법제교류 연구 16-18-④
International Legal Collaboration Research 16-18-④

A Comparative Study on Cybersecurity Legislation in Mongolia and South Korea

Hye-Shin Cho · Batbayar Enkhee · Galbaatar Lkhagvasuren · Doljin Sodnom · Odgerel Tseveen

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

법제교류 연구 16-18-④
International Legal Collaboration Research 16-18-④

A Comparative Study on Cybersecurity Legislation in Mongolia and South Korea

Hye-Shin Cho · Batbayar Enkhee ·
Galbaatar Lkhagvasuren · Doljin Sodnom ·
Odgerel Tseveen

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

A Comparative Study on Cybersecurity Legislation in Mongolia and South Korea

연구자 : Hye-Shin Cho (Handong Global University)
Batbayar Enkhee (National Legal Institute of Mongolia)
Galbaatar Lkhagvasuren (Judicial General Council of Mongolia)
Doljin Sodnom (National University of Mongolia)
Odgerel Tseveen (National Legal Institute of Mongolia)

2016. 10. 20

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

Abstract

Ⅰ. Purpose and Scope of Research

□ Cyber security issues have recently become considered as some of the most pertinent emerging agenda in Mongolia and South Korea. Now, cyberspace has become an environment for crime, hacking, and terror.

□ South Korea, which has a high reputation as an “Internet Strong Nation,” is expected to play a contributory role in the cybersecurity sector. On the other hand, in Mongolia the legal frameworks on cyber law and information security has not been sufficiently studied and developed in Mongolia.

□ This research aims to develop reasonable comments, solutions, and conclusions that lead to recommendations for effective and trustworthy legislative solutions in Mongolia and South Korea.

Ⅱ. Contents

□ In Mongolia, until 2002, legal provisions and sanctions did not exist for those who commit a crime in the information sector. The first legislation regarding cybersecurity was included in

the Mongolian Criminal Law in 2002, under the title, “Crime against computer information.”

□ With the advent of modern technology and the proliferation of activities involving exchanges of information, the need for the protection of human rights in cyberspace has been in discussion since 2010. Even though the Mongolian E-government has steadily made progress, human rights and freedom are still not being considered thoroughly enough in cyberspace.

□ The Information Technology, Post and Telecommunication Authority of Mongolia have been forming working groups to develop a draft law on data protection. Furthermore, the Mongolian parliament has been discussing a draft law on information security. As a part of creating an enabling legal environment, the Law on e-Signature and more than ten priority standards related to information security were approved, and currently, relevant organizations are working on drafting laws on cybersecurity and data protection. The Cyber Security Department has submitted the draft law on information security to the Parliament in February 2016.

□ Recently, National Cybersecurity Center has been forming working groups to develop a Draft Law on Cyber Security. The Minister of Justice and the Chairman of the General Intelligence Agency have approved, by a joint decree, the concept of Draft Law on Cyber Security.

□ Korea shows a high dependency on Information Communications, and Korea also has a highest Internet usage rate and the largest number of Internet users in the world. On the other hand, the risks of injurious behaviors or infringements of basic human rights that happen in cyberspace such as infringement of personal data, leakage of business information, cybercrime, or cyber terror also increase along with the exponential growth of dependency on cyberspace. On top of this, in case of South Korea, the possibility of cyber terror by North Korea stands as a very serious danger factor.

□ Korean cybersecurity legislation has developed in reaction to the advancement of Information Communication and its related technologies and infrastructures, as well as the counteracts to increasing cyber danger factors. The occasional cybersecurity related incidents and accidents, and the following frequent enactments and revisions of legislation directly show the progress of rapid maturation of Korean cybersecurity legislation.

□ In comparison, amongst all, one aspect to pay attention to in Korean cybersecurity legislation is the governance encompassing public as well as private sector. Besides, establishing a governance that leads out private sector's capacity and voluntary compliance is crucial, and Korean cybersecurity legislation seems to have a strong suit in this aspect.

□ By the way, in spite of the short history of development of cybersecurity legislation, Mongolia puts much effort in counter-acting to international cybercrime or cyber terror in cooperation with the related countries. Also, it is worth paying attention to the systematization of legislation based on the concept of National Security Concept, and its subcategories. A broader and more systematized cybersecurity legislation is expected once the Law of Data Protection Act, which is in the process of enactment, and legislations such as Law Information Security enact.

Ⅲ. Expected Effects

□ It is very likely that Mongolia will not experience the same process of development of ICTs and related legislations that South Korea has experienced. Therefore, if Mongolia carefully analyzes the technologies and legislations of those countries, as well as Korea, who already established these aspects, Mongolia will be able to find the most suitable legislation and governance in the near future. For such reasons, a cooperation and further research of related countries, especially Mongolia and South Korea whom were subject to this research, are expected.

➧ Key Words : Cybersecurity, Mongolia, South Korea, National Security, Cyber Crime, Information Protection.

Contents

Glossary

Korean	English
집적정보통신시설	Accumulated Information Communication facility
정보통신서비스	Information Communications Service
미래창조과학부	Ministry of Science, ICT, and Future Planning (“MSIP”)
미래창조과학부장관	Minister of MSIP
<보안업무규정> (대통령령)	<Security Operation Regulation> (Presidential Decree)
<정보및보안업무기획*조정규정> (대통령령)	<Intelligence and Security Business Planning, Rules, and Regulations> (Presidential Decree)
<전산망 보급확장과 이용촉진에 관한 법률>	<Act on Expansion of Dissemination and promotion of Utilization of Information System>
제어시스템 보안 워크숍	Workshop on Information Security and Cryptology (“WISC”)
한국정보보호학회	Korea Institute of Information Security and Cryptology (KIISC)
정보통신부	The Ministry of Information and Communication
한국정보보호센터	Korea Internet & Security Agency (KISA)
한국정보보호산업협회	Korea Information Security Industry Association (“KISIA”)
블록암호 알고리즘	Block cryptographic algorithm (SEED)
정보보호시스템 평가*인증 제도	Evaluation and authentication system of the information security system

Korean	English
<전산망보급화장과이용촉진에 관한법률>	<Act on Promotion of Utilization of Information and Communications Network>
<국가정보통신보안기본지침>	<National Information Communications Security Guidelines>
<전자서명법>	<Digital Signature Act>
국가보안기술연구소	National Security Research Institute (NSR)
<정보통신기반 보호법>	<Act on the Protection of Information and Communications Infrastructure>
<전자정부구현을위한행정업무등의전자화촉진에관한법률>	<Promotion of Digitalization of Administration for Materialization of Digital Government Act>
<정보통신망 이용촉진 및 정보보호 등에 관한 법률>	<Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.>
한국사이버테러정보전학회	Korea Information Assurance Society (KIAS)
한국정보보호진흥원	Korea Information Security Agency (KISA)
국가정보보호백서	National Information Security White Paper
국가정보보안연합회	National Information Security Association (NISA)
정보보호시스템 공통평가기준	Information security system evaluation's Common Criteri (CC)
1.25 인터넷 대란	1.25 Internet Crisis
인터넷침해사고대응지원센터	Korea Internet Security Center (KrCERT)
대국민 행정서비스용 블록암호 알고리즘	National Block Cipher for Administrative System (ARIA: Academy, Research, Institute, Agency) was developed

Korean	English
국가사이버안전센터	National Cybersecurity Center
<국가위기관리기본지침>	<National Cybersecurity Crisis and Emergency Management Manual>
<국가사이버안전관리규정>	<National Cybersecurity Management Regulation>
사이버안전의 날	Day of Cybersecurity
국제상호인정협정	Common Criteria Regulation Arrangement (CCRA)
<전자정부법>	<Electronic Government Act>
방송통신위원회	Korea Communications Commission
행정안전부	Ministry of Public Adminstration and Security
지식경제부	Ministry of Knowledge Economy
보안관제체계	Security control centers
7.7 DDos 침해사고	7.7 Ddos infringement
국가 사이버위기 종합대책	National Cyber Crisis Comprehensive countermeasures
한국인터넷진흥원	Korea Internet & Security Agency (KISA)
정보통신국제협력진흥원	Korea ICT International Cooperation Agency
한국지식정보보안산업협회	Korea Information Security Industry Association (“KISIA”)
사이버사령부	Cyber Warfare Command
전자금융거래	Electronic financial transaction
공인인증	public certification authority system
<개인정보 보호법>	<Personal Information Protection Act>
3.4 DDos 침해사고	3.4 DDos infringement incident

Glossary

Korean	English
국가 사이버안보 마스터플랜	National Cybersecurity Master Plan
정보보호의 날	Information Protection Day
민관군 사이버위협 합동대응팀	Civil-Government-Military joint response team against cyber threat
3.20 사이버테러	3.20 Cyber Terror
6.25 사이버공격	6.25 Cyberattack
국가 사이버안보 종합대책	Comprehensive plan on cybersecurity measures
정보보호최고책임자협의회	Chief Information Security Officer (CISO) Conference
사이버안전훈련센터	Cybersecurity Training and Education Center (CSTEC)
<정보보호산업의 진흥에 관한 법률>	<Promotion of Information Security Industry Act>
개인정보 유효기간제	Personal Information Expiration System
금융보안원	Financial Security Institute (FSI)
한국전자통신연구원	Electronic and Telecommunications Research Institute (ETRI)
정보통신기술	Information and Communications Technologies (ICT)
사물인터넷	Internet of Things (IoT)
랜섬웨어 침해대응 센터	Ransomware Computer Emergency Response Team Coordination Center (Ran CERT)
국방부	Ministry of National Defense
국군기무사령부	Defense Security Command
국군사이버사령부	Defense Cyber Command
국가정보원	National Intelligence Service (NIS)

