography shall be punished by imprisonment with prison labor for a period of not less than one year but not more than ten years.

(6) Any person who attempts to commit an offense as prescribed in paragraph (1) shall be punished.\(^{124}\)

This article defines as criminal the production, importation, exportation, sale, lending, distribution, public exhibition, transportation or possession of child pornography or the attempt of the same. These measures match the provisions as defined in the Convention on Cybercrime.

However, there are some differences in the definitions of terms that could create complications. The age of a minor is defined as a person under the age of nineteen “provided that persons for whom the first day of January of the year in which they reach 19 years of age has arrived shall be excluded”.\(^{125}\) This intends that on the first day of the year in which one reaches nineteen years of age, regardless of the date of birth. Consequently, a child born in the month of June would be considered as nineteen at the age of eighteen years and six months; their age at the first of January. The Korean definition of child is older than the United Nations and EoC definition of a child by a period of up to one year. This could cause some confusion in limited cases, where the age of the subject of the material is eighteen years of age.

The term ‘child pornography’ as defined by the act on ‘The Protection Of

\(^{124}\) Ibid. Art 8
\(^{125}\) Act on the Protection of Children and Juveniles From Sexual Abuse (Korea)2009 art 2.1
Children And Juveniles From Sexual Abuse’ includes the depiction in the form of film, video, game software, or picture or image, etc. displayed on computers or other communication media of a minor performing an act of:

(a) Sexual intercourse;
(b) Pseudo-sexual intercourse using parts of the body, such as the mouth and anus, or implements;
(c) Touching or exposing the whole or part of the body, which causes sexual humiliation or repugnance of ordinary people;
(d) Masturbation.126

The terminology used for the definition of child pornography matches that of the CoE Convention on Cybercrime. The terminology utilized in the Korean legislation is sufficiently flexible to include all of the acts defined in the convention although they are not as explicitly defined. For example, bestiality could be considered as act defined by either art. 4.b or art. 4.c and Sadistic or masochistic abuse in a sexual context would be an act as defined by art. 4.c of the Act On The Protection Of Children And Juveniles From Sexual Abuse.127

The measures for child pornography in Korea could be considered as being in harmony with the CoE Convention on Cybercrime.

(2) Infringements of copyright and related rights

Title four of the CoE Convention on Cybercrime pertains to offences related to infringements of copyright and related rights. Article ten within this section pertains to offences related to infringements of copyright and related rights defines such an offence as follows:

1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions,

---

126 Act on the Protection of Children and Juveniles From Sexual Abuse (Korea)2009 art 4
127 See Act on the Protection of Children and Juveniles From Sexual Abuse (Korea)2009 art 4
where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3) A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.  

Korea acceded to the Bern Convention for the Protection of Literary and Artistic Works in 1996, adopted the WTO the Agreement on Trade-Related Aspects of Intellectual Property Rights in 1995 and adopted the WIPO Copyright Treaty in 1996 with the agreements entering into force in, 1996, 1995 and 2002 respectively. The 1957 Copyright act of Korea was subsequently updated to meet the obligations of such treaties and to include for the infringement of copyright and related rights by means of a computer system.

The act permits a variety of legal options for action against parties related to the breach of copyright and related rights online, including criminal prosecutions. The act defines infringements in article 124 as follows:

128 Convention on Cybercrime (Council of Europe) 2001 art 10  
130 See Ibid.  
(1) Any act that falls under any of the following shall be deemed an infringement of copyrights or other rights protected pursuant to this Act:

1. The importation into the Republic of Korea, for the purpose of distribution therein, of goods which would constitute an infringement of copyrights or other rights protected pursuant to this Act if they were made in the Republic of Korea at the time of such importation;
2. The possession, for the purpose of distribution, of goods produced by any act that constitutes an infringement of copyrights or other rights protected under this Act (including those imported as provided in foregoing Subparagraph 1) with the knowledge of such infringement; and
3. The use for business of copies of a program produced by infringing on the copyright of the program (including imported objects under Subparagraph 1) by a party who acquired it with the knowledge of such infringement.

(2) Any act of providing, manufacturing, importing, transferring, lending, or interactively transmitting technologies, services, products, devices, or components thereof for the primary purpose of circumventing technological protection measures for copyrights or other rights protected pursuant to this Act by such means as eliminating, modifying, or bypassing such technological protection measures without legitimate rights to do so shall be deemed an infringement of copyrights or other rights protected pursuant to this Act.

(3) Any act conducted without legitimate rights with the knowledge or negligent ignorance of the fact that an infringement on copyrights or other rights protected pursuant to this Act is caused or concealed that falls under any of the following shall be deemed an infringement on copyrights or other rights protected pursuant to this Act: provided that this paragraph shall not apply to those cases where such act is deemed unavoidable for technical reasons, or in the light of the nature of works, etc. or the purpose, manner, etc. of the use thereof:

1. Any act of intentionally eliminating, modifying, or falsely adding right management information in an electronic format; and
2. Any act of distributing, publicly performing, publicly transmitting, or importing for the purpose of distribution of the original or
copies of works, etc. with the knowledge of the fact that right management information in an electronic format has been eliminated, modified, or falsely added.

(4) Any act of using a work in a manner defaming the honor of its author shall be deemed an infringement of his moral rights.\textsuperscript{132}

Notably, these measures include the any knowing or negligent infringement of copyright as well as the commercial use of software, distribution, importation, and possession of works for the purposes of distribution that infringes copyright or related rights. The removal, modification or false addition of digital rights management information to works in an electronic format is also considered an infringement of copyright and related rights.\textsuperscript{133}

The chapter eleven of the copyright act of Korea also provides penal provisions. Specifically, article 136.1 provides measures for a crime of infringement of property rights as follows:

(1) Any person who infringes upon author’s property rights or other property rights protected pursuant to this Act (excluding the rights under the provision of Article 93)\textsuperscript{134} by means of reproduction, public performance, public transmission, exhibition, distribution, rental, or production of a derivative work, may be punished by imprisonment for not more than five years or a fine of not more than KRW 50 million, or both.\textsuperscript{135}

Article 136.2 of the Act provides measures for offenses not involving the infringement of protected property rights as follows:

Any person, who falls under any of the following, may be punished by imprisonment for not more than three years or a fine of not more than KRW 30 million, or both:
1. Any person who has defamed the author or performer by infringing on author’s or performer’s moral rights;
2. Any person who has made registration, as provided in Articles 53 and 54, falsely (including those cases where the provisions herein

\textsuperscript{132} Copyright Act (Korea) 2009 art 124
\textsuperscript{133} Ibid art 124.3.1
\textsuperscript{134} See Copyright Act (Korea) 2009 art 93 which provides protection to database producers allowing them to retain the rights for the reproduction, distribution, broadcasting or interactive transmission of all or part of a database.
\textsuperscript{135} Copyright Act (Korea) 2009 art 136.1
apply mutatis mutandis in accordance with Paragraph (3) of Article 63, Articles 90 and 98, and Paragraph (6) of Article 101-6);  
3. Any person who has infringed upon a database producer’s rights protected pursuant to Article 93 by means of reproduction, distribution, broadcasting, or interactive transmission;  
4. Any person who has committed an act deemed to be an infringement pursuant to Paragraph (1) of Article 124;  
5. Any person who has committed an act deemed to be an infringement pursuant to Paragraph (2) of Article 124 in the conduct of business or for a profit-making purpose; and  
6. Any person who has committed an act deemed to be an infringement pursuant to Paragraph (3) of Article 124 as a business or for a profit-making purpose: provided that said provision shall not apply to any person lacking the knowledge, by negligence, of the fact that such act causes or conceals infringement on copyrights or other rights protected pursuant to this Act.136

Infringements of copyright and related rights considered as unjust but not an issue of property or moral rights are stated in Article 137, ‘Crimes Of Unjust Publications, etc.’ as follows:

Any person who falls under any of the following may be punished by imprisonment for a term of not more than one year or a fine of not more than KRW 10 million:  
1. Any person who has made a work public under the real name or pseudonym of a person other than the author;  
2. Any person who has publicly performed or communicated to the public a performance or distributed copies of the performance under the real name or pseudonym of a person who is not the actual performer;  
3. Any person who has violated the provision of Paragraph (2) of Article 14137;  
4. Any person who has operated copyright trust services without a

136 Ibid art 136.2  
137 See Copyright Act 2009 (Korea) art 12.2 which states “Even after the death of the author, no person who exploits his work shall commit an act which would be damaging to author’s moral rights if he were alive; provided that such an act is deemed to have not defamed the author in light of the nature and extent of the act, and in view of the prevailing social norms.”
permit as prescribed under Paragraph (1) of Article 105;
5. Any person who has committed an act deemed to be an infringement pursuant to Paragraph (4) of Article 124;
6. Any person, who has interfered with the business of an online service provider by intentionally requesting such online service provider to stop or resume reproduction or interactive transmission as provided in Paragraph (1) or (3) of Article 103 with the knowledge that he does not have the authority to do so; and
7. Any person who has violated Article 55-2 (including those cases where the provisions herein apply mutatis mutandis in accordance with Paragraph (3) of Article 63, Articles 90 and 98, and Paragraph (6) of Article 101-6).  

The provisions in article 137.6 are of particular interest as they provide criminal measures for the abuse of the copyright system to interfere with the operation of an online business by requesting the takedown or reinstatement of a work knowingly without authority. The copyright system provides the right of copyright holders to request the immediate cessation of transmission of their works where such transmission violates their copyright or related rights. This measure attempts to reduce the impact of copyright on online businesses by discouraging improper use of the copyright protection system. The provisions in the act pertaining to the operation of online businesses also provide the limitations of liability of online service providers with the understanding that it is not feasible for service providers to be aware of the copyrights associated with all of the data transferred through and stored on their services. Article 102 of the Act, “Limitation on the Liability of Online Service Providers”, defines these limitations as follows:

(1) In connection with the provision of services by an online service provider related to reproduction or interactive transmission of works, etc., the liability of such online service provider for infringement by other persons on copyrights or other rights protected pursuant to this Act may be reduced or waived in those cases where such online service provider prevents or stops reproduction or transmission thereof when made aware that

---

138 Copyright Act (Korea) 2009 art 137
139 See Ibid. art103.1
140 Ibid. art 102
Copyrights or other rights protected pursuant to this Act would be infringed upon due to the reproduction or interactive transmission of works, etc. by the other persons.

(2) In connection with the provision of services by an online service provider related to reproduction or interactive transmission of works, etc., such online service provider’s liability for infringement by other persons on copyrights or other rights protected pursuant to this Act shall be waived in those cases where such online service provider attempts to prevent or stop reproduction or interactive transmission thereof when made aware that copyrights or other rights protected under this Act would be infringed upon due to the reproduction or interactive transmission of works, etc. by the other persons, but it is technically impossible to do so. 141

Copyright or related rights holders are necessarily provided with the ability to request that an infringing use of their work on an online service be discontinued. This ability and the responsibilities of online service providers in relation to these requests are defined in Article 103, ‘Discontinution of Reproduction or Interactive Transmission’ of the Copyright Act as follows:

(1) Any person who claims that his copyrights or other rights protected under this Act are infringed upon due to the reproduction or interactive transmission of works, etc. by the use of services provided by an online service provider (hereinafter referred to as “claimant” in this Article) may request such online service provider to cease the reproduction or interactive transmission of such works, etc. after providing evidence for such fact.

(2) In those cases where it is requested to stop reproduction or interactive transmission pursuant to foregoing Paragraph (1), an online service provider shall immediately stop the reproduction or interactive transmission of such works, etc. and give notice thereof to the person who reproduces or interactively transmits such works, etc. (hereinafter referred to as “reproducer/interactive transmitter”) and the claimant of such request.

(3) In those cases where a reproducer/interactive transmitter, who is notified pursuant to foregoing Paragraph (2), proves that his reproduction or interactive transmission is based on legitimate

141 Ibid.
rights and requests resumption of the reproduction or interactive transmission of works, etc., the online service provider shall promptly notify the claimant of such request for resumption and a scheduled date of resumption, and resume the reproduction or interactive transmission on such scheduled date.

(4) An online service provider shall designate a person who will be responsible for receiving requests to stop or resume reproduction or interactive transmission pursuant to foregoing Paragraphs (1) and (3) (hereinafter referred to as “receiver” in this Article) and make a public announcement thereof to allow those who use his facilities or services to easily have knowledge thereof.

(5) In those cases where an online service provider makes a public announcement pursuant to foregoing Paragraph (4), and stops or resumes the reproduction or interactive transmission of works, etc. pursuant to foregoing Paragraphs (2) and (3), such online service provider’s liability for the infringement by other persons on copyrights and other rights protected under this Act as well as the damages incurred upon the reproducer/interactive transmitter may be reduced or waived: provided that said provision shall not apply to any liability incurred from the time when such online service provider gains knowledge of the fact that copyrights and other rights protected under this Act are infringed upon due to reproduction or interactive transmission of works, etc. by other persons to the time when a request to stop reproduction or interactive transmission pursuant to foregoing Paragraph (1) is made.

(6) Any person who requests that the reproduction or interactive transmission of works, etc. be stopped or resumed in accordance with foregoing Paragraphs (1) and (3) without any legitimate rights shall make compensation for any damages incurred thereby.

(7) The matters necessary for provision of evidence, suspension, notification, resumption of reproduction or interactive transmission, designation of a receiver of notices, public announcement, etc. pursuant to foregoing Paragraphs (1) to (4) shall be set forth by Presidential Decree. In such case, the Minister of Culture, Sports and Tourism shall engage in prior consultation with the heads of the appropriate central administrative authorities.142
Operators of service that allow the sharing of data among their users without any interaction with the service provider such as peer-to-peer file sharing services are considered a ‘Special Online Service Provider’. These providers have additional responsibilities under copyright laws, such as the use of technical measures to intercept the illegal transmission of copyright works. The additional responsibilities are defined in Article 104, “Liability, Etc. of Special Types of Online Service Providers” of the Copyright Act as follows:

(1) Online service providers whose main purpose is to enable different people to interactively transmit works, etc. among themselves by computers (hereinafter referred as “special types of online service providers”) shall take necessary measures such as technological measures for intercepting illegal interactive transmission of works, etc. upon the requests of rights holders. In such cases, matters related to requests of rights holders and necessary measures shall be set forth by Presidential Decree.

(2) The Minister of Culture, Sports and Tourism may determine and notify the scope of special types of online service providers in accordance with Paragraph (1). 143

The Council of Europe Convention on Cybercrime provides measures to ensure that the protection of copyright and related rights as defined in the Bern Convention for the Protection of Literary and Artistic Works, the WTO the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty. 144 Korea is a party to these international agreements and has updated its legislation to protect these rights in the case that they are violated by means of information and communications technology. 145 The measures provided in the CoE Convention on Cybercrime are intended for the use of criminal sanctions only in cases of piracy on a commercial scale, but allows that states implement laws criminalizing types of infringement other than commercial. 146 The Korean provisions arguably go far beyond this. However, practical applications of the criminal provision of copyright law have shown degrees of restraint by the prosecutor's office. 147 The

---

142 Ibid. art 103
143 Ibid. art 104
144 (Council of Europe n.d.)[110]
145 (WIPO 2013)
146 (Council of Europe n.d.)
provisions in Korean law for copyright and related rights are designed to meet the obligations of the international treaties to which Korea is a party, extend these protections into the online environment and provide guidance on the management of author’s and related. For this reason we understand that the Korean law is in harmony with the CoE Convention on Cybercrime provisions for copyright.

E. Ancillary liability and sanctions

(1) Attempt and aiding or abetting

Article eleven of the CoE Convention on Cybercrime provides measures for the attempt and the aiding or abetting of a cybercrime as follows:

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.148

The measures aim to criminalize the aiding or abetting of a cybercrime, however they are designed to fall short of implicating Internet or online service providers even though they act as a conduit to criminal activity as a service provider without criminal intent is not liable and consequently not required to monitor the use of their service to avoid criminal liability.149

The Criminal Act of Korea provides measures for the aiding or abetting of a criminal act in section three, ‘Complicity’ as follows:


148 Convention on Cybercrime (Council of Europe) 2001 art 11

149 (Council of Europe n.d.)
Article 30 (Co-principles)
When two or more persons have jointly committed a crime, each of them shall be punished as a principle offender for the crime committed.

Article 31 (Instigator)
(1) For a person who instigates another to commit a crime, the same punishment shall be applied to the instigator as one who actually commits the crime.
(2) When a person is instigated and consents to carry out a crime but does not reach the commencement stage for the commission thereof, the punishment for conspiracies or preparations thereof shall apply mutatis mutandis to the instigator and the instigated person.
(3) Even though the instigated person does not consent to the commission of a crime the preceding paragraph shall apply to the instigator.

Article 32 (Accessories)
(1) Those who aid and abet the commission of a crime by another person shall be punished as accessories.
(2) The punishment of accessories shall be mitigated to less than that of the principals.

Article 33 (Complicity and Status)
To a person who collaborates in the commission of a crime in which a person’s status is an element the provisions of the preceding three Articles shall apply even though that person lacks such status: Provided, That when the severity of a punishment varies with the accused’s status, the heavier punishment shall not be imposed on that person who lacks such status.

Article 34(Principle through Innocent Human Agent and Aggravation of Punishment for a Particular Instigation or Aiding and Abetting)
(1) A person who commits a crime by instigating or aiding and abetting another who is not punishable for such conduct, or who is punishable as an offender through negligence, shall be punishable in accordance with the provision for an instigator or accessory.
(2) A person who causes the results envisaged in the preceding paragraph by instigating or aiding and abetting another person
who is under his control and supervision, shall be punished by increasing one half of the maximum term of maximum amount of penalty provided for the principal in the case of instigating, and with the penalty provided for the principal in the case of aiding and abetting.\textsuperscript{150} (Criminal Act 2005(Korea) Section III)

The CoE Convention on Cybercrime measures criminalizing the attempt to commit a crime provides great flexibility in the implementation of this measure to maximize the ease of adopting the convention.\textsuperscript{151} Korea law criminalizes the attempt of criminal acts, including those concerning computer systems.

Specifically, section two of the General Provisions in the Criminal Act of Korea provides measures for the attempt of criminal offenses as follows:

Article 25(Criminal Attempts)
(1) When an intended crime is not completed or if the intended result does not occur, it shall be punishable as an attempted crime.
(2) The punishment for attempted crime may be mitigated than that of consummated crime.

Article 26 (Voluntarily Ceased Crime)
When a person voluntarily ceases his criminal act which he began or prevents the result of the culmination thereof, the punishments shall be mitigated or remitted.

Article 27 (Impossible Crime) Even though the occurrence of a crime is impossible because the means adopted for the commission of the crime or because of mistake of objects, the punishment shall be imposed if there has been a resulting danger but the punishment may be mitigated or remitted.

Article 28 (Conspiracy and Preparation)
When a conspiracy or the preparatory actor for a crime has not reached commencement stage for the commission of the crime, the person shall not be punishable, except as otherwise provide by Acts.

\textsuperscript{150} Criminal Act (Korea) 1953 Section 3 arts 30-34
\textsuperscript{151} (Council of Europe n.d.)
Article 29 (Punishment of Attempts)
The punishment for attempted crimes shall be specifically provided in each Article concerned.\textsuperscript{152}

The Korean legislation matches the requirements of the CoE Convention on Cybercrime in regards to provisions for the aiding and abetting of cybercrime as well as the attempt at cybercrime. Korean legislation could be considered as being in harmony with the Convention on Cybercrime in this respect.

(2) Corporate liability

Article twelve of the CoE Convention on Cybercrime provides measures for corporate liability as follows:

1) Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:
   a) a power of representation of the legal person;
   b) an authority to take decisions on behalf of the legal person;
   c) an authority to exercise control within the legal person.

2) In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3) Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4) Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.\textsuperscript{153}

\textsuperscript{152} Criminal Act (Korea) 1953 Section 2 arts 25-29
\textsuperscript{153} Convention on Cybercrime (Council of Europe) 2001 art 12
The constitutional court of Korea decided in November of 2007 that a legal person cannot be held responsible for a crime where the law did not specify such a responsibility.\(^{154}\) This decision was made based on the rational that doing so would violate a fundamental principle of Korean law; that anyone without responsibility for an act cannot be criminally punished.\(^{155}\) Following this decision, the punishment of legal persons for criminal acts has not been deemed unconstitutional if the law stipulates a responsibility. Consequently, legal persons or corporations are punishable by laws that specifically mention such a responsibility.\(^{156}\) In the case of Cybercrime, legal persons can be held criminally liable for acts against the machine and content related crime.

The PICNUIP Act provides a specific measure by stipulating joint penal provisions for legal persons and individuals involved in a criminal act. Article 75 of the Act, Joint Penal Provisions states:

> If a representative of a corporation, or an agent, an employee, or other servant of the corporation commits a violation under Articles 71 through 73 or 74 (1) in connection with the business of the corporation or the individual, not only shall such violator be punished accordingly, but the corporation or the individual shall be punished by a fine under the relevant Article: Provided, That this shall not apply where the corporation or individual has not been negligent in giving the due attention and supervision concerning the relevant duties to prevent such violation.\(^{157}\)

Consequently, a corporation is liable to be fined where an agent, employee or other servant of the corporation commits a crime of illegal access, data interference, system interference, or misuse of devices (i.e. a crime against the machine).

Similar provisions have also been made regarding content-related crimes of copyright and related rights infringement and child pornography offences.

---

154 See 19-2 KCCR 520, 2005 Hun-Ka 10. 2007, Nov. 29 [Constitutional Court (Korea) Trans. http://search.ccourt.go.kr/ths/pr/eng_pr0101_E1.do?seq=1&cname=%EC%9B%88%EB%AC% B8%ED%8C%90%EB%A1%80&eventNum=14836&eventNo=2005%ED%97%8C%EA%B0%8 010&pubFlag=0&ctId=010400]

155 Ibid. P176

156 Ibid.P175-176

157 Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc. (Korea) 2001 art 75
Article 141 of the Copyright Act of Korea provides joint penal measures as follows:

If a representative of a legal person, or an agent, employee, or other employed persons of a legal person or an individual has committed a crime as prescribed under this Chapter with respect to the affairs of the legal person or the individual, the fine prescribed under each of the Articles concerned shall be imposed on such a legal person or an individual in addition to the punishment of the offender: provided that this provision shall not apply if the legal person or individual was not idle in considerable attention and supervision.158

Consequently, a corporation is liable to be fined where an agent, employee or other servant of the legal person commits a crime concerning the infringement of copyright or related rights.

In regards to child pornography offenses Article 20 of the ‘Act on the Protection of Children and Juveniles from Sexual Abuse’ states joint penal provisions as follows:

If the representative of a corporation, or an agent, employee or any other employed person of a corporation or an individual commits an offense prescribed under any of Articles 8 (3) and (4), 11 (3) and 12 (2) and (3) in connection with the business of the corporation or individual, not only shall such offender be punished accordingly, but the corporation or individual shall also be punished by the fine prescribed in the relevant provisions, and if such person commits an offense prescribed under any of Articles 8 (1), (2), (5) and (6), 9, 11 (1), (2) and (4) and 12 (1), not only shall such offender be punished accordingly, but the corporation or individual shall also be punished by a fine not exceeding 50 million won: Provided, That the same shall not apply where the corporation or individual has not neglected to exercise due diligence and supervision for the relevant duties in order to prevent such offense.159

As stated in this article, a corporation is potentially criminally liable to be fined where an agent, employee, operative of the company, or an individual

---

158 Copyright Act (Korea) 2009 art 141
159 Act on the Protection of Children and Juveniles From Sexual Abuse (Korea) 2009 art 20
acting in connection with the corporation commits an offence related to child pornography. In the case of offences that do not have a specified fine requiring the imprisonment of an offender, a corporation shall be punished by a fine not exceeding 50 million won.\textsuperscript{160}

Korean law is largely congruent with the CoE Convention on Cybercrime in regards to corporate liability as legal persons involved in crimes against the machine and content-related crimes are punishable. It must also be mentioned that the decision of the constitutional court on the application of criminal penalties to legal persons does not affect the possibility of civil action against such persons in the case of computer assisted crimes.

\textbf{F. Sanctions and measures}

Article thirteen of the CoE Convention on Cybercrime provides that the measures against cybercrime as defined in articles two through eleven are punishable by dissuasive sanctions, including incarceration as follows:

1) Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2) Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.\textsuperscript{161}

The Convention on Cybercrime requires that the cybercrime offences defined in article two through eleven be punishable under criminal law with sanctions that are effective, proportionate and dissuasive’ and include prison sentences. As shown in the table below, Korean law provides the possibility of imprisonment for all of the listed offenses with the exception of the possession of child pornography. The majority of crimes also include an alternative fine payable in Korean Won (KRW).

\textsuperscript{160} Ibid.

\textsuperscript{161} Convention on Cybercrime (Council of Europe) 2001 art 13
<table>
<thead>
<tr>
<th>Offence</th>
<th>Imprisonment</th>
<th>Maximum Fine (KRW)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Against the Machine</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Illegal Access</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc. (Korea) 2001 art 63.1.1 Prohibition on Intrusive Acts</td>
<td>max 3 years</td>
<td>30,000,000</td>
</tr>
<tr>
<td><strong>Data Interference</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc. (Korea) 2001 2011 art 71.10 Prohibition on Intrusive Acts</td>
<td>max 3 years</td>
<td>30,000,000</td>
</tr>
<tr>
<td>Criminal Act (Korea) 1953 art 141.1 Criminal Act Destruction of Public goods.</td>
<td>max 7 years</td>
<td>10,000,000</td>
</tr>
<tr>
<td>Criminal Act (Korea) 1953 art 366 Destruction and Damage, etc. of Property</td>
<td>Max 3 years</td>
<td>7,000,000</td>
</tr>
<tr>
<td><strong>System Interference</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Act on the Protection of Information and Communications Infrastructure (Korea) 2009 art 28 Critical Information Infrastructure</td>
<td>Max 10 years</td>
<td>100,000,000</td>
</tr>
<tr>
<td>Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc. (Korea) 2001 art 71.10 Prohibition on Intrusive Acts</td>
<td>max 3 years</td>
<td>30,000,000</td>
</tr>
<tr>
<td><strong>Misuse of Devices</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc. (Korea) 2001 art 71.9 Transmitting or distributing malicious programs</td>
<td>max five years</td>
<td>30,000,000</td>
</tr>
<tr>
<td><strong>Computer Related Offences</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Computer Related Forgery</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criminal Act (Korea) 1953 art 225 Counterfeit or Alteration of Official Documents</td>
<td>max 10 years</td>
<td>None</td>
</tr>
<tr>
<td>Criminal Act (Korea) 1953 art 226 Drafting in False Capacity</td>
<td>max 10 years</td>
<td>None</td>
</tr>
<tr>
<td>Criminal Act (Korea) 1953 art 227 Preparation of False Document</td>
<td>max 10 years</td>
<td>None</td>
</tr>
<tr>
<td>Criminal Act (Korea) 1953 art 227.2 False Preparation or Alteration of Public Electromagnetic records</td>
<td>max 10 years</td>
<td>None</td>
</tr>
<tr>
<td>Offence</td>
<td>Imprisonment</td>
<td>Maximum Fine (KRW)</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>--------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Criminal Act (Korea) 1953 art 229 Uttering False Public Document</td>
<td>max 10 years</td>
<td>None</td>
</tr>
<tr>
<td>Criminal Act (Korea) 1953 art 228.1 Untrue Entry in Authentic Deed</td>
<td>max 5 years</td>
<td>10,000,000</td>
</tr>
<tr>
<td>Criminal Act (Korea) 1953 art 231 Counterfeit or Alteration of Private Document</td>
<td>max 5 years</td>
<td>10,000,000</td>
</tr>
<tr>
<td>Criminal Act (Korea) 1953 art 232 Drafting Private Document in False Capacity</td>
<td>max 5 years</td>
<td>10,000,000</td>
</tr>
<tr>
<td>Criminal Act (Korea) 1953 art 232.2 Falsification or Alteration of Private Electromagnetic Records</td>
<td>max 5 years</td>
<td>10,000,000</td>
</tr>
<tr>
<td>Criminal Act (Korea) 1953 art 234 Uttering False Private Documents</td>
<td>max 5 years</td>
<td>10,000,000</td>
</tr>
</tbody>
</table>

**Computer Related Fraud**

<table>
<thead>
<tr>
<th>Offence</th>
<th>Imprisonment</th>
<th>Maximum Fine (KRW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal Act (Korea) 1953 art 227.2 Manipulating public electromagnetic records</td>
<td>max 10 years</td>
<td>None</td>
</tr>
<tr>
<td>Criminal Act (Korea) 1953 art 232.2 Manipulating private electromagnetic records</td>
<td>max five years</td>
<td>10,000,000</td>
</tr>
<tr>
<td>Criminal Act (Korea) 1953 art 347.2 Fraud by means of computers</td>
<td>max 10 years</td>
<td>20,000,000</td>
</tr>
<tr>
<td>Criminal Act (Korea) 1953 art 314.2 Interference with Business by computer</td>
<td>max 5 years</td>
<td>15,000,000</td>
</tr>
</tbody>
</table>

**Content Related Offences**

**Child Pornography**

<table>
<thead>
<tr>
<th>Offence</th>
<th>Imprisonment</th>
<th>Maximum Fine (KRW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Act on the Protection of Children and Juveniles From Sexual Abuse (Korea)2009 art 8.1 Production, import or export</td>
<td>min 5 years</td>
<td>None</td>
</tr>
<tr>
<td>Act on the Protection of Children and Juveniles From Sexual Abuse (Korea)2009 art 8.2 Commercial distribution or exhibition</td>
<td>max 7 years labour,</td>
<td>None</td>
</tr>
<tr>
<td>Act on the Protection of Children and Juveniles From Sexual Abuse (Korea)2009 art 8.3 Distribution or exhibition</td>
<td>max 3 years</td>
<td>20,000,000</td>
</tr>
<tr>
<td>Act on the Protection of Children and Juveniles From Sexual Abuse (Korea)2009 art 8.4 Possession</td>
<td>None</td>
<td>20,000,000</td>
</tr>
<tr>
<td>Act on the Protection of Children and Juveniles From Sexual Abuse (Korea)2009 art 8.5 child recruiting for pornography</td>
<td>min 1 year / max 10</td>
<td>None</td>
</tr>
</tbody>
</table>
As the CoE convention provides no specific requirements or precise definitions for the provision of sanctions other than the possibility of deprivation of liberty or a monetary fine it is difficult to ascertain the degree to which Korean legislation satisfies the requirements of the convention. Korean law does provide imprisonment for all cybercrimes with the exception of the possession of child pornography. The above table provides an easy reference as a basis of comparison between the sanctions allowed under Korean law and the enacted sanctions of other countries.