Korean	English
국가안보실	National Security Office (NSO)
미래전략수석실	Future Strategy Office (FSO)
국가정보원장	Head of NIS
사이버안전전략회의	National Cybersecurity Strategy Council ("Council")
사이버안전기본계획	Cybersecurity Master Plan
미래창조과학부	Ministry of Science, ICT, and Future Planning ("MSIP")
국가사이버안전센터	National Cybersecurity Center
국가사이버안전전략회의	National Cybersecurity Strategy Meeting
국가사이버안전대책회의	National Cybersecurity Countermeasure Meeting
사이버안보비서관	Secretary of Cyber Ssecurity
중앙행정기관	Central Administrative Agency
지방자치단체	Local governments
개인정보보호 관리체계	Personal Information Management System (PIMS)
인터넷침해대응센터	Korea Internet Security Center (KISC)
대학정보보호동아리	Korea University Clubs Information Security (KUCIS)
정보보호산업지원센터	Korea Information Security Industry Support Center (KISIS)
정보보호와 암호에 관한 국제학술대회	Annual International Conference on Information Security and Cryptology (ICISC)
IT보안인증사무국	IT Security Certification Center (ITSCC)
공동평가기준	Common Criteria (CC)

Korean	English
개인정보보호협회	Korea Online Privacy Association (OPA)
위치기반서비스	Location Based Service (LBS)
한국개인정보보호협회	The Korean Council on the Protection of Personal Information (KCPPI)
한국산업기술시험원	KTL
한국아이티평가원	KSEL
한국정보보안기술원	KOIST
한국융합보안학회	Korea Convergence Security Association (KCSA)
개인정보관리사	Certified Privacy Protection General (CPPG)
공공부문 정보보호	A Public Sector Information Protection
민간부문 정보보호	A Private Sector Information Protection
정보통신망	information network system (INS)
인증서발행국	Certificate Authorizing Participants (CAP)
인증서수용국	Certificate Consuming Participants (CCP)
평가 보증 등급	Evaluation Assurance Level (EAL)
국제침해사고대응팀협의회	Forum of Incident Response and Security Teams (FIRST)
행정전자서명 인증체계	Government Public Key Infrastructure (GPKI)
한국정보통신진흥협회	Korea Association for ICT Promotion (KAIT)
한국정보기술연구원	Korea Information Technology Research Institute
정보통신기반시설	ICT infrastructure

Korean	English
정보통신기반보호위원회	Information Communications Infrastructure Protection Committee
국무조정실장	head of the office for Government Coordination
국가정보화 기본법	<Framework Act on National Informatization>
전자무역촉진에 관한 법률	<Electronic Trade Facilitation Act>
군사기밀보호법	<Military Secret Protection Act>
산업기술의 유출방지 및 보호에 관한 법률	<Act on Prevention of Divulgence and Protection of Industrial Technology>
기술의 이전 및 사업화 촉진에 관한 법률	<Technology Transfer and Commercialization Promotion Act>
민.군겸용기술사업촉진법	<Promotion of Technology Projects for Joint Civilian and Military Use Act>
신용정보의 이용 및 보호에 관한 법률	<Credit Information Use and Protection Act>
민간분야실무위원회	Private Sector Administrative Committee
전자문서 및 전자거래 기본법	<Framework Act on Electronic Documents and Transactions>
금융실명거래 및 비밀보장에 관한 법률	<Act on Real name Financial Transactions and Confidentiality>
인터넷주소자원에 관한 법률	<Internet Address Resources Act>
위치정보의 보호 및 이용 등에 관한 법률	<Act on the Protection, Use, Etc. of Location Information>
통신비밀보호법	<Protection of Communications Secrets Act>
개인정보보호위원회	Personal Information Protection Committee
행정자치부	Ministry of Government Administration and Home Affairs

Chapter 1. Introduction

Ⅰ. Research Background and Purpose

Cyber security issues have recently become considered as some of the most pertinent emerging agenda in Mongolia and South Korea. Now, cyberspace has become an environment for crime, hacking, and terror. Governments, private companies, and non-state actors are making efforts to develop stronger capabilities for securing their resources and activities in cyberspace. Amid the fast spread of these new problematic phenomena, many countries and international organizations focus more on crafting security measures and enhancing multilateral cooperation to fend off cyber-threats.

South Korea, which has a high reputation as an “Internet Strong Nation,” is expected to play a contributory role in the cybersecurity sector. Its cutting-edge digital technology, efficient computer networks, and the world's top high-speed internet penetration rate could lead to its vulnerability to cyber threats, especially suspected as the work of North Korea. In the same vein, South Korea takes a national security and defense-focused approach to cybersecurity.

In Mongolia also, data access and ownership rights, data privacy and confidentiality, freedom of information, legal publishing, preservation and management of legal information, the internet and social media regulation and the malicious use and misuse of data are emerging topics. Since 2010, National Security Concept has been the basic regulation of information security such as cybersecurity. But the legal frameworks on cyber law and information security has not been sufficiently studied and developed in Mongolia. Therefore, it is timely and meaningful to conduct a comparative study on Cyber Law and Cybersecurity Issues in Mongolia and South Korea in order to share experiences and develop the solutions to these problems together.

Ⅱ. Research Methodology

This research uses empirical analysis, case analysis, and comparative analysis methods, to develop reasonable comments, solutions, and conclusions that lead to recommendations for effective and trustworthy legislative solutions in Mongolia and South Korea.

The methodology is also principally analytical. The primary materials, especially cybersecurity, provided a basis for analyzing the types of legislation that drive the system and the interests considered relevant enough to be covered in that legislation, while secondary materials included analyses of scholarly books, articles, and reports. In conducting this research, there were also substantial reviews and analyses of literature on international laws and policies related to cybersecurity. In addition to these sources, this research focused on their analysis of cybersecurity legislations and the backgrounds to issues.

This research has been jointly conducted by Korean and Mongolian research team. Mongolian research team put together the first and second chapter <Introduction> and <Current Cybersecurity Legislations in Mongolia>, and Korean research team wrote third and fourth chapter, <Current Cybersecurity Legislations in South Korea> and <Conclusion>. Particularly for chapter three and four, Haedn Cha (Handong International Law School) and Ching-Chan Lee (Handong Global University, Law Department) aided the research as Research Assistants.

Chapter 2. Current Cybersecurity Legislations in Mongolia

Ⅰ. Development of Regulatory Framework

In Mongolia, according to the Democratic Constitution which was put into force in 1992, all information except personal, organizational, and state secret became open to the public. Due to this major change in the social system, different types of legislation stood in need of an effective legal system. Until 2002, legal provisions and sanctions did not exist for those who commit a crime in the information sector. The first legislation regarding cybersecurity was included in the Mongolian Criminal Law in 2002, under the title, “Crime against computer information.”

However, due to the lack of knowledge among the majority of law enforcement officers, judicial officers, and judges on what information, data, or cybersecurity is, or how an investigation should be conducted, this new statute was not effective at all. Over the past 14 years, only a few number of information crimes were registered with the police or investigation departments. The majority of them were not submitted to the court, which means that most cases of crimes against information security were shrouded in Mongolia until today.

According to the United Nations E-Government survey, Mongolia ranked 76th out of 193 countries in 2012 and ranked 65th in 2014.[1] In addition, according to the International Telecommunication Union report, Mongolia ranked 84th out of 193 countries in 2015.[2]

[1] United Nations E-Government Survey 2014 E-Government For The Future We Want. Dec 8, 2014 http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf

Another indicator of the level of cybersecurity in Mongolia is the Global Cybersecurity Index (GCI), which aims to effectively measure each nation state's level of cybersecurity development. Launched by the International Telecommunication Union (ITU), this initiative's ultimate goal is to help foster a global culture of cybersecurity and its integration at the core of information and communication technologies. The GCI initiative establishes its basis upon the current mandate of the ITU and the related projects and activities of the ITU's Telecommunication Development Bureau, the BDT.[3]

Global Cybersecurity Index and Cyberwellness Profiles by ITU (2015)[4]

Country	*Index*	*Global Rank*
The United States of America	0.824	1
The Republic of Korea	0.706	5
Russia	0.500	12
China	0.441	14
Mongolia	0.412	15

With the Global Cybersecurity Index of 0.412, Mongolia shares the global rank of 15 along with four other nations, Argentina, Cameroon, Croatia, and Kenya; and is ranked behind 52 nations. In an effort to increase the GCI and rank higher, the Mongolian government adopted the

[2] International Telecommunication Union (ITU). Measuring the Information Society Report 2015. p.46 http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf

[3] Conceptual Framework, Global Cybersecurity Indexhttps://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_Conceptual_Framework.pdf

[4] Global 2015 results of Global Cybersecurity Index and Cyberwellness Profiles by ITU http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf
ABIResearch. "Global Cybersecurity Index & Cyberwellness Profiles". *Report*. ITU.April 2015. http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

"E-Governance National Program" in 2012, which will be implemented until 2016.[5] This is an action program by the Mongolian government and its agencies; and it is also included in the "National Security Concept" as the main policy on e-governance and information security in the country.[6]

With the advent of modern technology and the proliferation of activities involving exchanges of information, the need for the protection of human rights in cyberspace has been in discussion since 2010. Even though the Mongolian E-government has steadily made progress, human rights and freedom are still not being considered thoroughly enough in cyberspace. The official responsibility of a government is to ensure the human rights and the basic liberties of its citizens, not only in the physical environment, but also in cyberspace, by adopting laws such as cybersecurity legislation and data protection act.

Ⅱ. Main Issues in Establishing Cybersecurity-Related Laws

1. Protection for Human Rights and Freedom in Cyberspace

On December 18th, 2013, the UN General Assembly adopted resolution 68/167 (The Right to Privacy in the Digital Age), which called on its member states to implement measures to put an end to the violation of the right to freedom of expression, the right to seek, receive, and

[5] 101st Resolution of the Mongolian Government on E-Governance has passed on 4th of April, 2012 http://legalinfo.mn/annex/details/6019?lawid=9465

[6] 48th Resolution of the Mongolian Great Khural on National Security Concept has passed 15th of July, 2010

disseminate information.[7] In Mongolia, information on newly advanced technology and internet usages has been on a constant increase each year[8]; and as a UN Member State,[9] it adopted the policies and regulatory acts from the resolution 68/167.

2. Legal Regulation of Data Protection[10]

Data protection issues have created the conditions that negatively impact the safety and inviolability of the information including organizational data as well as secrecy on the private matter due to the vulnerability of citizen's legal awareness.

Therefore, the Information Technology, Post and Telecommunication Authority of Mongolia have been forming working groups to develop a draft law on data protection.[11] Currently, online businesses and the usage of online services are increasingly growing in Mongolia, resulting in a centralization of data in the digital environment. The process of data collection: processing, transmission, verification and storing activities are

[7] Resolution adopted by the General Assembly on 18 December 2013
http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167;
General Assembly. UN. The right to privacy in the digital age. November 2013.
http://www.hrw.org/sites/default/files/related_material/UNGA_upload_0.pdf;
http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

[8] Main Indicators of Telecommunications Sector by 1st half of 2015. Communications Regulatory Commission of Mongolia. http://crc.gov.mn/main.php?cid=1&do=191&did=0

[9] Mongolia and the United Nations http://www.un.int/mongolia/mongolia/mongolia-and-united-nations-0

[10] Definition of Data : The quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media. http://www.oxforddictionaries.com/definition/english/data

[11] Annual report 2014 of Information technology, Post and Telecommunication Authority of Mongolia (ITPTA) http://itpta.gov.mn/new/?page_id=6490

expanding, and at the same time leading to the trends of losing data protection, creating data overlapping and further having a tendency to violate the privacy of public organizations and individuals. As of today, there is no specific regulation on the protection of data and information of individuals, organizations, and the public. The draft law, in addition to covering matters related to internal communication, also addresses matters related to global technological development trends such as Cloud computing, relationship, and regulation related to the usage of big data.[12]

The Structure of the Draft Law on Data Protection of Mongolia[13]

Chapter 1. General provisions	- The framework of the law - The purpose of the law - Legal definitions - Legislations on data protection - Types of data - Biometric data
Chapter 2. The data protection system	- Protection of personal data - Obligations of organizations and officers for ensuring and controlling the implementation of the law
Chapter 3. Principles and requirements for data protection	- Principle of data protection - The purpose of data protection - Limitlessness of data protection - Public data resources

[12] ITPTA. White Paper on the development of the ICT-2016. p. 11. http://cita.gov.mn/wp-content/uploads/2015/06/KHARILTSAA_KHOLBOO_TAILAN_ENGLISH.pdf
Working group of the draft law. The Concept of the draft law on data protection of Mongolia. 2015.08.31.

[13] Working group of the draft law. The Concept of the draft law on data protection of

Chapter 4. Rights and obligations of the data holder	- Access to the data - Rights of the data holder on marketing and political activities - Rights of the data holder on data processing - Complaints about illegal operators operating - Approval of data holder on data processing
Chapter 5. Rights and obligations of the data developer	- Personal data protection on information systems of state organizations, local administration organizations, and public registration office - Obligations of the operator on collecting personal data - Security in processing personal data - Obligations of the operator on the disclosure of personal data - Obligations of the operator in detecting incidents, and collecting, developing, transferring, blocking and removing personal data - Obligations to notify about developing personal data
Chapter 6. Control and Liability	- Internal control on the security of data processing - Organizational and technical measures of data processing on data security - Duties on system registration of data and monitoring bodies
Chapter 7. Miscellaneous	- Entry into force

Mongolia. 2015.08.31

3. Legal Regulation on Cyber Crime

According to the Mongolian Criminal Code, the target or the object of cybercrime includes PC, software program, hardware devices, data that are saved and transmitted through information network, data protected network, and computer based data.[14] In regards to the court resolved cybercrime cases in Mongolia, there were quite a lot of children among the cybercrime victims, who did not even know that they had become a victim and for how long they have been victimized.[15]

According to the National Program for Information Security, public organizations such as National Intelligence Agency, National Police Authority, and Information Technology, Post and Telecommunication Authority are responsible for the implementation of these codes in order to combat cybercrime.[16] The main purpose of this program is to ensure national security and to protect the citizens' fundamental rights and freedoms by creating an electronic database of Mongolian government agencies, non-governmental organizations, citizens, businesses, and the supporting infrastructure through a gradual implementation of the measures.[17] The program was implemented from 2010 to 2015[18], and in the implementation process, the

[14] Criminal Code of Mongolia, 2002
http://www.unodc.org/res/cld/document/mng/2001/criminal_code_of_mongolia_html/Mongolia_Criminal_Code_2002.pdf

[15] Electronic database of Mongolian Court Decisions.
Case Index 105/2015/0230/э http://www.shuukh.mn/eruuanhan/8177/view
Case Index105/2015/0270/эhttp://www.shuukh.mn/eruuanhan/7992/view

[16] 141st Resolution of the Mongolian Government on National Program for Information Security has passed 2nd of June, 2010

[17] National programs. CRChttp://www.crc.gov.mn/en/k/1g/1q

[18] Cyberwellness Profile Mongolia https://www.itu.int/en/ITU-D/Cybersecurity/Documents/

assessment of information security risks was conducted among various government organizations. New departments such as the Cyber Security Department within the General Intelligent Organization and the Cyber Crime unit of NPA at the Criminal Police department have been established along with public and non-government CERTs. Also, a number of activities have been organized every year as a tradition to inform those organizations and the general public about cybersecurity, such as “Information Security Day”, “KharuulZangi” ethical hiking contest, and other activities which bring specific results. Considering that the implementation period of the current program is coming to an end, there are studies being carried out on developing the program anew.[19]

However, despite the implementation of National Program for Information Security by the Mongolian government, cyber-attacks and threats to cybersecurity have been continuing.[20] Therefore, there is a constant need to ensure cybersecurity in Mongolia. As a response, the Mongolian parliament has been discussing a draft law on information security.[21] As a part of creating an enabling legal environment, the Law on e-Signature and more than ten priority standards related to information security were approved, and currently, relevant organizations are working on drafting laws on cybersecurity and data protection. The Cyber Security Department has submitted the draft law on information security to the Parliament in February 2016.

Country_Profiles/Mongolia.pdf

[19] ITPTA. White Paper on the development of the ICT-2016. p. 18. http://cita.gov.mn/wp-content/uploads/2015/06/KHARILTSAA_KHOLBOO_TAILAN_ENGLISH.pdf

[20] IT Expert underlines the need for firm cyber security measures and public awareness. The UB Post. 2016.03.14 http://ubpost.mongolnews.mn/?p=18801

[21] Draft Law on Information Security of Mongolia. Website of Mongolian Parliament 2016.04.05. http://www.parliament.mn/laws/projects/814

The purpose of the law on information security is to regulate relations in regards to cybersecurity in Mongolia and to protect the rights of the citizens and legal entities so that they may seek and receive specific guidelines on cybersecurity.