### VII. CONCLUSION

The provision of additional communication instruments may provide a foundation for better interactions between the cybercrime investigators of different nations where language and cultural differences impede cooperation. The CoE Convention on Cybercrime, by virtue of being developed from an understanding based on practical and universal aspects of investigation and technology provides a system of classifying and comparing cybercrime legislation. This report provides a classification by means of the CoE Convention on Cybercrime of the cybercrime laws of Korea in order to demonstrate the level of harmony between the substantive law described in the convention and legislation already existing in an a nation external to the convention. Despite some minor differences, Korean law provides an equivalent legal instrument for all of the substantive laws described in the Convention. There is therefore little issue
with a lack of dual criminality presenting an obstacle to transnational cybercrime investigations between Korea and signatories to the Convention on Cybercrime. We feel that the CoE Convention on Cybercrime has value as an instrument in harmonizing efforts between countries as it can provide a basis for enabling and improving communication at a practical level.
REFERENCES

Aquilina, James; Casey, Eoghan; Malin, Cameron; Rose, Curtis “Malware Forensics: Investigating and Analyzing Malicious Code”. Syngress Publishing Burlington, 2008


Constitutional Court of Korea, 19-2 KCCR 520, 2005 Hun-Ka 10. 2007, Nov. 29 [Constitutional Court (Korea) Trans. http://search.ecourt.go.kr/ths/pr/eng_pr0101_E1.do?seq=1&cname=%EC%98 %81%EB%AC%B8%ED%8C%90%EB%A1%80&eventNum=14836&eventNo =2005%ED%97%8C%EA%B0%8010&pubFlag=0&cId=010400]

The Equivalence of Korean Cybercrime Law to the Council of Europe Convention on Cybercrime


International Telecommunications Union, “ITU Cybercrime Legislation Resources:


Legislation


Act On The Prevention Of Sexual Assault And Protection, Etc. Of Victims Thereof (Korea) 2011 [Ministry of Government Legislation (Korea) trans. http://www.moleg.go.kr/lawinfo/engLawInfo?pstSeq=58519&searchCondition=AllForEngLaw&searchKeyword=%EC%84%B1%ED%8F%AD%EB%A0%A5]


Digital Signature Act (Korea) 2009 [Ministry of Government Legislation (Korea) trans.
Cybercrime in the Republic of Korea

http://www.moleg.go.kr/lawinfo/engLawInfo?pstSeq=52443&searchCondition=AllForEngLaw&searchKeyword=%EC%A0%84%EC%9E%90

Game industry Promotion Act (Korea) 2006 [Korean Legislation Research Institute trans.]
http://elaw.klri.re.kr/eng_service/lawTotalSearchABC.do?param=G

Internet Multimedia Broadcasting Business Act (Korea) 2008 art 27(5) [Ministry of Government Legislation (Korea) trans.]
http://www.moleg.go.kr/english/korLawEng?pstSeq=47561

Law on the protection and use of location information (Korea) 2008 [Ministry of Government Legislation (Korea) trans.]
http://www.law.go.kr/engLsInfoPWah.do?lsiSeq=85238

Personal Information Protection Act (Korea) 2011 [Korean Legal Information Institute trans.]
http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf

Protection of Communications Secret Act (Korea) 1993 [Seoul Electronic Commerce Center trans.]
http://ecc.seoul.go.kr/eng/03_data/law_popup2.asp?vnum=8&tab=0&ary=law Data

Telecommunications Business Act (Korea) 2008 Arts 54 and 69 [Ministry of Government Legislation (Korea) trans.]
http://www.moleg.go.kr/english/korLawEng?pstSeq=47567

http://www.moleg.go.kr/lawinfo/engLawInfo?pstSeq=52442&searchCondition=AllForEngLaw&searchKeyword=%EC%A0%84%EC%9E%90

Use and Protection of Credit Information Act (Korea) 2009 [Ministry of Government Legislation (Korea) trans.]
http://www.moleg.go.kr/english/korLawEng?pstSeq=52589
THE CURRENT TRENDS OF VOICE PHISHING FRAUD: LEGISLATION AND POLICY IMPLICATION

Yoon, Hae Sung *

I. INTRODUCTION

Voice phising fraud crime is thriving as its techniques have become more sophisticated and intelligent. Recently, loan fraud, such as card loan, etc., in variant forms of voice phising, is causing harm in many cases¹, and this had amplified public awareness in regards to legislative supplementation and intensification of punishment. In fact, there have only been two cases in Korea where an offender of tele-financial fraud disguised as a kidnapper was sentenced 2 years and a collector of bank accounts was sentenced 1 year and 6 months² after their charges, such as fraud, attempted fraud, violation of electronic financial business law, etc., were recognized and so were their complicity and participation in the crime. Also, in the case of card loan fraud, because its techniques are clever and evolving over time, lower instance cases are hard to find. And, because voice phising has a characteristic of an international crime, unless the principal offender is apprehended, it would be difficult to find Supreme Court cases of tele-financial fraud due to having structural and systematic limitations.

Due to such reasons, the present regulations are limited in its implementation considering how voice phising fraud crimes are becoming more clever and

¹ The government had cracked down on 26,700 people who infringed upon the lives of citizens (voice phising, etc.) between last March and June (Asia Economy, 23th July, 2013), and according to the regular briefing of the Financial Supervisory Service, there were 32,996 cases and 15,551 people that were affected by financial fraud, such as voice phising, pharming, etc., using the financial payment system. The average damage incurred to an individual is 9,920,000won (Credit TV, July 2).
intelligent, which is why regulating more broadly is essential for the relief of the victims. False pretenses cannot be applied to voice phishing fraud crimes because there is no act of disposition of property by victims’ error, and the victims do not recognize the wire transfer that’s been made. Therefore, establishing a new rule of punishment should be reviewed which conforms to false pretenses of the Special Act.

Consequently, seeing that there is more need to seek for legal and institutional directions on practical issues along with comparative legal approach than case analysis, this report will review 1) the revision of regulations that could cover the crimes of variant voice phishing frauds such as card loan, cash service, bank credit loan, etc., and 2) the validity of establishing a new special penalty clause targeting the criminals of voice phishing fraud and its sentencing guidelines and to seek for the direction of legal system. International trends will be examined for this purpose and its major implications will be reflected in the legal system for review.

II. REVIEW OF AMENDMENT DIRECTION ON THE DEFINITION OF REGULATION FOR VOICE PHISHING FRAUD CRIME

A. Understanding National and International Trends and Analysis of Types

(1) National Trends and Analysis of Types

Recently, mortgage frauds prevailed by luring victims to similar web pages to demand personal and financial information for card loans and by promising to grant loans through advertisements, etc., after which the scammers request for money and disappear with it. Looking at the procedure of the card loan fraud, the scammers lure victims to a fake web page and make them enter their personal and financial information to get loans.³ The scammers then use that personal and financial information to access the real web page or ARS to legally request for loans after which they withdraw the money from the victims’ accounts and disappear. In the case of loan fraud, victims apply for loans by being deceived by the scammer’s advertisements, and the scammer requests for money in the

³ In the case of using a phishing site, most loan applications are made by getting the new authentication code and with the victim’s name or through ARS with the credit card information obtained from the phishing site.
name of credit deposit, after which the scammer disappears with the money that was transferred by the victims.

(2) International Trends and Analysis of Types

As fraud methods diversify in Japan, the Japanese Police Department decided to call voice phishing as ‘furikomi’\(^4\) fraud in December 2004,\(^5\) and as more diversified types of fraud came about in the recent years, the new term ‘special fraud’ covers both the ‘furikomi fraud’ and the ‘fraud similar to furikomi’. Special fraud refers to all frauds that use telecommunications to make victims transfer money to disguised accounts or through other methods while having never met the victims.\(^6\)

In Taiwan, it was common to use the method of deceiving people by saying that they are entitled to a tax return or pension, or that they have won a lottery or a prize. Other methods, such as threatening with basic information, were used as well.\(^7\)

(3) Analysis of Problems Raised from Analysis of Types

The recent method of card loan fraud is skillfully using the card loan service of financial institutions by getting the loans with the personal and financial information (security card numbers) that was gathered through a fake web page that is similar to the genuine web page of financial institutions. In other words, in order to use the card loan service of financial institutions, the scammers establish a fake or a similar web page and collects personal and financial information and apply for card loan as a disguised applicant and takes the money. The fact that sophisticated

\(^4\) ‘Furikomi’ is originated from the expression ‘deposit the money’.


\(^7\) Usually, the main offenders are members of Jukryunbang, and it is managed by Taiwanese in charge (mainly members of Sahaebang), a call center management team, domestic account opening team (fake account collection), cash withdrawal team, etc. The account opening team enters into a country with the valid passports and opens accounts with forged passports received from Taiwan or China by mail, and the cash withdrawal team withdraws money from the receiving account or transfers the money to another account for withdrawal and delivers it to the remittance team, which then delivers it to Taiwan or China to the people in charge for distribution. (Japanese Police Detective Bureau - 「Shinmoon Koishin」, January 7\(^{th}\), 2009).
security procedures and identity clearance do not take place in such a case was abused in this method.

**B. Review of National and International Definition of Regulation**

**(1) Understanding National Legislations**

Under the domestic legislations, voice phishing fraud is categorized as a telecommunication financial fraud. Article 2 of the Special Act on Return of Damages by Telecommunication Financial Fraud states that, "telecommunication financial fraud is act using the telecommunications, as stated in Article 2, paragraph 1 of the Framework Act on Telecommunications, to gain profit in property by deceiving and threatening unspecified individuals or to have a third person gain profit in property by having remit and transfer money, and to have remit and transfer money by using personal information. It excludes, however, the acts disguised as supplying goods and services".

As it shows in the Special Act, acts disguised as supplying goods and services are excluded from the definition of telecommunication financial fraud, hence, bank services such as card loan service cannot be included as the object of relief because it is about providing service. Also, loan fraud and commodity fraud are not covered by the definition of telecommunication financial fraud of the Special Act. This provisory clause was inserted during the legislation process to prevent the abuse of payment suspension from being extended to delay in shipment or supply of service, and it excludes general commodity sale fraud, etc., as legislators did not want suspension of payment to be too broadly interpreted. Currently, however, it is the victims who experience the damage caused by fraud, which is done by abusing the system.

**(2) Understanding International Legislations**

In the case of Japan, the ‘Act on Damage Recovery Benefit Distributed from Fund in Bank Accounts Used for Crimes (hereinafter ‘Furikomi Fraud Aid Act’), which corresponds to Korea’s Special Act, is put into place. Article 2

---

8 It was regulated for the payment suspension to be expanded and not be abused based on the electronic commerce, etc.. National Assembly Secretariat, the State Affairs Committee Meeting Minutes (Legislative Bill Examination Subcommittee), 294th Meeting Minute of National Assembly, 10th Sep. 2010.
of the Act states that “criminal acts using the wire transfer’ (hereinafter ‘deposit’) refer to fraud and other property infringement committed to obtain others’ property as methods to have victims send money to the savings account, etc. Paragraph 5 of Article 2 defines ‘damage recovery dividends’ as “funds paid by financial institutions at the amount equivalent to extinguished savings or savings-related bonds, which is the amount of loss incurred by criminal acts using wire transfer”. As appears in this provision, ‘funds equivalent to extinguished savings or savings-related bonds’ are the actual amount of money in the transferred bank account, etc. In order for such bonds (accounts) to be considered as ‘damage recovery dividends’, the Act states that they have to be paid by financial institutions and be incurred by criminal acts using wire transfer. Therefore, damage recovery dividends are seen as bonds in Japan, and it should be paid by financial institutions and be the lost property incurred by ‘criminal acts using wire transfer’.  

Thus, it can be interpreted that victims are eligible for relief even if unauthorized person withdraws or transfers money for getting the service of financial institutions (card loan, loan), or closes savings account or bonds and withdraws the money to transfer to another account, or cancels insurance and transfers the money to another account and the financial institutions pay for the damages of transferred account, etc., which is used for criminal acts using wire transfer. The reason is because ‘criminal acts using wire transfer’ are considered broadly as crimes of gaining another person’s property by infringing upon the property. The important element here, however, is that the wire transfer needs to be made. The wire transfer is broadly defined by covering the methods of transferring money from victim’s account including depositing and transferring of money at the ATM. Therefore, in the case of Japan, if the Act was legislated to relieve the damage incurred by telecommunication financial fraud through the damage recovery dividends, it can be said that the broad scale of damage recovery dividends was implemented for relieving the victims while acknowledging the fact that the wire transfer, etc., is done by tele-financial fraud crime and that the most services are related to financial institutions.

9 The ‘Furikomi Fraud Aid Act’ was enacted on 21st December 2007 and its purpose is stated in Article 1, which states that it was designed to quickly recover the damages of property for the victim of fraud by providing damage recovery dividends.

10 Therefore, damage recovery dividends do not apply to cases when the money was transferred from non-financial institutions or when the damage in property was incurred by crimes other than the crime using the wire transfer.
In the United States, there is a regulation in 18 U.S.C. Chapter 113A, which regulates telemarketing fraud, and §2325 excludes commodity purchase by catalog and defines telemarketing fraud as ‘(a) purchases of goods or services, (b) participation in conference, horse racing, lottery, or (c) charitable donation and contribution or financial donation or other valuables using the telephone’. Also, 18 U.S.C. Chapter 113A §2326 defines additional punishments. In the case of Utah state, the Senate Bill 52, which was enforced on May 1st, 2006, solely has criminal punishments regarding anti-phishing and states that “any person who has devised object or purpose of the scheme or artifice to defraud for obtaining sensitive personal identifying information, regardless of the value is guilty of a second degree felony”. It also states that “sensitive personal identifying information” means information regarding an individual’s social security number, driver's license number, automated or electronic signature, unique biometric data, and any other information that can be used to gain access to an individual’s financial accounts or to obtain goods or services.

C. Seeking an Amendment Direction

As it shows in the case studies, the commonly used method of obtaining victim’s property is using personal information that is hacked to establish a phishing website and pretending to protect the account or information and to provide loan service. Financial services such as card loan, loan fraud, and insurance refund have the special characteristic of objectifying the usage and supply of services of the financial institutions. In order to relieve damages incurred by subjects of refund (loan fraud), it is persuasive to delete the part in the conditional regulation where it says acts disguised as providing service. However, telecommunication financial fraud can be abused when delivery or service is simply delayed, hence, a careful consideration should be made.