4. Legal Issues on Censorship and Internet Filter

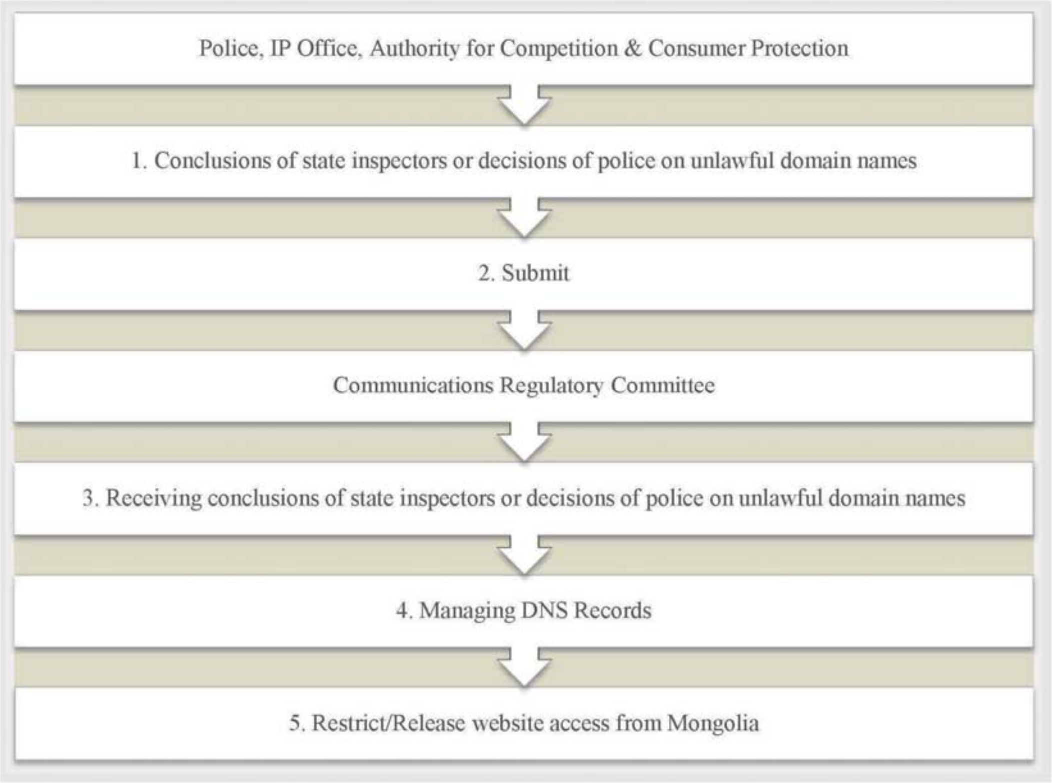
According to the resolution No. 8 “General Condition and Requirement on Digital Content” (2011) adopted by the Communications Regulatory Committee (CRC) of Mongolia, internet providers must use a government specified filtering system.[22] This resolution--which was amended twice from 2012 to 2015 on areas such as the content aggregator, website service provider, a log file of users’ comments, and complaint management--mandates that the IP addresses of the customers be publicly visible under the user-generated content. It has been restricting the individual’s right to anonymity in an unlawful way. For example, by April 1st, 2015, the CRC had restricted a total of 217 websites from being accessed from Mongolia.[23] But the number of restricted sites from 2015 to present remains undisclosed.[24]

[22] Resolution No 8 of 2011 on “General Condition and Requirement on Digital Content” adopted by the Communications Regulatory Committee (CRC) of Mongolia http://crc.gov.mn/file/newfile/togtool-2014-40.pdf

[23] List of Offensive Domain Names. Communications Regulatory Committee (CRC) of Mongolia http://www.black-list.mn/index.php

[24] http://www.black-list.mn/

The Process of Restricting or Releasing Unlawful Domain Names/ Websites in Mongolia


Police, IP Office, Authority for Competition & Consumer Protection
1. Conclusions of state inspectors or decisions of police on unlawful domain names
2. Submit
Communications Regulatory Committee
3. Receiving conclusions of state inspectors or decisions of police on unlawful domain names
4. Managing DNS Records
5. Restrict/Release website access from Mongolia

5. Actions Towards National Security

The National Cybersecurity Center of General Intelligence Agency is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy, and roadmap in Mongolia. In addition, the National Cybersecurity Center has been forming working groups to develop a Draft Law on Cyber Security. The Minister of Justice and the Chairman of the General Intelligence Agency have approved, by a joint decree, the concept of Draft Law on Cyber Security.[25] Cybersecurity has

[25] Cyberwellness Profile Mongolia https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Mongolia.pdf

become one of the issues receiving global attention at the current stage of rapid development in information technology. Since 2002, policy developers of the information and telecommunications sector have been conducting surveys and studies related to information security and the legal environment. This resulted in the drafting of a law and recommendations on cyber security which were presented at the National Security Council in 2008. The draft law and related materials were transferred to newly established Cyber Security department in 2012 according to their functions. The Cyber Security department has drafted a new law on information security and has submitted it for approval to the Parliament in February, 2016.

The approval of this law will allow for the establishment of the framework for nationally integrated management and monitoring on information security. It would also define the roles, participations, and responsibilities of the government and private citizens to ensure information security of information which they own and create a favorable legal environment to reduce potential psychological and economic damages of organizations and the general public.[26]

The Structure of the Draft Law on Information Security of Mongolia[27]

Chapter 1. General provisions	Article 1. The purpose of the law
	Article 2. Legislation of cybersecurity
	Article 3. Framework of the law
	Article 4. Legal definitions
	Article 5. Principles of ensuring cybersecurity

[26] ITPTA. White Paper on the development of the ICT-2016. p. 10. http://cita.gov.mn/wp-content/uploads/2015/06/KHARILTSAA_KHOLBOO_TAILAN_ENGLISH.pdf

[27] Draft Law on Information Security of Mongolia. Website of Mongolian Parliament 2016.04.05. http://www.parliament.mn/laws/projects/814

Chapter 2. Competence of organizations and citizens on ensuring cyber security	Article 6. Competence of the Parliament
	Article 7. Competence of the Government
	Article 8. General obligations of the organizations and citizens
	Article 9. Obligations of state organizations on ensuring cybersecurity
	Article 10. Obligations of critical infrastructure organizations on ensuring cybersecurity
	Article 11. Competence of the state administrative body in charge of information and communication issues
	Article 12. Competence of the General Intelligence Agency on ensuring cybersecurity
Chapter 3. Activities on ensuring cybersecurity	Article 13. Activities on ensuring cybersecurity
	Article 14. Preparing and implementing policy or standard on cybersecurity
	Article 15. Ensuring security of information database and information systems
	Article 16. Risk assessment on information security
	Article 17. Detecting and combating incidents on cybersecurity
	Article 18. Combating cybercrime
	Article 19. Services on cybersecurity
	Article 20. International cooperation on cybersecurity
Chapter 4. Control of activities on ensuring cybersecurity	Article 21. Control of activities on ensuring cybersecurity
Chapter 5. Miscellaneous	Article 22. Finance of activities on ensuring cybersecurity
	Article 23. Liabilities
	Article 24. Entry into force

There is a need for Mongolia to become a party to the Convention on Cybercrime, which was convened on November 23rd, 2001 in Budapest.[28)] Mongolia has defined its foreign policy to actively engage in the international peacekeeping operation; and in the field of national security and defense, it has continued to develop various bilateral and multilateral relationships and cooperation with other countries, including its two neighboring countries (Russia and China), the USA, NATO member countries, the European Union, and the countries of the Asia-Pacific regions.[29)]

Ⅲ. Current State of Related Laws and Regulations

1. Overview

According to Article 11 of the Constitution of Mongolia, it is the duty of the State to ensure national security and public order. Also, under Article 19 of the Constitution, one shall not infringe on national security, rights, and freedoms of others, or violate public order in exercising his or her rights and freedoms. Nowadays, cybersecurity directly pertains to national security. Therefore, it can be understood that the Mongolian Constitution regulates Mongolian cybersecurity as well.

The Great Khural (Parliament) of Mongolia passed the renewed National Security Concept of Mongolia at its plenary session on July 15th, 2010.

28) Convention on Cybercrime. Budapest, 23.XI.2001. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

29) 48th Resolution of the Mongolian Great Khural on National Security Concept has passed 15th of July, 2010

It announced that national security shall consist of the following main components:[30)]

- Security of the existence of Mongolia;
- Security of population and genetic identity;
- Security of civilization;
- Economic security;
- Internal security;
- Human security;
- Security of the natural environment; and
- Information security.

This renewed National Security Concept determined the ways and the means to ensure information security in Mongolia. Particularly in regards to the last component, information security, the researchers have been expressing the need to manage and regulate cybersecurity.

In order to regulate cybersecurity, it becomes necessary to define it explicitly. The CIA Triad defines information security as Confidentiality, Integrity, and Availability of information.[31)] Since 2010, Mongolia has incorporated this CIA Triad in the National Security Concept in relation to the management of cybersecurity.[32)]

[30)] http://www.nsc.gov.mn/sites/default/files/images/National%20Security%0Concept%20of%0Mongolia%20EN.pdf

[31)] Anthony Henderson. The CIA Triad: Confidentiality, Integrity, Availability. Panmore Institute. 2015.07
http://panmore.com/the-cia-triad-confidentiality-integrity-availability

[32)] National Security Concept of Mongolia,3.6.2, 3.6.3, 3.6.4. http://legalinfo.mn/annex/etails/3350?lawid=6163

CIA Triad in the National Security Concept of Mongolia

CIA	Explanation	Corresponding Clause in the National Security Concept
Confidentiality of information	“Safety shall be ensured through protection against illegal access, intrusion, and disclosure of information or its components.”	Clause 3.6.3.1
Integrity of information	“Integrity of information shall be ensured through protection of information, information space and infrastructure from illegal intrusion, manipulation or theft.”	Clause 3.6.2.1
Availability of information	“The availability of information shall be made by providing rights and freedoms to search, collect, generate, transmit and disseminate information not prohibited by law and free access to information infrastructure, components, and services.”	Clause 3.6.4.1

Corresponding to the National Security Concept organized above according to the CIA Triad, various Mongolian legislations on cybersecurity may be organized as in the following table. Details are provided in the following pages.

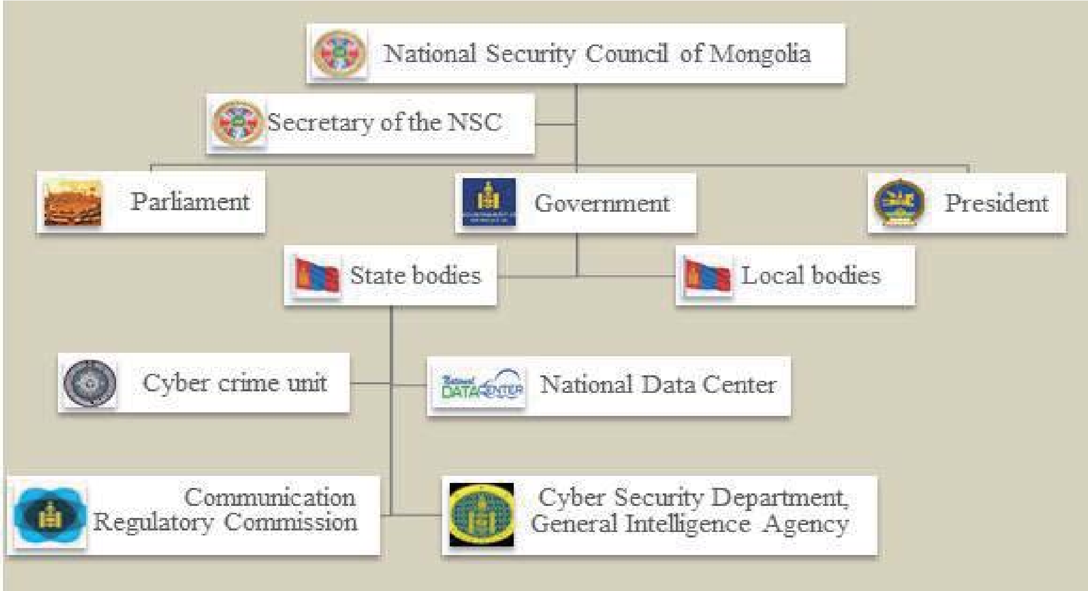
Mongolian Legislations on Cybersecurity

CIA	Explanation	Corresponding Clause in the National Security Concept
Confidentiality of information	- Law on State Secrets - Law on	- General Intelligence Agency - Legal entities - Individuals

CIA	Explanation	Corresponding Clause in the National Security Concept
	approval of the List for State Secrets - Law on Organization Secrets - Law on Individual's Secrets	
Integrity of information	- Criminal Code - Law on National Security	- National Police Agency of Mongolia - National Security Council - The State Great Khural - President of Mongolia - National Security Council - Government of Mongolia - Law enforcement and special task-force organizations (National Police Agency of Mongolia, the General Intelligence Agency) - Local governments
Integrity of information	- Law on the Information Transparency and Right to Information	- Secretariat of the State Great Khural(Parliament) - Office of the President - Government Cabinet - Administrative office of the National Security Council - State central administrative or other state administrative organizations - Judiciary and prosecutor offices of all instances - Institutions established by the State Great Khural with the exception of the Government Cabinet - Administrative offices of local municipal and self-governing bodies - Local government owned or partial ownership legal entities

CIA	Explanation	Corresponding Clause in the National Security Concept
		- State-owned or partially owned legal entities those - Non-governmental organizations executing the particular functions of the executive branch Mongolian National Public Radio and Television organization

National Cybersecurity Performance System and Directions


National Security Council of Mongolia
Secretary of the NSC
Parliament
Government
President
State bodies
Local bodies
Cyber crime unit
National Data Center
Communication Regulatory Commission
Cyber Security Department, General Intelligence Agency

2. Laws Related to Confidentiality of Information

(1) Law on State Secrets; Law on Approval of the List for State Secrets

According to the Law on State Secrets[33], no one shall search for, possess, or distribute state secrets. States secrets are defined as the materials

[33] Mongolian Law on State Secrets, 1995 https://www.agidata.org/pam/Legislation.axd/Mongolia(1995)StateSecrets%5BEN%5D.pdf.

that contain some information, documents, and items related to the cyber security of Mongolia. This definition is described in the provisions of the Law on Approval of the List for State Secrets.[34] State secrets are categorized into the following three levels: 1) Most confidential 2) Confidential and 3) Classified.

Scopes of State Secret

Within scope of the national security of Mongolia	1. The concept of the national security of Mongolia and the confidential parts of information, documents, and other matters for ensuring economic security as appropriate. 2. Vital information related to foreign policy and official opinion of Mongolia and agreements on their drafts of Mongolia established with other foreign countries, which are appropriate to be classified as confidential.
Within scope of intelligence, counterintelligence, and secret operations:	1. Intelligence and counterintelligence, proceedings, and information on methods, types, tools and facility, sources of information, a number of staff, organizational structure, documents, archive, database and financing used for secret operations. 2. The codified system of the government communication, and other relevant documents to this system, its encryption, method and proceeding to use them. 3. Information on supply and reserve of arms and special equipment to police, intelligence agencies, detention units, plans for operation during public disorder by police, intelligence agencies, and internal military units, information on tools and facility to protect vital important objects, plans for operation by detention units during war and within war period, and other relevant documents.

[34] Mongolian Law on approval of the list for state secrets http://www.forum.mn/res_mat/secrecylist_eng.pdf

	4. Actions were taken by state competent institutions in order to safeguard national security of Mongolia
Within scope of defense	1. Defense policy and concept, military doctrine, and classified parts of other related documents as appropriate. 2. Strategy, operative tactics, reports on their implementation, military strategy, operative and resource position, warfare operating documents for preparation for and performing battles, combat methods, readiness to military actions and mobilization, mobilization reserve, and information on its utilization. 3. Scientific and research, experimental and construction works with purposes to create, purchase, and renovate military equipment and programs implemented for these purposes and report of their implementation and their impacts. 4. Titles and types of secret armament and equipment, technical specification and potentials during battles. 5. Information on location, purposes, rating of readiness, protection, chart, and accompanying documents, or expenditure budget of strategically important objects for the national defense, and territories assigned for constructing objects, and other related materials. 6. Purpose, arms, and technical supplies, classified or specially appointed locations, authentic titles, an amount of weapons and troops of armed forces or other military troops. 7. The target of recruits, annual recruits and plans by the ministry of Mongolia and special agents in provinces and the capital city. 8. Organization, methods and operations of forces of the national borders, and border inspection authorities, other information related to them. 9. Plans to utilize public mobilization of civic protection and to provide public security during a public emergency and

	location and purposes of special objects and information and other items on ways to utilize infrastructure during the time.
Within scope of economy, science, and technology:	1. Scientific and research works, experiments, discovery, charts and national and other technology that have a vital bearing on state security, economy and defense. 2. Real and potential mobilization capacity of military production, the real amount and location of the national reserve. 3. Reserves, extraction, and supply amount of raw materials that are bearing vital importance on defense and economic security. 4. Methods and tools to protect state secrets, and actions are taken for this purpose and reports on them.

(2) Law on Organization Secrets[35)]

Law on Organization Secrets describes that “organization secrets” shall be reports, documents, and items defined as organization secrets according to the Mongolian legislation and that which contain in its information, a divulgence of which will cause harm to human dignity and the legal interest of an organization. Organization secrets include reports, documents, and items on cybersecurity of an organization.

Confidential information, technological solutions, and equipment may be considered to be an organization’s privacy if they are related to the unique activities of an organization or are protected by the organization in order to protect its markets or its advantages in the course of fair competitions, and that which may damage the legitimate interests of the organization.

[35)] Mongolian Law on Organizations Secrets, 1995 http://mongolianlaws.com/index.php?lid=LW1995051600&action=show

According to Article 5, the privacy of an organization shall be protected by the organization itself. Organizations shall develop and follow their internal procedures to protect their privacy in compliance with the laws. Also, persons in charge of confidential matters or those that had access to them in the course of their duties or professional activities shall have the duty to maintain strict confidentiality. They have the responsibility to protect not only the privacy of the organization, but also the privacy of the individuals. Organizations shall protect the privacy of individuals, to which they had access in the course of their activities, in the same way as they protect their own privacy.

However, there is a limit as to which information an organization may keep confidential under the accounts of privacy. Organizations may not keep confidential the following information:[36]

1) Information that discloses the current or potential impact on the human health and the environment as the result of activities, production, services, and equipment used by the organization.
2) Information that discloses the effects of all poisonous or radioactive substances which are administered by the organization and that may present danger to the human health and the environment if their storage procedures are breached.
3) Information on crimes and other information provided in the laws.