The cases of US and Japan provide implications to Korea as they define the fraud types in detail or apply the components in broad scale. Nevertheless, there is a difference between the two States as the US defines and regulates only the telemarketing fraud and the purchase of

12 Utah Code Ann. §76-10-1801 –Communication Fraud, Penalties (http://le.utah.gov/~code/TTITLE76/htm/76_10_180100.htm)
goods or services while Japan broadly defines and regulates deposit fraud when it is used regardless of supply of goods or services. What is clear is that the fraud is done by using the telephone, and because the methods of telecommunication financial fraud are evolving and getting more clever, there is a limitation in providing protection with the Special Act of Korea. Therefore, in order to overcome the limitation and to achieve the objective of the Special Act, it should be amended to allow the relief for the victims who are affected by the financial services, etc. To do that, it would be meaningful to consider the method of specifically defining and regulating the acts and preparing corresponding punishments like the US or consider the method of emphasizing the acts and broadly defining and regulating them like Japan.

III. REVIEW OF AMENDMENT DIRECTION ON THE DEFINITION OF PENAL PROVISIONS ON VOICE PHISHING FRAUD CRIME

A. Analysis of Types

It is observed that there are four categories of voice phishing in regards to acts of disposition. First is the ‘compensation type’, which says that the victim is entitled to pension, insurance and tax return, etc., or that the victim had won a prize. Second is ‘protection type’, which lures by saying that it provides protection to the victim from financial information (credit card or bank account related information) being exposed or from crimes. Third is ‘threatening type’, which states that the victim’s child is kidnapped, and fourth is ‘duty imposition type’, which lures to pay fees for alumni reunion or college registration, etc.

In the case of ‘compensation type’ or ‘protection type’, because the crimes are committed by “luring the victim to an ATM to transfer money after providing fake authentication code and the security code of the

13 In the case of voice phishing fraud crime, because there is no face-to-face interaction between the offender and the victim, the victim can only judge according to the words spoken by the offender, and if the victim is not well aware of the electronic finance system or the online security, there is a higher risk for the victim to fall into the trap. (Kim, Sung Un/Yang, Yung Jin, “Evolution of Tele-Financial Fraud Crime: Analysis of Voice Phishing Victim Aid and Response”, Korea Public Security and Administration Society No. 32, 2008, p. 121).
corresponding institution through the telephone”, the victim does not recognize that the money is being transferred to the offender’s account from his or her account. Therefore, an act of disposition by the victim’s error cannot be acknowledged. On the other hand, in the case of ‘threatening type’ or ‘duty imposition type’, offenders use fake bank accounts to lure the victims to transfer money, hence, the victims recognize that they authorize the wire transfer, in which case, the act of disposition is acknowledged.

Also, in the case of phishing and pharming, because offenders identify victims’ personal or financial information through fake (illegal) financial site using phishing and pharming to use it on a real financial website for personal profit in property, the act of disposition cannot be acknowledged. This is because the method of using phishing and pharming obtains personal or financial information by luring the victim to a fake financial website through email or telephone, the method itself cannot be considered to have incurred loss in property. Furthermore, other than using phishing and pharming to obtain personal or financial information, the act of using the information to gain profit in property through wire transfer, etc. cannot be punished as fraud because it is not acknowledged as an act of disposition. Therefore, strictly speaking, an act of obtaining personal and financial information is a pre-phase to fraud, hence, it is questionable whether it can be acknowledged as an act of disposition and loss in property.

**B. Punishment of Fraud Under the Criminal Code**

Because voice phishing fraud is an act of defrauding one’s property, the application of criminal code is a problem. In the Criminal Act, Article 347, paragraph 1 states that “a person who defrauds another, thereby taking property or obtaining pecuniary advantage from another, shall be punished by imprisonment for not more than ten years or by a fine not exceeding twenty million won”\(^\text{14}\), and paragraph 2 states that “the preceding

\[14\] Art. 339 of the Taiwanese Criminal Act states that “a person who by fraud causes another to deliver to him property belonging to such other or to a third person for purpose to exercise unlawful control over other’s property for himself or for a fourth person shall be sentenced to imprisonment for not more than five years or short-term imprisonment; in lieu thereof, or in addition thereto, a fine of not more than one thousand yuan may be imposed”. Also, Art. 339-2 states that “a person who for purpose to exercise unlawful control over other’s property for himself or for a third person takes property of another through an ATM machine shall be sentenced to imprisonment
paragraph shall apply to a person who, by the methods of the preceding paragraph, causes a third person to take property or to obtain pecuniary advantage from the latter”. Therefore, in order for a false pretense to be constituted, defrauding is structurally necessary, and the victim needs to dispose property which leads to loss in property, and the offender obtains profit in property. 15

The problem is whether the act of deceiving the victim to transfer money to the offender’s account by calling the victim on the cell phone and tricking to enter authentication code (= bank account number for criminal usage) and security code (= amount of money to transfer) can be acknowledged as an act of disposition. For example, in case of luring the victim to an ATM for a tax refund, an act of having the victim to enter specific numbers by saying that it is for the purpose of strengthening the security measure becomes questionable whether it constitutes an act of disposition or not if the victim does not recognize the fact that he or she transferred money by error.16 Based on the criminal code, false pretense is consisted of fraud, error, act of disposition of property, damage and profit in property. Therefore, if the victim had entered in information as it was told without recognizing the fact that the money was being transferred, an act of disposition is absent to constitute a false pretense. Hence, under such structure, it is difficult to say that it constitutes a false pretense without an act of disposition.17 Furthermore, regarding the act of obtaining

for not more than three years, short-term imprisonment, or a fine of not more than ten thousand yuan. A person who takes an illegal benefit in property for him or causes a third person to take it by means specified in the preceding paragraph shall be subject to the same punishment”.

15 In the case of Taiwan, as the economy changes and the electronics and telecommunications develop, fake bank accounts and fake phones are used to lure victims to transfer money, and this is clearly a violation of the Chinese Criminal Law and its method has a legal meaning (Song, Su Hwan, “Special Prevention Measure Research on Tele-Financial Fraud”, National Taebuk University Criminology Institute, 2008, p. 20).


17 There is also an opinion that objective loss in property is enough without the act of disposition (Lee, Jae Sang, Criminal Code in Detail, Pakyoungsa, 2004, 18/31; Park, Sang Ki, Criminal Code in Detail, Pakyoungsa, 2005, p. 314). It is saying that if there is an objective loss in property, the tele-financial fraud crime can be punished even if the act of disposition is absent. (Kim, Sung Don, Criminal Code in Detail, SKKUP, 2009, p. 333), (Lim, Woong, Criminal Code in Detail, Bupmoonsa, 2011, p. 367-368), (Oh, Young Geun, Criminal Code in Detail, Pakyoungsa, 2005, p. 402-404), (Supreme Court judgement 1987. 10. 26. 87 Do 1042; Supreme Court judgement 2001. 7. 13. 2001 Do 1289).
personal and financial information, the act itself cannot be punished by the criminal code because there is no profit in property.

C. Indirect Principle Offender of Fraud By Using Computer, etc.

The Criminal Act has a regulation to punish the principal offender who commits a crime through an act of an innocent human agent in Article 34, paragraph 1, which states that “a person who commits a crime by instigating or aiding and abetting another who is not punishable for such conduct, or who is punishable as an offender through negligence, shall be punishable in accordance with the provision for an instigator or accessory.” According to this provision, ‘a person who is not punishable for such conduct’is someone whose action does not constitute a criminal act due to not fulfilling the requirements for a crime such as applicability of elements of crime, illegality, and responsibility. Therefore, whether or not the person who has the victim to enter information at the ATM and gains profit in property is a principal offender, who commits a crime through an act of an innocent human agent, should be considered.

Based on the Criminal Act, a principal offender who commits a crime through an act of an innocent human agent (indirect principal offender) is someone who seemed to be an accomplice or more like an instigator on the surface but is considered to be the principal offender and not an accomplice because the offender uses the victim as a tool by controlling the will.18 In case when refund fraud, among voice phishing fraud crimes, is understood as a form of crime of indirect principal offender, it is true that the existence of direct principal offender becomes somewhat vague as the victim is used as a tool by the offender. Meanwhile, the reason why the indirect principal offender (Criminal Act, Art. 34-1) has the characteristic of principal offender compared to instigator (Criminal Act, Art. 31-1) is because the offender controls the victim’s action to achieve the objective. In the same standpoint, the action control as the sign of the principal offender in accordance with the ‘action control theory’ is recognized as a form of what is known as dominant intention control.19 Therefore, the dominant intention control by the offender towards the victim in the case of refund fraud is not only found in the fraud itself but also in the psychological pressure using the complexity or the

professionalism of the financial information system.

Consequently, in terms of tele-financial fraud crime, when reviewing Article 347-2 of the Criminal Act, if the fact that the offender defrauded the victim who did not recognize the money being transferred is considered as a form of ‘crime of indirect principal offender using the act without structural elements’ and seen as if “the offender gained profit in property by using the victim with the authority to transfer money to a designated account while the offender does not have the authority to transfer the victim’s money at the ATM”, then the victim is used as a tool that does not conform to a structural element (tatbestandslos handelndes Werkzeug), hence, the offender becomes the indirect principal offender of the fraud by use of computer, etc. Therefore, because interpretatively it becomes possible to punish the fraud as the principal through innocent human agent of the fraud by use of computer, there is no need to establish structural elements for each types in the Criminal Act.

D. International Trend

In order to review the validity of establishing special penalty clause regarding voice phishing, the structure of the tele-financial fraud organization needs to be studied and preparing the structural elements needs to be considered and then preparing sentencing guidelines should be followed. First, in the case Taiwan in terms of structural elements, Article 35921 of the criminal code, the crime of acquiring electronic records, is applied to the acts of stealing account passwords, etc. through fake websites or the trojan horse virus, and the act of using the information to log into the bank website to transfer money is considered to be a complete crime, which is punishable under Articles 35822 (Offenses Against the Computer Security) and 339-323 (computer fraud crime) of the criminal

21 Article 359: A person without reason obtains, deletes or alters the magnetic record of another’s computer or relating equipment and causes injury to the public or others shall be sentenced to imprisonment of no more than five years or short-term imprisonment; in lieu thereof, or in addition thereto, a fine of not more than two hundred thousand yuan may be imposed.
22 Article 358: A person who without reason by entering another’s account code and password, breaking his computer protection, or taking advantage of the system loophole of such other accesses his computer or relating equipment shall be sentenced to imprisonment for not more than three years or short-term imprisonment; in lieu thereof, or in addition thereto, a fine of not more than one hundred thousand yuan may be imposed.
23 Article 339-3: A person who for purpose to to exercise unlawful control over other's property
code and could be sentenced up to 3 or 7 years of criminal liability.\textsuperscript{24}

The US severely punishes those who use or obtain personal information without proper authority through 18 U.S.C. § 1028 (fraud and related activity in connection with identification documents, authentication features, and information) (a)(7), which states “whoever knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person\textsuperscript{25} with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law can be fined or sentenced imprisonment for not more than 15 years”.

In terms of sentencing guidelines, the US has a regulation in 18 U.S.C. Chapter 113A §2326 enhanced penalties, which states that “a person who is convicted of an offense under section 1028, 1029, 1341, 1342, 1343, or 1344, or a conspiracy to commit such an offense, in connection with the conduct of telemarketing—

(1) shall be imprisoned for a term of up to 5 years in addition to any term of imprisonment imposed under any of those sections, respectively; and (2) in the case of an offense under any of those sections that— (A) victimized ten or more persons over the age of 55; or (B) targeted persons over the age of 55, shall be imprisoned for a term of up to 10 years in addition to any term of imprisonment imposed under any of those sections, respectively”.\textsuperscript{26} Thus, the US is regulating fraud by its types, and the fact that additional penalty is applied to cases of fraud in connection with the conduct of telemarketing and fraud targeted persons over the age of 55 is found especially interesting. This has an implication to us in regards to fraud.

\textsuperscript{25} ‘Personal Identification Information’ includes (A) name, social security number, date of birth, driver’s licence, resident registration number, permanent residency number, passport number, employee or taxpayer number, and (B) physical characteristics such as finger print, voice print, and retinal image.
\textsuperscript{26} http://codes.lp.findlaw.com/uscode/18/I/113A
When punishment cases are studied in major States in relation to tele-financial fraud, Japan had a case where an organized crime was severely punished for deposit fraud and tele-financial fraud.\textsuperscript{27} The organization systematically defrauded under the leadership of a respected authority and gained 146,000,000 ¥, and the offender was sentenced 20 years for violating the Organized Crime Punishment Act (organized fraud), etc.\textsuperscript{28} Also, in the US, there was a case in December 2006, where the head of an organization called RCMP gained from 8 million to 13 million dollars from 500 people over the period of 3 years. The offender was charged with stealing money by using the telephone with other 39 members of the organization, and 22 people in 25 cases were indicted for wire fraud\textsuperscript{29}, mail fraud\textsuperscript{30}, and telemarketing fraud targeting elderly people\textsuperscript{31}. Especially, in case of defrauding elderly people, 10 years of additional penalty may be sentenced if found guilty. In relation to personal and financial information, there was a case in the United Kingdom where the offender stole over 6,500,000 pounds by using credit card information and password received from an unknown person in Russia from 2003 to 2004.

\textsuperscript{27} In the case of voice phishing fraud crime from May 2006 to August 2007, the Court imposed 20 years of imprisonment because the crime was organized and conducted under the leadership of the offender, which is a severe violation of the law (Sankyung Newspaper, 24\textsuperscript{th} March 2010).


\textsuperscript{29} 18 U.S.C §1343 Fraud by Wire, Radio, or Television: Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation occurs in relation to, or involving any benefit authorized, transported, transmitted, transferred, disbursed, or paid in connection with, a presidentially declared major disaster or emergency (as those terms are defined in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122)), or affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

\textsuperscript{30} 18 U.S.C. §1344 Bank Fraud.

\textsuperscript{31} 18 U.S.C. Chapter 113A : Telemarketing fraud, §2326 Enhanced penalties : A person who is convicted of an offense under section 1028, 1029, 1341, 1342, 1343, or 1344, or a conspiracy to commit such an offense, in connection with the conduct of telemarketing (1) shall be imprisoned for a term of up to 5 years in addition to any term of imprisonment imposed under any of those sections, respectively; and (2) in the case of an offense under any of those sections that (A) victimized ten or more persons over the age of 55; or (B) targeted persons over the age of 55, shall be imprisoned for a term of up to 10 years in addition to any term of imprisonment imposed under any of those sections, respectively.
for buying and selling commodities online, and the offender was arrested and sentenced 6 years in prison. Also, in the case of US, there was a case where the offender used a fake email and a website to lure MSN customers to access the website and acquired their MSN account and credit card information for fraud and for getting it to the third person, and the offender was arrested and sentenced 5 years of probation and 6 months of house arrest.32

Also, Patricia Ann Johnson(35) in Memphis was sentenced 5 years in prison on Jan. 26th 2012, according to 18 U.S.C 1028(a)(7)33 for stealing personal and financial information34, and on May 15th 2012, there was a phishing case that used personal information obtained from spam mail and a fake website, which was sentenced 5 years in federal prison with the charges of bank fraud (18 U.S.C. §134435), wire fraud(18 U.S.C §1343), stealing personal and financial information(18 U.S.C §102836), computer fraud·complicity(18 U.S.C §103037), and complicity of money laundering(18 U.S.C §195638).

33 18 U.S.C 1028(a)(7) - Identity Theft : Knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law shall be punished as an offense under paragraph (3) or (7) of such subsection and be fined under this title or ordered imprisonment for not more than 5 years. And, knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents shall be punished by fine and imprisonment or both.
35 18 U.S.C. §1344 Bank Fraud: Whoever knowingly executes, or attempts to execute, a scheme or artifice—
(1) to defraud a financial institution; or
(2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises; shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.
36 18 U.S.C §1028a – Aggravated Identity Theft:
(a) Offenses.—
(1) In general.— Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.
37 18 U.S.C §1030 - Fraud and related activity in connection with computers.
38 USC § 1956 - Laundering of monetary instruments.
Thus, the international trend is to punish severely if the telecommunication fraud crime is considered as the organized crime by sentencing over 20 years, but in case of acquiring personal and financial information, it is punished by sentencing 6 years, which conforms to larceny. The act of accessing a fake website for fraud or providing information is punished by being sentenced 5 years of probation and 6 months of house arrest for committing the crimes of collecting personal information, luring, and information offering, and the crime of stealing personal and financial information can be sentenced 2 years in prison in addition to relevant crimes.

E. Seeking an Amendment Direction

(1) Seeking an Amendment Direction for the Criminal Act

Voice phishing fraud crime occurs without the knowledge of the victim through telecommunications such as telephone, and the victim can judge only the authenticity of the information delivered or the instruction provided because they don’t meet in person. Hence, if the offender lures the victim to an ATM while pretending to be a staff of the Health Insurance Corporation or the National Tax Service and obtains money by instructing the victim to enter the security code or safety code, which are in fact the account number and the amount of money to be transferred, and if the victim was not aware of the fact that the money was being transferred, it becomes difficult to apply the fraud crime because the element of ‘disposition of property’ is not found.\(^{39}\) Therefore, in order to punish such case as a fraud crime, strengthening the structural element in regards to act of disposition could be considered by redefining it as “an act of using false information for fraud to bring damage in the property, or using the act to enter information without authority to obtain profit in property or to have the third person obtain the profit”. Also, in order to punish all types of tele-financial fraud as fraud crimes, damage in property needs to be defined but acknowledged when there is an objective damage. However, because granting of property in some voice phishing fraud types is done as a proper duty or obligation, it is difficult to acknowledge it as profit in property.\(^{40}\) Even with such point taken into consideration, if

---


40 The investigation is done while acknowledging the fact that the damage of the victim incurs when the offender or the third person obtains profit in property because in practice, the damage incurs
punishment is possible as principal through innocent human agent of the fraud crime using computer, etc., amending the Criminal Code regarding voice phishing is not necessary.

(2) Amendment Direction for the Special Act

Because the objective and the contents of current ‘Special Act on Return of Damages by Telecommunication Financial Fraud’ are focused on the relief of the victim, if the Act was amended to punish the offender, it not only contradicts to the objective of the Act but also shows systematic contradiction. Therefore, in order to establish new penalty clauses to punish the offender, the name and the objective of the Act should be changed. The current Act, which was legislated for the relief of the victim, should change its name to ‘Special Act on Prevention and Return of Damages by Telecommunication Financial Fraud’ if its focus is on both punishment and relief. Then, the types and the penalty clauses should be specifically provided in accordance with the principle of clarity. Meanwhile, the direction of penalty clauses can be considered from different angles. First, as it shows in foreign legislation cases, if telecommunication financial fraud is separated with telecommunication financial threat, etc., or punished as fraud crime, the structural element can be subdivided by types of act or methods prefiguratively or enumeratively. Second, even if the title and the objective of the Special Act are changed and amended to reflect the will to punish tele-financial fraud crimes, in order to overcome the systematic limitations of the current legal system, it should be considered to regulate and punish the act of luring someone to transfer money as the crime of objective or the crime of risk despite the fact that there is no act of disposition in property. This can be done by putting in specific examples in the provisions of the Act based on the ‘objective’ of obtaining profit in property through tele-financial fraud, and it will strengthen the regulations for pre-stage voice phishing fraud crimes such as creating fake or similar websites to collect personal and financial information or helping to get a loan for the purpose of taking the commission.

Also, preparing additional punishments or imposing concurrently the punishments can be considered as it is the practice in the US. If the victim of telephone fraud is over 55 years old or the range of victims and scale is too big, it can be considered to regulate it with additional punishments or by

without the victim recognizing the act of disposition.
imposing concurrently. Another measure is to punish the ‘act of crime using wire transfer (deposit)’as the tele-financial fraud crime if it fulfills the components such as having caused damage in property or having incurred profit in property as it is done in Japan.

(3) Amendment Direction for Personal and Financial Information

In the Criminal Act, there is no direct definition for information, and ‘electromagnetic record’, which is similar to information, is understood as record that is made electronically and magnetically. ID and password are categorized as information in regards to voice phishing but personal and financial information are not categorized clearly. Normally, personal information such as the resident registration number is traded for money, but it is used as the ‘key’ to access a website, and personal and financial information are used to access certain medium or to verify and certify in the case of phishing and pharming. The password, security card, and authentication certificate are security measures to block the unauthorized access, and they are considered as special media such as electromagnetic records, etc., based on the Criminal Act. Personal and financial information have the formal ‘procedural characteristic with inherent values, but in the cyberspace such as internet, especially in the financial website, it plays a role of the key, and it should be strictly protected by law for having the trade value(latent). 41

Fake websites not only collect personal information, but also request financial information such as authentication certificate, credit card number, etc., and the user voluntarily enter in personal or financial information which are then taken by the offender. The offender obtains profit in property by luring the user to a fake website for obtaining personal and financial information. Therefore, if it becomes a structural element, the act of obtaining personal and financial information through a fake website and using the information to receive loan service is considered to be an infringement on someone’s secrecy and stealing information. Hence, based on the principle of clarity, establishing a new type for such act in the Special Act can be considered. For example, strictly regulating the act of

41 In the case Taiwan, the forms of illegal organizations obtaining personal information are through ‘fake name’, ‘related organization’, ‘type of telecommunication business’, ‘internet administration’, ‘trading stolen information of public and private organizations’. (Song, Su Hwan, “Special Prevention Measure Research on Tele-Financial Fraud”, National Taebuk University Criminology Institute, 2008, p. 14).
hacking and stealing personal and financial information and using the obtained information to input into date processing systems such as computer, etc., can be considered by establishing a provision that states “anyone who damages one’s information that is processed, recorded or transferred by the information network system, or who steals or leaks one’s password or personal and financial information by luring the person to a fake website, shall be punished by imprisonment for not more than 5 years, or a fine not exceeding 50 million won”. This is because it is critical to regulate the voice phishing fraud crime in the early stage as the offender steals personal and financial information through hacking and uses them for phishing and pharming.

IV. CONCLUSION

When the types of recent voice phishing fraud crimes are looked into, it is pointed out that reliving the victim under the current Special Act is difficult because the usage and supply of service such as card loan, loan fraud, insurance fee refund, etc., are objectified. Therefore, it seems persuasive to propose a direction for the relief of victim by deleting the provision of clue on the supply of service in the Special Act. Also, there is a need to put efforts into overcoming the structural and systematic limitations as the voice phishing fraud crimes are becoming more organized and habitual, cunning and intelligent in its method, and creating more damages. This is because it is difficult to regulate all as the fraud crime because the tele-financial fraud crimes are operated under the systematic system divided by the roles, and also because there are different forms of crime such as fraud, disguise, threatening, intimidation, etc. Therefore, this report tried to seek for institutional direction for the legislation centering around the practical issues along with the comparative consideration. As a result, although it is difficult to apply the criminal code regarding the act of disposition, it can be punished as the indirect principal offender of crime of the usage of computer, etc., and because the recent voice phishing crime is committed by using personal and financial information, it would be meaningful to seek for ways to punish it at the pre-stage of the crime.

For this purpose, establishing new rules of punishment in the Special Act can be considered, and it means that a thorough review should be done to see whether the crime can be punished in the pre-stage of preparation if it
cannot be punished with the current structural and systematic limitations. Also, it can be considered to regulate the act as the crime of risk or as the crime with objective as the offender’s purpose was to obtain and use personal and financial information to gain profit in property.

Finally, the title and the legislative purpose of the ‘Special Act on Return of Damages by Telecommunication Financial Fraud’ should be amended, and it should specify not only the relief of the victim but also the rules of punishment in order to respond to rapidly evolving fraud crimes.
I. INTRODUCTION

In December 2011, the Constitutional Court of Korea made a six to two ruling that Paragraph 1, Article 93 of Election Act was in violation of the constitution, stating that the provision of law in question is against the constitution as far as it is interfered as to include ‘the method of posting texts or videos, etc., using the information network, homepages, online bulletins, and chatting rooms, or transmitting them via emails’. This ruling by the Constitutional Court also interpreted online election campaigns as “in line with some of the goals in public elections, including “equality in opportunity, transparency, and cost efficiency” and it was stated in the verdict that prohibiting Internet campaigns and punishing the violator of such a prohibition cannot be seen as “a proper means to fulfill the purpose of enactment of the Act.” In addition, as there are other legal measures specified to prevent dispersion of slander or false claims, the court said it would be “excessive to entirely and uniformly ban and punish all of such activities only because of the chances of illegality.” Therefore, “it does not meet the minimum requirements of the violation.” On top of this, “whereas the benefit of the ban in terms of the fairness in elections is neither self-evident nor specific, the losses due to a complete restriction of the freedom to express political opinions and freedom to engage in campaign activities on the Internet over a period of 180 days until the
election day are significant, which deprives the balance of the legal benefit of banning campaign activities.”

This ruling modified the existing decision by the Constitutional Court\(^2\) which supported the judgment by the Supreme Court\(^3\) that interpreted Internet homepages as one of the means of illegal acts set forth in Paragraph 1, Article 93 of Election Act\(^4\) and resulted in revision of Election Law (Dec. 29, 2012, No. 11374) Therefore, campaign activities on the Internet are no longer a crime of illegal campaign activity as stated in Subparagraph 5, Paragraph 2, Article 255 of Election Act. Moreover, considering the intention of the Constitutional Court, such activities shall not remain as a criminal offense.

However, the judgment of partial violation of the constitution by the Constitutional Court did not change the wording of Paragraph 1 of Article 93 in spite of the revision of Election Act due to the mode of specifying the conditions allowed and prohibited. In addition, the revised Election Act specifically mentioned Internet homepages and emails as the allowed means of campaign activities before the commencement of the legal campaign period, leaving ambiguity on whether the campaign activities on the SNS can be seen as such allowable activities. However, since most of the

---

2 The Constitutional Court 2009. 7. 30. 2007Hannu718.

3 See The supreme Court 2004. 11. 25. 2004DO4045; The Supreme Court 2006. 6. 27. 2004DO6167; The Supreme Court 2007. 2. 22. 2006DO7847; and The Supreme Court 2008. 9. 25. 2008DO6555.

4 Article 93 (Prohibition of Unlawful Distribution or Posting, etc. of Documents and Pictures)
   (1) No one shall distribute, post, scatter, play, or run an advertisement, letter of greeting, poster, photograph, document, drawing, printed matter, recording tape, video tape, or the like which contains the contents supporting, recommending or opposing a political party (including the preparatory committee for formation of a political party, and the platform and policy of a political party; hereafter the same shall apply in this Article) or candidate (including a person who intends to be a candidate; hereafter the same shall apply in this Article) or showing the name of the political party or candidate with the intention of influencing the election, not in accordance with the provisions of this Act, from 180 days before the election day (the time when the reason for holding the election becomes final, in case of a special election) to the election day: Provided, That the same shall not apply to acts falling under any of the following subparagraphs: <Amended by Act No. 5412, Nov. 14, 1997; Act No. 5537, Apr. 30, 1998; Act No. 6663, Mar. 7, 2002; Act No. 7189, Mar. 12, 2004; Act No. 7681, Aug. 4, 2005; Act No. 9974, Jan. 25, 2010> 1. Cases where any candidate or any person falling under any of the subparagraphs of Article 60-3 (2) (including the chief of an election campaign liaison office, in cases falling under subparagraph 2, and, in such cases, “preliminary candidates” shall be deemed “candidates”) personally hands out the name cards of a candidate under Article 60-3 (1) 2 during the election campaign period; and 2. Ordinary political party activities under Article 37.
prohibitions and liberties specified in Election Act are related to punishment clauses and constitute criminal charges, they should be subject to the principle of punishment by law. The current Election Act\(^5\) has a very complicated structure in which the essence of requirements and conditions are difficult to grasp due to complicated rules and frequent revisions because of political interests, and there are iterations of similar elements for which a multitude of rules are presented as exceptions and principles, making the essence of the prohibition very unclear. Therefore, even an experienced legal expert would find it difficult to navigate through the provisions of Election Law without stepping on the lines between what is legal and illegal. In this article, we will examine the essence of Election Act in the perspective of criminal law theory with a focus on expression of political opinions on the SNS.

II. NON-CRIMINALIZATION OF CAMPAIGN ACTIVITIES ON THE SNS

A. Difficulties in Distinguishing Simple Expressions of Political Opinions and Campaign Activities on the SNS

(1) Tolerance of the Expression of Political Opinions in Principle

Paragraph 1, Article 58 of Election Act defines a campaign activity as “activities to cause a candidate to win or lose an election” and specifies that “simple expressions of opinions on the election (subparagraph 1),” “expression of supports or disapproval of the recommendation of a party candidate by a political party (subparagraph 3),” and “encouraging participation in voting itself, without expressing any support or disapproval of a specific party or candidate (subparagraph 5)” are not campaign activities.\(^6\) The precedents in the Supreme Court stated that “campaign activities are all active, planned, necessary and advantageous activities for gaining votes for a candidate or causing one to lose the election, where the intent of winning the election or defeating a competing candidate is objectively recognized.”\(^7\) When it is not certain whether an action can be

\(^5\) Significantly revised on February 29, 2012, followed by two more amendments; however, regulations relating to campaign on the Internet remained as revised due to decision of the Constitutional Court.

\(^6\) Subparagraph 2, Subparagraph 4, and Subparagraph 6 are the regulations on the activities of politicians.

\(^7\) See The Supreme Court 1999. 4. 9. 98DO1432; The Constitutional Court 1994. 7. 29. 93Hung4; and
recognized as a campaign activity, “since the freedom of expressing one’s political opinions should be guaranteed as far as it does not compromise the fairness in elections,” the judgments should be made in dubio pro libertate at all times.

For this reason, the judgment concerning whether an activity falls into the category of a campaign activity should depend on “subjective elements that could relatively be objectified.” If it cannot be clearly determined as a campaign activity, one should be given the freedom to express his or her political opinions. That is, all activities specified in each paragraph in Article 58 of Election Act that are not interpreted as campaign activities should be considered as allowed activities based on the principle of constitutional interpretation of the law. For this reason, regardless of the judgment by the Constitutional Court and revisions thereof, expression of political opinions through the SNS is allowed at any time in principle, be it during the official campaign period or not.