If any information that applies under the above limitation is kept private by an organization, such confidentiality would be regarded as illegal. Therefore, appropriate authorities and officials, in the course of inspections

[36] Article 6. Information prohibited from being kept confidential. Law on Organization Secrets of Mongolia

and in conformance with their full rights, may disclose confidential information that was illegally kept secret. They may also disclose some confidential information related to delinquencies and incompliance to the public in order to ensure that this does not damage the legitimate interests of others.[37)]

(3) Law on Individual's Secrets

Crimes related to individual's secrets shall be classified as follows: confidential correspondence, health secrets, stock secrets, family secrets, and other secrets defined by legislation. Nowadays, many individual's secrets are available on the internet.

Article 2 of Chapter 1 of the Law on Individual Secrets defines "individual privacy" as "information, documents, or physical items that are kept confidential…disclosure of which might cause significant damage to legitimate interests, reputation, and esteem of the person in question." Moreover, Article 5 of Chapter 2 provides that persons who have access to private information of other individuals by law or trust are prohibited from disclosing the information. Article 6 of the same law does include provisions that allow for individual privacy to be overridden, but such overriding is permissible only when it is to protect national security and defense, a very limited set of conditions.

There exist laws other than the Law on Individual Secrets that also protect individual privacy. For example, Article 136 of the Criminal Law provides for up to 5 years of imprisonment for disclosing information on individual privacy. Also, various legislations describes that the following

[37)] Article 7. Accessing privacy of organizations. Law on Organization Secrets of Mongolia http://www.globeinter.org.mn/old/en/elaws/elaw04.html persons and entities have a legal duty to protect information on individual privacy:

- Civil servants (Article 13, Law on Civil Service);
- Government organizations and officials, in relation to petitions and complaints (Article 7.1.5 of the Law on Resolution of Petitions and Complaints Issued by Citizens to Government Organizations and Officials);
- Employees of the State Security Protection system (Article 17.1.2 of the Law on Special State Protection); and
- Employees in charge of official statistics (Article 22.1 of the Law on Statistics).

Moreover, international law recognizes the protection of individual privacy as a valid reason for imposing restrictions on the freedom of information. However, the presumption in favor of the freedom of information is that a State cannot refuse to disclose information unless the disclosure threatens or imposes a substantial harm to the privacy interest.

Furthermore, it is essential that the privacy provisions be subject to being overridden by the general public interest so that the information may be disclosed where the public interest in having the information is greater than the harm to the privacy interest being violated. Such an override is widely accepted around the world, since otherwise, privacy laws would seriously inhibit investigative reporting. Practically every instance of corruption involves some privacy interest.

As to the case where the individual concerned has consented to the disclosure of his or her private information, the information should simply be disclosed without the application of a further examination. Mongolian law does not appear to apply the same level of concern to the question of monitoring communications. Article 12.1.1 of the Law on Secret Agency gives the State Secret Agency the power to monitor post and other communications secretly, in accordance with the law. It is not clear which conditions are imposed on monitoring, but it should be allowed only after receiving an approval by a judicial authority or when it is considered as an exceptional case that requires urgent action.[38)]

3. Laws Related to Integrity of Information

(1) Criminal Code of Mongolia

In regards to the cybersecurity protection, the purpose of the Criminal Code of Mongolia shall be to protect from criminal encroachments the individual's rights and national cybersecurity of Mongolia. For attaining this purpose, the Criminal Code of Mongolia determines which acts or omissions represent a danger to the humans and national cybersecurity.

The Mongolian Criminal Law was revised in 2015, and will come into force in 2016. This revision includes a chapter with more detailed articles and provisions on Information Security and Cybercrime. But no one knows, at the present moment, whether this law will be effective or not. It is regrettable but true that the majority of Mongolians, in general, have yet to attain legal literacy, especially for new types of social relations and its legislation.

[38)] ARTICLE 19/Globe International. Mongolia in Transition: An Analysis of Mongolian Laws Affecting Freedom of Expression and Information. July 2002. p.30-31 http://www.opensocietyforum.mn/res_mat/A19%20Analyses_eng.pdf

Re*visions Made in the Mongolian Criminal Law 2015*

	Criminal Code of Mongolia, 2002	Criminal Code of Mongolia, 2015
Target	Computer, software and its devices; Data on computer and information systems; Protected information systems	Electronic devices and information systems
Criminal activities	Intentional alteration, damage or destruction; Copying of the data stored in a computer without permission or obtaining it in other ways.	Viewing and accessing of the data without permission; Hiding of the data; Restricting of the data.
Subject/Criminal person	16 years old	14 years old
Unserved term	From 6 months to 5 years	1-5 years

(2) Law on National Security

Law on National Security regulates various activities to ensure the cybersecurity of Mongolia and its participation by legal entities and citizens. This law defines various special agencies engaged in safeguarding national security. According to the Law on National Security, national security is a condition in which Mongolia’s national interests are solidly secured both internally and externally. The term, “national interests,” include Mongolia’s independence, territorial integrity, the existence of Mongolian nation and culture, national unity, and the conditions in which human rights, as well as balanced economic and ecologic development, are secured. “Activities to ensure national security” refer to state strategies that are intended to guarantee, secure, and strengthen the national interests undertaken by organizations, business entities, officials, and citizens.

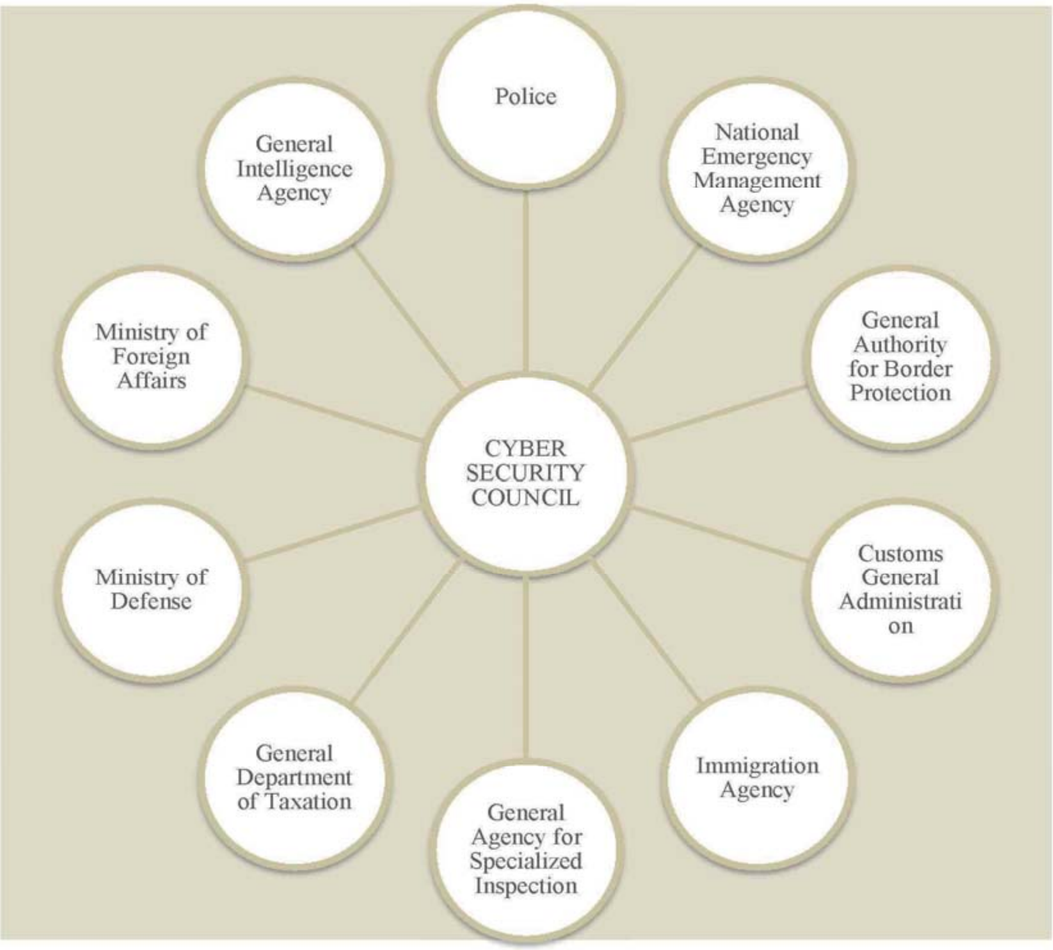
Mongolian Special Agencies on National Security
(According to Article 7 of Law on National Security)

National Security Council	The highest state consultative body coordinating the elaboration and implementation of the integral state policy on ensuring national security and executing control over how this coordination is being carried out.
Special agencies	Environmental protection agency
	Customs service
	Agency for diplomatic security
	Disaster Management Authority
	Agency for Specialized Investigation
	Army
	Tax authority
	Special agency
	Department of Citizenship and Migration
	Registration office
Additional organizations	State organizations
	Local self-governing bodies

The integrated effort in ensuring national security is coordinated by the Executive Office of the National Security Council, whose function is to support the members of the Council fulfill their duties in ensuring national security. It also has the duties to organize and coordinate inter- and intra-government institutions in implementing national security policy and monitor their activities.[39]

[39] What is National Security? http://www.nsc.gov.mn/?q=en/aboutns

National Special Agencies on Cybersecurity


Police
National Emergency Management Agency
General Authority for Border Protection
Customs General Administrati on
Immigration Agency
General Agency for Specialized Inspection
General Department of Taxation
Ministry of Defense
Ministry of Foreign Affairs
General Intelligence Agency
CYBER SECURITY COUNCIL

4. Laws Related to Availability of Information

(1) Law on Information Transparency and Right to Information[40)]

In the Law on Information Transparency and Right to Information, it is written that, “the purpose of this law is to regulate relations pertaining to

[40)] Law on the information transparency and right to information of Mongolia http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan047231.pdf ensuring transparency of the state, and rights of citizens and legal entities to seek and receive information."