(2) De-facto Banned Expressions of Political Opinions due to the Characteristics of the SNS

In a modern democracy where the interests in the real life clash all the time, it is not always easy to distinguish a simple expression of political opinion from a campaign activity. In particular, the SNS allows any users to use it at a very low cost, and contents are produced, responded to, and reproduced at all times. For this reason, the SNS reveals the personality of an active user to the public in no time, and the persona of a user of the SNS can no longer be distinguished from his or her

---

12 See Won Sang Lee, Il Nam Han, Hyun Wook Chun (2011). Take advantage of Internet services and new types of media, black propaganda and slander to predict aspects of an effective regulation plan, Central Election Commission Research Project.
13 See Won Sang Lee, Il Nam Han, Hyun Wook Chun (2011). Take advantage of Internet services
‘electronic persona’. As such, because of the nature of the SNS that causes its use to be recognized as the media itself, the expression is always an outright burst of his or her subject intentions. Therefore, it is still possible in most cases to identify the outcome of the election the individual hopes for based on the general activities on the SNS and the general persona that is revealed by the posts, even if the expressed contents do not contain any desire of a candidate to win or lose the election.

Therefore, it is virtually impossible to distinguish simple expressions of political opinions from campaign activities on the SNS, and the elements that prohibit the campaign activities get to bind almost all expressions of political opinions demonstrated on SNS. That is, because they failed to consider the fact that simple expressions used on SNS and election campaigns using the same media cannot be distinguished from one another, the phrase “and other similar things”, which does not clearly specify the subject of the action and was used in Paragraph 1 of Article 93, has been interpreted as a de-facto ban on all expressions of political opinions on SNS. Such ambiguity of the punishment clauses of the law constitutes an excessive restriction on the freedom of speech by going too far beyond the initial legislative intent, i.e. advancing democracy by ensuring a fair election.

This is the reason why the Central Election Administration Committee argued in its opinion for revision of laws on the politics on Jul. 21, 2003 that it is desirable to allow campaign activities on the Internet at all times, with more of such opinions continuously being issued afterwards. The Constitutional Court also ruled that the problems “originated from the fact that the law created to regulate campaign activities in age of ‘offline’ is still in effect in the age of Internet”. For this reason, the logical foundation

of the argument that Paragraph 1, Article 93 of Election Act is partial violation of the constitution can only be established under the premise of allowing campaign activities on the Internet at all time.

B. Ambiguity of the Prerequisites in Paragraph 1, Article 93 of Election Law

(1) Duplicated Prohibition of Campaign Activities Before the Official Campaign Period

It was not easy to apply the judgment of partial violation of the constitution by the Constitution Court to the actual provisions of law from the beginning, because of the complex structure of Election Act. While Paragraph 2, Article 58 of the Act states “any person is free to perform a campaign activity,” Article 59 allows such activities only “from the starting date of the campaign period to the day immediately before the election day” as a matter of principle. Therefore, unless otherwise specifically allowed in each Paragraph of the same article or other provisions of Election Act, a campaign activity can be legal only if it is performed during an official campaign period, regardless of the method and media. Outside of this period, such an activity will, in most cases, constitute a crime of ‘violating the official campaign period’ punishable by Article 254 of Election Act.

On the other hand, Paragraph 1 of Article 93, which is the subject of the judgment by the Constitutional Court, bans distribution or posting of documents or posters to influence the election until 180 days before an election. Here, any actions aimed to influence the election by supporting, recommending, or disapproving a candidate or promoting the name of a candidate eventually influences the result of the election for the candidate in question, and the behavior described in Article 93 is not distinguishable in its essence from the concept of campaign activities set forth in Paragraph 1, Article 53 of Election Act, resulting in duplicated ambiguity. Therefore, if one conducts the activities in Paragraph 1, Article 93 using printed materials, etc., starting from 180 days before the election until the beginning of the official campaign period, it will constitute the crime of illegal campaign activity set forth in Subparagraph 5, Paragraph 2 of Article 222 due to the violation of Paragraph 1 of Article 93, and the crime of violating the campaign period in Paragraph 2 of Article 254 due to the violation of Article 59. But then, both of the provisions specify the legal punishment of a fine up to KRW 4 million or 2 years of imprisonment.
In addition, the crime of violating the campaign period in Paragraph 1 of Article 254 even specifically describes the violating behavior as to “printed materials, etc.” Therefore, in terms of the principle of the law, there is scarcely any chance that the prerequisites of Paragraph 1 of Article 93 will become applicable from 180 days before the election until the preceding date before the commencement of the official campaign period.

Therefore, the old Election Act\textsuperscript{17} describes it that campaign activities using SNS until the commencement of the official campaign period remained banned even if the objects of the actions described in Paragraph 1 of Article 93, do not include homepages and emails. Although the decision by the Constitutional Court concerned interpretation of Paragraph 1 of Article 93, the complex structure of the Act necessitates going beyond just amending the wording of Paragraph 1 of Article 93 in order to fully realize permission of online campaign activities at all times.

\textbf{(2) Banning of Campaign Activities During an Official Campaign Period}

It is allowed to distribute or pose legally allowable documents and posters in accordance with Election Act during an official campaign period. However, even during an official campaign period, campaign activities using printed materials, such as posters, official election gazettes, or election pledge books can be accepted as legal only when they are conducted under the strict guidelines set forth in Article 64 to 66 of Election Act. The contents of these provisions concern the materials prepared and used by candidates themselves, and the general public cannot perform any actions which involve distributing or posting printed materials even during an official campaign period. In addition, the violation of Article 64 to 66 is punished by a fine up to KRW 4 million or up to 2 years of imprisonment in accordance with Paragraph 2 of Article 255. Paragraph 1 of Article 93, does not seem to have significant benefit in this case as well.

In addition, Paragraph 1 of Article 109, limits the method of campaign activities using ‘the means of electronic communication’ during a campaign period to those specifically allowed by the law. Paragraph 1, Article 2 of Electronic Communication Business Act defines ‘electronic communication’ as “transmission or receipt of symbols, texts, sounds, or videos via

\textsuperscript{17} February 29, 2012, before being amended by Law No. 11,374.
electronic means.’ Therefore, campaign activities using the Internet are only allowed in the conditions specifically mentioned in Paragraph 1 of Article 109 as exceptions. Paragraph 1 of Article 255 states that any violation of Paragraph 1 of Article 109 shall be punished by a fine up to KRW 6 million and or up to 3 years of imprisonment. In the end, the prerequisites in Paragraph 1, Article 93 is not much likely to become applicable to the illegality committed during an official campaign period. In this regard, Paragraph 1 of Article 93 may become unnecessary. It is believed to be of a declarative function to block any other type of campaign activities that could not be covered by other provisions of the law due to a loop hole or a defect in the law.

Campaign activities are essentially aimed to cause a candidate to win or lose the election, and such activities are performed in the forms of expression of one’s opinion by their nature. However, the ambiguous definition of behaviors in Paragraph 1 of Article 93 may be applicable to any expressions of any dispersible media, banning all campaign activities other than using one’s own voice. The original intent of Article 93 is to “prevent the imbalance between candidates due to their differences in economic capabilities, unfair competitive practices, and any results that harm the tranquility and fairness of the election based on the principle of equal opportunity to campaign activities as set forth in Paragraph 1 of Article 116 of the constitution to ensure fulfillment of the common good of the constituency and those involved in the election process” with a view to prohibit any campaign activities that is only available to candidates with considerable economic means. Therefore, the prerequisites in Paragraph 1 of Article 93 of Election Act should only be applied to campaign causing economic expenditure that is so significant to harm the fairness of the election.

Nevertheless, ambiguity in Paragraph 1 of Article 93 caused it to be understood as banning all the other campaign activities than what is specifically approved by the law. In the end, Paragraph 1, Article 93 imposes an extreme restriction on the freedom to choose the mode of

18 Refer to Supreme Court precedents 2004. 11. 25. 2004DO4045.
19 The Constitutional Court 2009. 7. 30. 2007 Hunma718.
20 See Won Sang Lee, Il Nam Han, Hyun Wook Chun (2011). Take advantage of Internet services and new types of media, black propaganda and slander to predict aspects of an effective regulation plan, Central Election Commission Research Project. p.66-67.
campaign activities despite the fact that Paragraph 2 of Article 58 of the same law declares the freedom of campaign activity as a matter of principle. As a result, it bans every other campaign activity that is not specified otherwise in the law as exceptions in principle. Accordingly, campaign activities using the SNS can be seen as legal only when there is a specific provision that allows it, even during an official campaign period. Therefore, it was necessary for the previous version of Election Act to allow campaign activities using the internet at least during the official campaign period, which was banned in duplication by both of Paragraph 1, Article 93 and Paragraph 1, Article 109. For this reason, it had to include a separate clause in sub-Paragraph 1, Paragraph 1, Article 82 to 84 that allows campaign activities using Internet homepages and email.

C. Provisions that Allow Campaign Activities Using the SNS in Current Election Act

For this reason, Paragraph 1 of Article 93 of Election Act maintains its current wording in spite of the ruling of partial constitutional violation by the Constitutional Court. The law makers had to choose the option of adding a new provision that allows campaign activities on the Internet before the official campaign period instead of revising Paragraph 1 of Article 93. The law makers removed Subparagraph 1 that defined the campaign activities using homepages or emails of Article 82 to 84 which defined the campaign activity using information-communication network. Then, they expanded the scope of Paragraph 3 of Article 59 that regulated campaign activities before the commencement of the official campaign period using homepages by ‘candidates’ or parties to include the general public.

Revised Paragraph 3 of Article 59 concerns “campaign activities by posting texts or videos on Internet homepages, bulletins, and chat-rooms or sending them by emails.” Article 82 to 84 of Election Act before amendment was one of those provisions that defined the method of campaign activities, which only concerned the activities during an official campaign period. Therefore, it was necessary to place the provision that allowed campaign activities using the Internet under Article 59 that allowed campaign activities before the commencement of the official campaign period as exceptions in order to clarify the intention of the decision by the Constitutional Court. As such, the complicated structure of Election
Act, where prohibitions and exceptions are interwoven to form very complicated embroidery caused the provision in question, for which the Constitutional Court gave a ruling, remained intact, while two other provisions had to be amended instead. As a result, campaign activities using the Internet became allowed as exceptions by adding specific provisions to allow them while the umbrella provision of a general ban remained as it was.

III. REGULATION OF THE METHODS OF CAMPAIGN ACTIVITIES USING SNS

A. Whether SNS can be Included in the Campaign Activity Methods Allowed

(1) Structure of SNS

As mentioned above, Article 59 of Election Act concerns the official campaign period, while Paragraph 3 of the same article allows campaign activities using homepages and emails before the commencement of an official campaign period as an exception. However, it is limited to the traditional ways of using the Internet, namely homepages (bulletins and chat rooms) and emails. Thus, it requires some contemplation to determine whether the SNS falls in this category or not. On the other hand, as Paragraph 1 of Article 109 bans campaign activities using electronic communication networks as a principle, unless otherwise allowed as exceptions, it is necessary for campaign activities using the SNS to be clearly allowed by Article 59 in order to become a legal method of campaign activity. The majority opinion for this matter in favor of the subjects of the actions sees it as legal. However, the problem is that there is no discernable legal foundation or theoretical ground that supports such a conclusion.21

SNS is the acronym of Social Network Service. The SNS22 is also defined as a web-based service involving (1) constructing a personal profile, (2) making a list of users who share the connection, and (3) providing interactions with other users based on such a list.23 Due to the rapid

advance of information technology, SNS is also evolving rapidly, and it is generally referred to as the Social Media due to the progress in the methods of sharing various types of contents. The SNS is serviced in a way positively distinguished from emails. And, therefore, in the minds and perspectives of the general public, the SNS is something quite different from homepages or emails.

The SNS is divided into ‘information oriented’ types and ‘relationship oriented types’ based on which of these two aspects they focus on. Twitter is one of the most representative form of information-oriented ones, being the most popular micro-blog service in the world. Facebook is a social networking type SNS and commonly recognized as a relationship-oriented type. If we take a closer look into how these SNS works, the relationship types could be seen as something closer to a homepage, while the information type is closer to emails. However, while they may differ in details, they share the fundamental function of posting or sharing messages, and they should be recognized as a new form of internet service. In addition, with the increase of the number of smart phones people use these days, more and more users now access their SNS using dedicated application software than a browser. Furthermore, some extreme cases include the SNS that can be accessed or used with computers or web browsers as secondary means or cannot be accessed with these traditional means at all.

(2) Problems with Application

Election Act does not provide any definition of an Internet homepage. In fact, a homepage means the starting page of a web browser. However, in Korea, the term ‘homepage’ has been customarily used as a synonym of ‘website.’ A website is a bundle or package of webpages, which are

26 See Won Sang Lee, Il Nam Han, Hyun Wook Chun (2011). Take advantage of Internet services and new types of media, black propaganda and slander to predict aspects of an effective regulation plan, Central Election Commission Research Project. p.35, 46.
displayed via URLs. URLs are composed of the name of a domain in the network which is built on IP, Internet protocol. In particular, websites are built in HTML format and can be accessed and used via a web browser. It is still possible to access Twitter or Facebook using a web browser in their form. Thus, they can be included in the conceptual range of a homepage in principle. However, in consideration of the fact that the perception of the SNS and the way it is used are completely different from the traditional homepages that mainly depend on bulletins and chat rooms, it is necessary to revise the wording of the relevant provisions of the law for clarification. In particular, mobile instant messengers or other new types of SNS no longer belong to the category of a homepage in their formats. Of course, most of these could be included in the conceptual category of emails. Election Act defines emails as “a communication system with which users exchange texts, voices, videos, or images over the network (Paragraph 1 of Article 59).” This is quite a broad definition; however, in spite of this, not all of the new generation of Internet access devices, such as smart phones, could be recognized as computers.

For this matter, there is a case in which the Central Election Management Committee gave an authoritative interpretation that defined ‘Kakao Talk’ as an email service. However, as mobile instant messengers are not distinguishable from the usual short text messages in practice and the mobile communication service providers recently launched a service called ‘Joyn’, which uses the data communication network instead of the conventional mobile network to transmit text messages, the border between them becomes more blur. Some argue that Joyn is the next text messaging technology that will replace SMS and MMS. However, if one sees Joyn, which works in the same way as Kakao Talk as text message, it is also subject to Paragraph 2, Article 59 of Election Act, and therefore, “only a candidate and a would-be candidate can transmit messages using an automated mass transmission service, and the number of mass transmission cannot exceed five times.” A violation of this provision will result in a fine up to KRW 4 million or 2 years of imprisonment in accordance with

27 Central Election Commission, Well-defined Election Campaign Guide, Feb. 2012, p.10. This book was published to inform the revision of the election law before the 19th election of members of the National Assembly in April 2012.
28 See May 25, 2013, Yonhap News Agency, Mobile carriers’ own messenger service struggling on competition.
Subparagraph 1, Paragraph 2 of Article 256. Also, if one uses the automated, mass transmission system, there are certain information to be included in the message, including the fact that the transmitted message is campaign activity information in accordance with Paragraph 2 of Article 82 to 85, the phone number of the sender, and the ways to express the intent to refuse the transmitted messages. Any violation of this provision will constitute a crime, which is punished by a fine up to KRW 1 million or 1 year of imprisonment. Therefore, the judgment of whether the said law is applicable to a messaging service can be different due to the uncertain conditions and prerequisites while they both use the same technology. In addition, while an automated mass transmission system means a system that sends the same messages to two or more recipients at the same time by transmission equipment. The authoritative interpretation by Central Election Management Committee has it that “transmissions using the built-in transmission mechanism of a phone (except for altering such transmission programs or installing a separate software for the purpose)” targeted to an audience not exceeding 20 people are not recognized as a use of an automated mass transmission system. However, most of mobile phones these days are smart phones and they all use applications to send text messages. According to this interpretation, there is another problem. That is, if applications such as Joyn are installed in the devices as a default feature at the factory, it is not an automated mass transmission system. However, if it is upgraded or newly installed, it becomes an automated mass transmission system.