This law regulates the following organizations financed by the state and local budget:

- Secretariat of the State Great Khural (Parliament);
- Office of the President;
- Government Cabinet;
- Administrative office of the National Security Council;
- State central administrative or other state administrative organizations;
- Judiciary and prosecutor's offices of all instances;
- Institutions established by the State Great Khural with exception of the Government Cabinet;
- Administrative offices of local municipal and self-governing bodies;
- Local government owned or partially owned legal entities;
- State-owned or partially owned legal entities;
- Non-governmental organizations executing the particular functions of the executive branch in accordance with Mongolian Law on Government, Section 1, Article 19; and
- Mongolian National Public Radio and Television organization.

However, there exist certain organizations outside the scope of this law, upon which, demanding transparency in information may be detrimental to the national security. This law shall not apply in ensuring transparency in the operation of the armed forces, border protection and internal troops, and national intelligence organization. In addition, information transparency encompasses the following categories:

- Operational transparency;
- Human resource transparency;
- Budget and financial transparency; and
- Transparency in the procurement of goods, works, and services by the state and local government.

On the other dimension of the duties to keep information transparent imposed upon the above-mentioned organizations, there exist the rights of the citizens and legal entities to have access to that information. Article 11 provides that citizens and legal entities shall be entitled to receive the following information, with the exception of certain information prohibited by law, in order that such publicly disclosure would ensure human rights, freedom, national security, and the organization's lawful interest.

The types of information to be publicly disclosed are specified in Article 3.1 of this law:

- All types of information, documents, agreements and contracts in possession of the organization;
- Information related to the property in possession of the organization; and
- Any other information related to the activities of the organization.

But, in the following circumstances, it is prohibited to disclose the information to others:

- If there are well-grounded reasons that the public release of the concerned information might be detrimental to the national security and public interest of Mongolia;

- If the concerned information is related to matters under review by the Mongol Bank, the Financial Regulatory Commission, or state administrative organizations in charge of the competition or specialized inspection;
- If it is necessary to protect the secrets of state, organization, and individual during the process of inquiry, investigation, and prosecution;
- If the concerned information is related to the process of concluding international treaty or agreement; and
- Other circumstances specified in laws and legislations.

Article 20 involves the disclosure of personal information. It describes that unless otherwise provided by law, if an individual has not expressed his or her agreement in a written form, it is prohibited to disclose his or her information. But exempt from this prohibition is a set of very basic information such as his or her parents' name, first name, age, gender, profession, education, official position, work address, and telephone number.

Also, according to Article 21, it is prohibited to disclose, without a written permission given by the respective official of the business entity (such as executive manager or other persons to whom the authority is given to), secret information, technological solution, project, research document, and other information related to required machineries and equipment, whose disclosure might be detrimental to the lawful interest of the organization, or those taken under its confidentiality or protection. This is for the purpose of protecting its market and advantage in the fair competition, or those related to the unique activities of the organizations and business entities specified under the article in the Law on Organization's secret.

Ⅳ. Current Issues and the Needed Improvements

In the National Security Concept, Mongolia has declared that positive neighbor-friendly relations and wide-ranging cooperation with the Russian Federation and the People's Republic of China shall be developed. Moreover, it announced that, pursuant to the "third neighbor" strategy, bilateral and multilateral cooperation with other highly developed democracies in political, economic, cultural and humanitarian affairs shall be undertaken.[41]

Despite these provisions that aim for benevolent international relationships, individuals and groups in China, Russia, USA, the Republic of Korea and England have attempted numerous cyber-attacks against Mongolia, most of which have been recorded.[42] It can be observed that our two neighbors and our tertiary neighbors are trying to access information and databases in Mongolia.

[41] National Security Concept of Mongolia. 2010. http://www.nsc.gov.mn/sites/default/files/images/National%20Security%20Concept%20of%20Mongolia% 20EN.pdf

[42] - Cyber-attacks numerous directed to the Mongolia on April 2016. Resource: Agency on National Cybersecurity of Mongolia, 2016.05.03 http://ncsc.gov.mn/?id=135
- Cyber-attacks numerous directed to the Mongolia. Resource: Agency on National - Cybersecurity of Mongolia, 2016 http://ncsc.gov.mn

The Number of Cyber-Attacks Directed Against Mongolia by Countries[43]

Date	Top 5 source of cyber-attacks by countries	Number of cyber-attacks directed against Mongolia
April 2016	China	22613
	USA	4034
	Russia	857
	ROK	927
	England	384
March 2016	China	50678
	USA	10850
	Russia	2649
	ROK	1546
	Finland	936
February 2016	China	18405
	USA	4536
	Russia	1143
	Taiwan	869
	ROK	621
January 2016	China	16815
	Finland	11419
	USA	4252
	ROK	752
	Russia	726

[43] - Cyber-attacks numerous directed to the Mongolia on March 2016. Resource: Agency on National - Cybersecurity of Mongolia, 2016.05.03 http://ncsc.gov.mn/?id=134
- Cyber-attacks numerous directed to the Mongolia on February 2016. Resource: Agency on National Cybersecurity of Mongolia, 2016.03.04http://ncsc.gov.mn/?id=132
- Cyber-attacks numerous directed to the Mongolia in January 2016. Resource: Agency on National Cybersecurity of Mongolia, 2016.03.04http://ncsc.gov.mn/?id=131

Ensuring cybersecurity concerns not only national activities but also international activities. It is related to the other countries' activities on cybersecurity. The United Nations Office on Drugs and Crime described that cybercrime is a part of a transnational organized crime, and each year, millions of victims are affected as a result of such activities.[44] It is true that cybercrime has risen to a transnational and global scale and scope. This current situation indicates that Mongolia will have to cooperate with other countries on cybersecurity.[45]

Then, it becomes necessary to examine with which nations Mongolia should cooperate with. The table below presents data on six countries and their national security level, demonstrated through three indicators: cyber offense, cyber dependence, and cyber defense.[46]

Overall Cyber-War Strength of Six Countries[47]

Country	Indicator			Total
	Cyber-Offense	Cyber-Dependence	Cyber-Defense	
China	5	4	6	15
Russia	7	5	4	16

[44] United Nations Office on Drugs and Crime. Transnational organized crime: the globalized illegal economy
https://www.unodc.org/toc/en/crimes/organized-crime.html

[45] 3.6.1.12. Develop and expand international cooperation to ensure information security, prevent the danger of confrontation in information space and combat cybercrime. National Security Concept of Mongolia, 2010

[46] Richard A.Clarke, Robert Knake.Cyber War: The Next Threat to National Security and What to Do about It. HarperCollins Publishers. 2010. p.148,
Georgetown Security Studies Review. Vol. 1 Issue 1. 2013.12.10. "Richard A.Clarke and Robert K Knake's "Cyber War: The Next Threat to National Security and What to Do About It" (Harper Collins, 2010) By David Vanca. http://georgetownsecuritystudiesreview.org/2013/12/10/richard-a-clarke-and-robert-k-knakes-cyber-war-the-next-threat-to-national-security-and-what-to-do-about-it-harper-collins-2010/

[47] Richard A.Clarke, Robert Knake.Cyber War: The Next Threat to National Security

Country	Indicator			Total
	Cyber-Offense	Cyber-Dependence	Cyber-Defense	
USA	9	2	4	15
Iran	4	5	3	12
Israel	8	3	4	15
North Korea	2	9	7	18

These three indicators can be understood to be the main directions for ensuring, cooperating, and developing cybersecurity with other countries. These criteria are important areas for Mongolia to further develop, so that it would improve the overall cybersecurity.

Also, in order to cooperate with other nations on ensuring cybersecurity, it is important to examine the existing international cooperation between the key countries and identify how they are combining efforts together to ensure and further strengthen cybersecurity.