B. Types of Still Prohibited SNS Election Campaign

(1) The Principal Limitation

Although it is allowed to campaign activities using the Internet under Paragraph 3, Article 59 of Election Act, it is only allowed when it complies with various restrictions by the Public Official Election Act. First of all, the person who can’t participate in election campaign regulated by Article 60 is not allowed to use SNS election campaign. In particular, Subparagraph 1, Paragraph 1 of Article 60 (Persons Barred from Election Campaign) allows election campaigns to Korean nationals only. However, since the SNS is communication tool across borders, foreigners who are interested in the political situation in Korea especially compatriot with

foreign nationality, could participate in election campaign through the SNS or de facto election campaign which does not distinguish the expression of political decision punished by a fine up to KRW 6 million or 3 years of imprisonment in accordance with Subparagraph 2, Paragraph 1 of Article 255. If the subjects reside outside Korea, enforcement of law is impossible to all intentions.\textsuperscript{30}

In addition, in Subparagraph 2 of the same Article, minors are prohibited from participating in election campaign. SNS campaign through minors can be also punished by a fine up to KRW 6 million or 3 years of imprisonment, Subparagraph 2, Paragraph 1 of Article 255 as well.\textsuperscript{31} There is high rate of minors in SNS user population because of its easy accessibility. It is not easy to expect minors to be fully aware of the contents of the Public Official Election and expect them to adhere to the law. In addition, public officials and those who are prohibited from campaigning through SNS are also included in the paragraph 1 of Article 60. Moreover, the violation of Paragraph 1 of Article 87 that organization or their representatives can’t campaign using SNS is punished by a fine up to KRW 6 million or up to 2 years of imprisonment in accordance with Subparagraph 11, Paragraph 1 of Article 255.

\textbf{(2) Contents limitation}

A person who conducts campaign activities using the SNS shall not disperse false information on the candidates. In addition, one shall not disclose a fact to disrepute the candidate unless it concerns the good of public (Paragraph 2, Article 82 to 84, Article 110). In case of disrepute a candidate by disclosing a fact, the perpetrator shall be punished by a fine up to KRW 5 million or 3 years of imprisonment. If the perpetrator dispersed false information on the candidate, he or she shall be punished by Article 250. Here, if the dispersed false information benefits the candidate, the violator shall be punished by a fine of KRW 30 million or 4 years of imprisonment (Paragraph 1) and 7 years of imprisonment or a fine between KRW 5 million and KRW 30 million. Normally, the SNS has a very strong capability in dispersing information, and it is expected to be able to spread political issues in a significant rate. In particular, the existing


media theory has it that the SNS, which is built on the willingness of the receivers to receive the information provided to them, is expected to have a reinforcement effect, which causes the supporters to unite under a cause, or a conversion effect, which can have a persuasive effect on voters with different political ideas. For this reason, some estimate that up to 8 to 12% of the total votes are swayed by the SNS. In particular, it is possible with the SNS to communicate with a certain group of audience strategically based on their preferences, to disperse a certain message very efficiently. In this regard, the media analyzed the result of the previous elections being influenced strongly by the SNS, as the participation rate of voters in their 20s and 30s increased significantly.

However, such an analysis is rather “inferential than evidential.” That is, it cannot be verified objectively. It would be a more rational conclusion to think that the increased interest in politics caused the users in their 20s and 30s to use the SNS more to participate in political communications. The SNS spreads by its nature its messages through the voluntary participation by the users which is a prerequisite. This result in a paradox that it can only exert its influence as far as the senders continuously tries to make and maintain new relationships. Most of the users just stand and watch as bystanders. Therefore, the characteristics of the Internet, that only 9% of the total users contribute to spreading of the message and only 1% creates meaningful messages, gets even more prominent. According

37 See Won Sang Lee, Il Nam Han, Hyun Wook Chun (2011). Take advantage of Internet services and new types of media, black propaganda and slander to predict aspects of an effective regulation plan, Central Election Commission Research Project. p.53.
38 Dong Hun Lee, Min Hoon Lee, Sung Min Park, Jun Hwan Lee (2010). Spread of new social media and corporate communication strategy, CEO Information No. 764, p. 4 SERI.
to the survey, 50% of the twits that are spread far beyond are created by approximately 20,000 users, which account for 0.05% of the total users.\textsuperscript{40}

As such, it is necessary for a user of the SNS to manage his or her reputation continuously to maintain his or her influence. When it comes to SNS, in which the users build relationships and communicate with one another based on their personalities, what is more important is the credibility of the senders, rather than the credibility of the messages themselves. For instance, a newcomer who is not well-known will have a significant difficulty in spreading his or her messages across the network no matter how many messages he sends away, as they will not be spread by others. However, some powerful users, whose identity has been exposed during the process of trust building over a long period of time, are more exposed to legal responsibilities and considerate of self-censorship in order to maintain their reputation among other users. In addition, the users who receive the messages actively are likely to have a similar kind of political interest with the senders who are reliable. In this regard, the effects of the political communication, especially those involved in campaign activities, can only be limited. It might be possible to strengthen the bonds between the supporters of the same political cause using the network of relationship that has been built over time; however, it will be very difficult to expect them to be effective in converting the supporters of other political causes. In the end, the SNS is not a significant factor that influences the overall approval rate in an election, and the effect of the illegal intervention in the election using the SNS may not be as significant as many would fear.\textsuperscript{41}

Rather, the use of SNS should be promoted and encouraged as a new forum of the collective intelligence where various political information can be dispersed and integrated proactively. SNS can still be a valuable tool to disperse the news on absurdities that are not covered by the established media due to various interests involved in the political event; however, it can still negatively influence the public over a short period of time. Such characteristics of the SNS will certainly contribute to the enhanced transparency in politics in general for the country. Any facts regarding a


\textsuperscript{41} See Won Sang Lee, Il Nam Han, Hyun Wook Chun (2011). Take advantage of Internet services and new types of media, black propaganda and slander to predict aspects of an effective regulation plan, Central Election Commission Research Project. p.60-61.
candidate for a public post should be dispersed as widely as possible in order to verify his or her personality and capability, while the allowable extent of such dispersion may depend on the nature of the information. In particular, the information that falls into disrepute a candidate should be put under even more strict eyes of verification. Regarding this matter, the court once ruled that “with regard to the allowable extent of disclosure on the personal information of a contender for an elected position, even if we consider the current situation in Korea in which the elections are deformed into partisan votes by the general constituency, making Korea an even more partisan state, and unless the necessity to elect an elite as our representative elite based on the essential implication of the representative system is not denied, the constituency should be given with the opportunity to access sufficient information to judge if a candidate has the personal traits, experience, and ability to carry out the duties of the elected position. Meanwhile, in a democracy, a statesman is a representative of the people and delegated by the constituency to conduct the matters of running the country, and, therefore, the allowable range of disclosing or revealing information regarding the conducts or other issues of such figures with more political functions who demand more respect from the people should be even greater. As it is also true that a statesman makes his political views realized in a series of confrontations between conflicting political ideas, he is to be of a position that has to defend himself under severe attacks from others. For this reason, these figures are required to tolerate the exposure of the negative aspects of his personality.” Thus, the constitution of the crime of slander on a political candidate as set forth in Article 251 of Election Act should be applied more carefully when it comes to campaign activities using the SNS and only become applicable to cases where disclosing facts for a purpose of malicious disputation that contributes to no public goods and compromises the fairness of an election. The crime of disrepute a candidate in Election Act is intended to protect the ‘fairness in election,’ not the personal honor of the candidate as individuals.

42 Seoul High Court 1993. 10. 7. 93NO1519.
IV. CONCLUSION

Regarding the use of SNS election campaign, when interpreting majority opinion on the Constitutional Court decision and considering the characteristics of interpreting SNS and election for public office, there are controversies over election campaign using Internet network, such as SNS: some insist that the freedom to express one’s personal political views should be widely accepted, while others question that, in the information society where “the Internet space is constantly spread before our eyes” and Internet network such as SNS has strong delivering and spreading power, we would not be able to ensure fairness of election campaigns only by imposing ex post facto punishment on slander and dissemination of false information. No one will not deny the fact that right to express political views must be ensured unless it does not undermined fairness of election.

As discussed above, when considering the structure of SNS that premises active participation of recipients, the effects of political communication through SNS is inevitably limited in reality; therefore, the possibility to undermine fairness of the election seems to be relatively low. On the other hand, SNS could be characterized to open the door for people to express and exchange their own views without restrictions and is expected to help politics become more transparent.43 To facilitate expressing political opinions and conducting election campaign with SNS, the current Public Election Act, which differently responds to using open network such as SNS - one time prohibits it while the other time permits as an exception - should be amended in order to remove any misunderstanding in interpreting provisions. Given the purpose of Article 251 (Slanders against Candidates) of the Act, to guarantee fairness of election, not to protect personal reputation, if SNS is useful to prove personality or capability of candidates to some extent, it does not constitute elements of the Act.

I. INTRODUCTION

A method highly likely to be employed by terrorist groups that are using 21st Century state of the art technology is cyber terrorism. In many instances, things that you could only imagine in reality could be made possible in the cyber space. An easy example would be to randomly alter a letter in the blood type of a terrorism subject in the health care data system, which could inflict harm to subjects and impact the overturning of the opponent’s system or regime.

Thus, terrorists prefer cyber terrorism over other physical terrorism methods because they may inflict greater harm with less cost. Unlike bombings or kidnapping hostages, cyber terrorist may invade their terror subjects anywhere anytime on the Internet.

With the North American Treaty Organization (NATO)’s misdirected shelling of the Chinese Embassy and its damage inflicted on China, a number of Chinese hacked into the White House and the U.S. Department of State websites. This caused the website of the White House to show various Chinese and English character scribblings, rending it inaccessible for an extended time.

In June of 1998, immediately following India’s nuclear testing, Dutch and British university students posted a mushroom image that symbolized nuclear weapons on the website of the Nuclear Weapons Research Institute.
of India. In September of 1998, Portuguese hackers invaded the systems of some 40 regions in Indonesia and created hyperlinks to a website that criticized the human rights conditions in Indonesia.

The CIH Virus Crisis which occurred on April 26, 1999 had significant implications in various aspects. A virus program made of just a few lines by Taiwanese college students without any specific objective ended up spreading widely throughout the Internet, causing damage to 30,000 PCs in Korea and over 2 billion won in monetary damages in repairs and data recovery.

Despite of such risks of cyber terrorism, a great number of Korean sites are employing loose security measures. In fact, there are many cases where a company with millions of subscribers has very slackened security systems. A nationwide preparation for cyber terrorism is called for. In this context, this research will analyze the current status of Korea’s cyber security systems and its laws from a policy perspective, and move on to propose improvement strategies.

II. KOREA’S CYBER SECURITY LAWS AND POLICY IMPLEMENTATION

Korea’s cyber security systems are governed based on the National Cyber Security Management Act (Executive Instructional Order 222), the Information Technology Infrastructure Protection Act (Code No. 8852), Information Technology Network Use Promulgation and Information Protection Act (Code No. 8867), Industrial Technology Information Security and Protection Act (Code No. 8900), Software Industry Promotion Act (Code No. 8852), etc. However, Korea lacks an integrated and systematic national cyber security policy, and policies are scattered throughout laws and regulations of various sectors such as those related to the national core infrastructure protection, information communication networks, industrial technology information, private sector software industry information, etc. As a result, cyber security organizations are also dispersed throughout various sectors and form the national cyber crisis management organizational structure. This includes the National Cyber Security Center, the Information Communication Infrastructure Protection Commission, the Private Information Conflict Mediation Commission, the Industrial Technology Protection Commission, the Software Business Conflict Mediation Commission. This current state requires a more systematic policy
approach.

An analysis on Korea’s current status of cyber security in the legal and policy perspective will be elaborated, based upon which derivative problems and future improvement strategies will be discussed.

A. Status of Korea’s Cyber Security Management System

The National Cyber Security Strategy Council was set up to discuss important issues such as the institution and improvement of a national cyber security management system, establishment of policies and interagency coordination, and the National Cyber Security Taskforce Council was established for efficient operations of this National Cyber Security Strategy Council for national cyber security management and countermeasures. In addition, for a comprehensive and systematic national approach to cyber attacks the National Cyber Security Center of the National Intelligence Service was appointed to oversee national cyber security policymaking; cyber risk information collection, analysis and dissemination; cyber attack incident investigations and recovery support; and national information communication network security verification. Central government agencies have been assigned to establish and implement cyber security measures for information communication network security enhancements.

In addition, a collaboration system was founded for inter-organizational cyber attack information sharing and a reporting mandates to the National Intelligence Service whenever incidents occur or risks are discovered. In the break out of a wide-span incident, the National Intelligence Service is to form and operate a joint governmental investigation team and a recovery support team. Cyber security technology development has been delegated to the National Security Technology Research Center.
B. The National Cyber Security Strategy Council and the National Cyber Security Taskforce Committee

In Korea, the National Cyber Security Strategy Council was established for deliberation of important issues on national cyber security, and the Strategy Council is chaired by the Head of the National Intelligence Service. The Strategy Council members consists of the Deputy Ministers of the Ministry of Education, Science and Technology, the Ministry of Foreign Affairs and Trade, the Ministry of Justice, the Ministry of National Defense, the Ministry of Public Administration and Security, the Ministry of Knowledge and Economy, the Ministry for Health, Welfare and Family Affairs, the Ministry of Land, Transport and Maritime Affairs, as well as the President's Office Diplomacy and Security Chief of Staff, the Korea Communication Commission Standing Committee Member, the Financial Supervisory Commission Deputy Chair, and a deputy minister-level public official of a central government agency designated by the Strategy Council Chair.

The Strategy Council will discuss: ① establishment and improvement of the national cyber security system, ② national cyber security related policies and interagency coordination, ③ implementation measures for executive
directives related to national cyber security, and ④ other matters raised by the Strategy Council Chair (National Cyber Security Management Code No. 6). In addition, for efficient operations of the Strategy Council, the council is mandated to retain a National Cyber Security Taskforce Committee. The Taskforce Committee Chair is to be the Deputy Chief of cyber security affairs for the National Intelligence Service, and Committee members consists of section head public officials of each Strategy Council member’s ministries. The Taskforce Committee shall discuss: ① National Cyber Security Management and Countermeasures, ② implementation measures of Strategy Council decisions, ③ matters assigned by the Strategy Council or its Chair, and ④ other matters raised by the Taskforce Committee Chair (National Cyber Security Management Code No. 7).

C. National Cyber Security Center

The National Intelligence Service launched a National Cyber Security Center in February of 2004 to oversee national cyber security measures, and in January 2005 based on the National Cyber Security Management Act (Executive Instructional Order 141) the Security Center has been in charge of establishing national cyber security policies, operational support for the Strategic Council and the Taskforce Team, collection, analysis and dissemination of national cyber security information, verification of the national information communication network, among others, to enable comprehensive and systematic countermeasures for cyber attacks.

First, to oversee the national cyber security policies, the Center established and operates programs for cyber security policy planning and coordination, established national cyber security related programs and guidelines, operates the National Cyber Security Strategy Council and Taskforce Committee, and cyber security information sharing programs among the private, government and military sectors.

Second, as a national cyber security assurance and preventative measure, the Center performs national information communications network security verifications, information security level evaluations, cyber security mock training sessions, information communications network security reviews and security-level evaluations.

Third, as part of its activities for comprehensive collection, analysis, and dissemination of national cyber risk information, the Center monitors cyber
security status of major agencies, announces official warnings for risk levels such as normal-attention-warning-risk-high risk, disseminates security analyses information, and develops cyber security technology, 24 hours 365 days a year.

Fourth, as part of its emergency response, investigation and recovery efforts following attack incidents, the Center registers cyber attack incidents, investigates incidents, develops countermeasures, takes preventative action of further escalation, provides recovery support, and establishes and operates a government-wide joint investigation and recovery support team.

In addition, the Center hosts a collaborative board for Korea’s cyber security specialized institutions, has established collaborative relations with advanced nations (i.e. the United States, Great Britain, France, Germany, Canada, Japan, etc.), and holds invitational seminars and events with international experts. Meanwhile, the Center has joint operations with designated government officials and assigned researchers from the National Security Technology Research Center, Korea Information Protection Promotion Agency, etc. to ensure proper coordination of cyber security measures.

D. Information Communications Infrastructure Protection Committee

To discuss major information communications infrastructure protection issues, an Information Communications Infrastructure Protection Committee was established under the umbrella of the Prime Minister. The law sets forth that the Committee shall discuss: ① policy coordination for the protection of major information communications infrastructure, ② comprehensive coordination for protection plans of major information communications infrastructure, ③ issues related to implementation outcomes of protection plans for major information communication infrastructures, and ④ major information communication infrastructure protection systems improvements (the Information Communications Infrastructure Protection Act, Article 3 and 4).

E. The Private Information Conflict Mediation Commission

As a dispute mediation institution founded in December 2001, based on Article 33 of the Information Communications Network Use Promotion and Information Protection Act, an office was established within the Korea
Information Protection Promotion Agency for the Conflict Mediation Committee. For efficient coordination of conflict mediation, the laws set forth that a Coordination Section composed of 5 or less members of the Conflict Mediation Committee shall be established, one of whom shall be a licensed attorney. Matters related to formation and operations of the Coordination Section is to be administered by the Ministry of Public Administration and Security (Information Communication Use Promotion and Information Protection Act, Article 33). The Mediation Committee not only protects citizens’ rights but also enhances business efficiency contributing to building sound distributive order, through various recurrence prevention measures such as by mediating private information conflicts between users and businesses, providing damage prevention promotions and training, making suggestions for legal improvements, advising corrective actions to business transaction models and user agreements, processing of violation incidents, etc. (Private Information Conflict Mediation Committee).

Figure 2: Committee Adjustment Procedure
F. Industrial Technology Protection Committee

The Industrial Technology Protection Committee is the highest decision-making organization created based on the ‘Industrial Technology Information Protection Act,’ which launched on April 28. It is formed by a total of 23 members, including 17 government committee members from government agencies (i.e., related central government agency heads and intelligence investigative agency heads, etc.) and 6 commissioned members from the private sector. For deliberation of industrial technology information protection issues, the Industrial Technology Protection Committee was established under the auspices of the Prime Minister. The Committee head shall be the Prime Minister, and members shall consist of: ① a member who is a head of a related central government agency designated by the President, ② a member who is the head of an intelligence investigation agency responsible for industrial technology information protection, ③ a member with expert knowledge and experience in the industrial technology information protection field designated by the Protection Committee, etc. The Minister of Knowledge and Economy serves as its advisor. The law sets forth that the Minister of Knowledge and Economy shall establish procedural directives by which to protect industrial technology information, after consultation with related central government agency heads and the Protection Committee, and enable relevant institutions to utilization of these directives (Industrial Technology Protection Act, Article 7 and 8).

The Protection Committee operates under a diverse opinion gather process related to national core technology selection process with related government ministries by means of surveys and meetings with industries, researchers and academia, etc., and makes minimal appointments after considering national security, national economic impact, international and domestic market share of related products, research trends and technology expansion and compatibility within respective fields, etc. Based on concerns of negative effects that national core technology export restrictions may pose on corporate global strategies and the corporation’s participation in national research and development, prudent implementation plans are set in place. For national core technologies that received national research and development support, an export approval process is in place based on the evaluation of its national security and national economic impact. For technology developed independently by private sector entities which may
have a serious impact on national security, ex post de facto measures such as export suspension, prohibition or return orders to original states will be taken (Ministry of Knowledge and Economy Press Release).

G. Software Industry Conflict Mediation Committee

It is difficult for the software industry to have a definitive contract objective in the initial phases of projects, and there are often wide opinion gaps between the client and business’ interpretation of objectives. This makes accountability a grey area in times of conflict, causing escalation of discord between the client and business. Rather than conflict resolution by court proceedings, a software business conflict mediation system has been introduced to save time and money by promoting settlements between contesting parties. A Software Industry Conflict Mediation Commission has been established under the Ministry of Knowledge and Economy to provide mediation services related to software ventures. The Mediation Committee evaluates and mediates disputes at the request of either or both parties. However, their services exclude cases that require legal interpretation of contacts to which the government is a party, cases to which subcontractor transaction fairness regulations apply, and issues to which the user agreement restriction laws apply.

The Mediation Committee mediates disputes related to: ① software business between the client and producer, ② accountability between joint contractors or between contractors and subcontractors for a software project, ③ accountability between the contractor and a third party for a software project, ④ guarantor accountability between software project contractor and a guarantor of the contact, and ⑤ accountability between involved parties to a software project (Software Industry Promotion Act, Article 37).

III. PROBLEMS AND IMPROVEMENTS OF CYBER SECURITY SYSTEMS

Cyberspace is a virtual space connected by a network of information technology devices, computers and the Internet, and has already settled itself as a common territory in citizen’s daily lives. It transcends national borders, across the globe, and is closely intertwined with government and private sector participation. Based on such unique aspects, it is developing
complex and highly advanced, and posed definite limits on either the government or the private sector to block cyber attacks that may occur without any limits on time and location. Moreover, cyber crises that are caused by cyber attacks may develop into a nationwide crisis even when targeted to a specific person, unlike physical order disruptions in reality. Risk for cyber catastrophes that may impose national and social damage, such as the 1.25 Internet Crisis that caused the paralysis of major nationwide information communication networks and lead to the leakage of national security and advanced technology from organized cyber attacked from overseas. However, as Korea does not have specific ways or procedures and policies set in place to manage a cyber crisis at the national level, a cyber crisis incident may pose a serious risks and great damage to national security and interests (Security News, 2008).

As previously mentioned, Korea’s legal system for cyber crisis management are governed based on the National Cyber Security Management Act (Executive Order 222), the Information Technology Infrastructure Protection Act (No. 8852), Information Technology Network Use Promulgation and Information Protection Act (No. 8867), Industrial Technology Information Security and Protection Act (No. 8900), Software Industry Promotion Act (No. 8852), etc. Thus, there is an absence of a comprehensive and systematic policy for national cyber crisis, currently scattered around fields of national core technology protection, information communication networks, industrial technology information, private software industry information, etc. This current states calls for the imminent action on establishing proper policies. In addition, national cyber security organizational structures are dispersed throughout sectors (the National Cyber Security Taskforce Committee, National Cyber Security Center, Information Communication Infrastructure Protection Commission, Private Information Conflict Mediation Commission, Industrial Technology Protection Committee, Software Industry Conflict Committee, etc. and requires action.

In the past, government-wide cyber attack response functions were disperse among the National Intelligence Service, the Ministry of National Defense and the Ministry of Information and Communication, and lacked in security programs, manpower and equipment with inadequate cyber attack crisis management response. To address this task at hand, on August 18, 2008, the National Cyber Security Management Act (Executive Instructional
The Act set forth national cyber security related organization structural and operational issues and strengthened interagency collaboration for cyber security. To protect national information communication networks from cyber attacks that threaten national security, the National Cyber Security Strategy Council, the National Cyger Security Taskforce Team was established, in addition passing legislation so that the National Cyber Security Center could be established within the National Intelligence Services. However, the National Cyber Security Management Act was of a directive nature, it was conflictive of related Information Communication Infrastructure Protection Act (Code No. 8852), Information Communications Network Use Promotion and Information Protection Act (Code No. 8852), Industrial Technology Information Protection Act (Code No. 8900), the Software Industry Promotion Act (Code No. 8852), etc. Provisions of each of these Acts had varying subjects to protect from cyber crises, and had redundant organizational structures and functions under each Act.

Therefore, to resolve problem areas identified above, the National Cyber Security Management Act should be amended so that national cyber security management regulations may be properly effective. If the National Cyber Security Management Act has been established, this will enable effective and proactive response to cyber security management within the framework of a comprehensive system of cyber security at a national level. The newly revised National Cyber Security Legislation will eliminate inefficient redundancies in cyber security functions that are scattered based on a number of laws.

Korea has developed into an advanced nation in information technology over the years through initiatives such as developing e-government, information technology industry promotion, etc. For sustained information technology development information security strengthening measures is needed. In this regard, we must be able to securely protect the networks, equipment, facilities, software and its systems related to information collection, processing, storage, retrieval, transmission, receipt, use, and others in the forms of communication infrastructures of wire, wireless, light beam, satellite as well as electronic formats. Information infrastructure protection regulations should be expanded to cover diverse structures from only the major information communication infrastructures, and more effort should be invested in stipulating basic areas in national information protection such
information infrastructure protection measures, attack response systems, information protection training and promotions, etc. (Korea Policy Portal, 2008).

As was seen from the 1.25 Internet Crisis (On January 25, 2008, the Internet was entirely paralyzed, causing a crisis and approximately 220 billion won in damages), the cyber attacks are rapidly emerging as a nationwide and social threat and is a direct risk factor to national security. Each national worldwide are fiercely engaging cyber information warfare to exploit the opponent nation’s secrets or national functions (June 2004 government agency system hacking incident originating from China; May 2004 attempts to paralyze Estonia’s information communications networks originating from Russia). As cyber attacks may have a serious national and social impact on a nation or society, it has already been identified as a new national security risk factor to which a response system by private and public sectors has faced its limits. Korea does not have policies, specific methods and processes with which to systematically manage nationwide cyber crises, and could cause a great threat and serious damage to national security and national interest in the break out of a cyber crisis. Therefore, legislation must be passed to enable pre-cyber attacks detection and prevention of crisis break outs, and to consolidate all national resources for a comprehensive national response system in which both the private and public sectors participate (Security News, 2008).

Second, efficiently ensure nationwide cyber security, a national cyber security standard and models should be proposed, and meanwhile a national cyber security management structure and system should be established to implement national cyber security policies at each government-agency and social-component levels. By developing a consistency in information protection laws, policies and programs through integrating and revising legislation and implementation systems, we will be able to more effectively respond to various threats to information protection. Therefore, the government should expand and strengthen the functions of its current ‘National Cyber Security Center’ to perform its integrated national cyber crisis management role in the areas of national cyber security management policy planning and coordination. Foremost, it must serve as the comprehensive collection, analysis, and processing of national cyber crisis related information, oversee each government and public agency, and establish a collaborative system with the private sector.
For voluntary information protection level evaluations public agencies’ Information Protection Management System authentications should be expanded; new regulations on administrative information protection system selections and use should be passed to simplify procurement of information protection products at administrative offices and propel their use; and establish regulations that promote sharing of attack information; and by setting attack information sharing regulations among information systems operators and information sharing/analysis centers, etc., so that we may effectively protect our national and social facilities from cyber attacks (Korea Policy Portal, 2008).

Also, a nationwide and comprehensive response system in which both government and the private sectors participate should be established to cyber attack detections before the fact and to block cyber crisis risks at an earlier stage, and in case of a breakout a nationwide effort shall be mobilized for quick response (Security News, 2008).

Finally, the National Cyber Security Center should serve the following functions. It’s major roles should include: 1) major policy planning, oversight and coordination related to national cyber security management; 2) planning and coordinating national cyber security management systems, warnings, drills, practice, and evaluations, etc.; 3) coordination and council on national cyber security management institutional efforts; 4) integrated response execution and coordination in the occurrence of a national cyber crisis; 5) establishment and implementation of national cyber crisis preventative policies; 6) determination of emergency response measures to be implemented by individual institutions in time of a national cyber attack incident; and 7) development of damage recovery and stabilization measures following a national cyber crisis.

IV. CONCLUSION

Korea’s cyber security systems are governed based on the National Cyber Security Management Act (Executive Order 222), the Information Technology Infrastructure Protection Act (No. 8852), Information Technology Network Use Promulgation and Information Protection Act (No. 8867), Industrial Technology Information Security and Protection Act (No. 8900), Software Industry Promotion Act (No. 8852). Therefore, Korea
lacks a systematic national cyber security policy. In addition, cyber security organizations, including the National Cyber Security Center, Information Communication Infrastructure Protection Commission, Private Information Conflict Mediation Commission, Industrial Technology Protection Commission, Software Business Conflict Mediation Commission, etc., are also dispersed over various sectors, and needs to be reorganized. Therefore, this research suggests the following solutions.

First, the National Cyber Security Management Act should be passed to have its effectiveness as the national cyber security management regulation. With the Act’s establishment, a more efficient and proactive response to cyber security management will be made possible within a nationwide cyber security framework, and define its relationship with other related laws. The newly passed National Cyber Security Management Act will eliminate inefficiencies that are caused by functional redundancies dispersed across individual sectors in current legislation.

Second, to ensure efficient nationwide cyber security management, national cyber security standards and models should be proposed; while at the same time a national cyber security management organizational structure should be established to implement national cyber security policies at each government-agencies and social-components. The National Cyber Security Center must serve as the comprehensive collection, analysis and processing point for national cyber crisis related information, oversee each government agency, and build collaborative relations with the private sector. Also, national and comprehensive response system in which both the private and public sectors participate should be set up, for advance detection and prevention of cyber crisis risks and for a consolidated and timely response using national resources in times of crisis.
REFERENCES


Korea internet security center : http://www.krcert.or.kr
Korea information security agency : http://www.kisa.or.kr

Ministry of Knowledge and Economy Press Release “Industrial Technology Protection general planning decision” 2008.8, 21

National Security Research Institute : http://www.nsri.re.kr
National cyber security center : http://www.nsri.re.kr
National intelligence service : http://www.nesc.go.kr
Prosecutors’ office : http://icic.sppo.go.kr

Security News (2008) “21C the National Cyber Security Management Act (Executive Instructional Order 222) verification”

The National Intelligence Service (2005) National cyber security measures

The republic of korea defense security command