International Cooperation on Cybersecurity

Parties	Announced date	Actual date	Purpose and direction
USA, Russia	2013.6.17.	2013	Developing cyber-capabilities[48)]
China, Republic of Korea, and Japan	2014.10.21[49)] 2015.10.13[50)]	2014	Creating a consultation mechanism on cybersecurity[51)]

and What to Do about It. HarperCollins Publishers. 2010. p.148, Georgetown Security Studies Review. Vol. 1 Issue 1. 2013.12.10. “Richard A.Clarke and Robert K Knake’s “Cyber War: The Next Threat to National Security and What to Do About It” (Harper Collins, 2010) By David Vanca. http://georgetownsecuritystudiesreview.org/2013/12/10/richard-a-clarke-and-robert-k-knakes-cyber-war-the-next-threat-to-national-security-and-what-to-do-about-it-harper-collins-2010/

Parties	Announced date	Actual date	Purpose and direction
USA, Japan	2015.4.28[52]	2013[53]	Preventing and combating cyber-attacks from China, North Korea, Russa, and Iran[54]
Russia, China	2015.5.08[55]	2009[56]	Ensuring cybersecurity[57]
Australia, Republic of Korea	2015.9.11[58]	2013[59]	Cooperating on developing cybersecurity
The USA, China	2015.9.25[60]	2015	Combating cybercrime and creating amechanism on cybersecurity
The USA, Republic of Korea	2015.10.16[61]	2013[62]	Preventing and combating cyber-attacks from North Korea
Estonia, Japan	2016.04.08[63]	2015	Ensuring cybersecurity for Tokyo Olympic games 2020

[48] The New Norms: Global Cyber-Security Agreements Face Challenges By Tim Maurer, February 5, 2016, IHS Jane's Intelligence Review http://carnegieendowment.org/2016/02/05/new-norms-global-cyber-security-protocols-face-challenges/iv53

[49] China, Japan, ROK hold cyber security meeting in Beijing (Xinhua)2014.10.22. http://www.chinadaily.com.cn/world/2014-10/22/content_18786642.htm

[50] S. Korea, Japan, China to hold cyber policy talks, 2015.10.13 http://english.yonhapnews.co.kr/news/2015/10/13/0200000000AEN20151013004800315.html?b1e08f30

[51] China, Japan, ROK hold cyber security meeting in Beijing (Xinhua)2014.10.22 http://www.chinadaily.com.cn/world/2014-10/22/content_18786642.htm
China, Japan, South Korea Talk Cyber Issues, By Emilio Iasiello, 2015.11.23, Dark Matters-Superior Attack Intelligence. http://darkmatters.norsecorp.com/2015/11/23/cyber-issues-china-japan-south- korea-talk/

[52] White House unveils cyber pact with Japan, By Cory Bennett Arpil 28 2015, Th Hill http://thehill.com/policy/cybersecurity/240283-white-house-unveils-unprecedented-cyber-partnership-with-japan

[53] Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group, May 30, 2015 http://www.mod.go.jp/j/press/news/2015/05/30a_1.pdf
Japan and the United States to Deepen Cybersecurity Cooperation: The growing threat

The table above shows the key players of cybersecurity (USA, Japan, Republic of Korea, Russia, China, Australia, and Estonia) and how these nations are cooperating and forming mutual international relationships on

of digital attacks moves Washington and Tokyo closer together in trying to secure cyberspace By Franz-Stefan Gady, June 02, 2015 http://thediplomat.com/2015/06/japan-and-the-united-states-to-deepen-cybersecurity-cooperation/

54) James Andrew Lewis. U.S.-Japan Cooperation in Cybersecurity (A Report of the CSIS Strategic Program). November 2015. p. 17 http://csis.org/files/publication/151105_Lewis_USJapanCyber_Web.pdf

55) The Next Level for Russia-China Cyberspace Cooperation? By Elaine Korzak, August 20, 2015 http://blogs.cfr.org/cyber/2015/08/20/the-next-level-for-russia-china-cyberspace-cooperation/

56) Соглашениемежду правительствами государств－членов Шанхай ской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. Екатеринбург, 16 июня 2009 года (Вступило в силу с 5 января 2012 года) https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf

57) Соглашение между Правительством Россий ской Федерацией и Правительством Китай ской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности, 2015.04.30 http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf

58) Australia-Republic of Korea Foreign and Defence Ministers 2+2 Meeting, Joint statement. 11 September 2015 http://foreignminister.gov.au/releases/Pages/2015/jb_mr_150911.aspx?w=tb1CaGpkPX%2FlS0K%2Bg9ZKEg% 3D%3D

59) Australia-Republic of Korea Foreign and Defence Ministers 2+2 Meeting, Joint statement. 11 September 2015 http://foreignminister.gov.au/releases/Pages/2015/jb_mr_150911.aspx?w=tb1CaGpkPX%2FlS0K%2Bg9ZKEg% 3D%3D

60) Fact Sheet: President Xi Jinping's State Visit to the United States, September 25, 2015. https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

61) Remarks by President Obama and President Park of the Republic of Korea in Joint Press Conference. The White House, Oct 16, 2015 https://www.whitehouse.gov/the-press-office/2015/10/16/remarks-president-obama-and-president-park-republic-korea-joint-press

62) US, South Korea join forces to prevent cyber-attacks by North Korea By Jennifer Chang, IDG News Service, Apr 3, 2013 1:25 PM http://www.pcworld.com/article/2032918/us-south-korea-join-forces-to-prevent-cyberattacks-by-north-korea.html

63) Japan, Estonia vow to strengthen cybersecurity cooperation. The Japan Times, April 8, 2016 http://www.japantimes.co.jp/news/2016/04/08/national/politics-diplomacy/japan-estonia-vow-strengthen-cybersecurity-cooperation/#.Vwg0IqQrLNN

cybersecurity. This demonstrates that Mongolia needs to cooperate more with its tertiary neighbors, such as Japan, South Korea, and the USA, as well as with Russia and China, in order to augment its cyber strength and achieve a higher level cybersecurity.

Chapter 3. Current Cybersecurity Legislations in South Korea

Ⅰ. Developmental Process of Regulatory Framework and Legislations[64]

1. Early Stage of Information Society (1980-1999)

Since the 1980s, an active nationwide informatization and its adverse effect came to the fore, and the information security related laws began to form their shapes. The <Act on Expansion of Dissemination and Promotion of Utilization of Information System> was the first statute regarding informatization and it regulated national policies and systems regarding the issue. This law did include regulations on securing of a computer network; however, it did not fully recognize the importance of information security.

Meanwhile, a private sector information security had been emphasized and information security policies began to be considered. Standard and notification about information security system began to be recognized with the <Framework Act on Informationalization Promotion> in 1995. This Act included promotion of informationalization as well as general regulations regarding information security.

In 1995, criminal statutes were amended to include laws on the infringement of secrecy for altering and forging digital records. In 1999, due to the increase in the usage of online transactions due to the increased internet supply, a <Digital Signature Act> was amended. The <Act on Expansion

[64] See, 2016 National Information Security White Paper, pp. 68-70.

of Dissemination and Promotion of Utilization of Information System> had also been amended to <Act on Promotion of Utilization of Information and Communications Network> in order to secure the circulation of information of individuals and corporation, which, also may be seen as amendments of counteracts against the adverse effects of informationalization.

2. Entrance into Communicopia (2000-2007)

As we have entered into the 2000s, national and societal reliance on information network has also intensified. As a result, the need for amendments on information security laws was noted in national security dimension. Invasion and destruction on national and societal core information and information network will endanger the national safety, and it will not only lead to societal and economic loss, but to the extent of endangering one's freedom and liberty.

In 2001, <Act on the Protection of Information and Communications Infrastructure> was established and proclaimed to protect ICT infrastructure that is important to the nation and society such as finance, telecommunication, or energy. Also, another criminal law against online fraud was enacted to prevent acts of inserting false information or ill-willed orders into a processor to steal others' assets.

<Act on Promotion of Utilization of Information and Communications Network> also changed its name to <Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.> (further, "Information Communications Network Act") and reinforced the policies regarding information security. This Act was again majorly amended after the 1.25 Internet Crisis to enhance the emergency computer

response policies. In 2004 and 2005, to resolve the infringement on personal information and damages from mass distribution of advertisements, punishments were prescribed harder than before.

In 2005, to protect national information network form cyber-attacks such as hacking or viruses that may also threaten national security, a National Cybersecurity Management Regulation was established under the Presidential decree to establish a systematically arranged cybersecurity organizations or their managements.

In 2006, in cases where the exportation of national core technology may possibly have a negative effect on national security, or when one does not report such possibility or faultily report to export the national core technology, then in order to stop, ban, or to return to the original state, an <Act on Prevention of Divulgence and Protection of Industrial Technology> was established.

In 2007, a traditional <Promotion of Digitalization of Administration for Materialization of Digital Government Act> was revised to <Electronic Government Act>. Along with this change, other laws were also amended for actualization of e-government.

3. Implementation Phase of 21st Century Information Knowledge Society (2008-2014)

By the late 2000s, information resources' intellectualization and an activation of common usage of the resource to enhance the national competition and to improve the quality of life to activate the so-called *information knowledge society* had become the major stream of information policy formation.

In 2009, a <Framework Act on Informationalization Promotion> was completely revised to <Framework Act on National Informatization> and <Information and Communications Technology Industry Promotion Act> was enacted to provide an institutional basis to vitalize the information security industry.

In 2010, <Act on Establishment of Infrastructure for Informatization of National Defense and Management of Informational Resources for National Defense> had been established and <Electronic Government Act> had been amended throughout to promote informationalization of national defense and administration, along with improving regulations on information security.

In 2011, <Personal Information Protection Act> was established and related Acts' personal information security regulations were amended to increase the security level. On the other hand, due to the establishment of <Framework Act on Intellectual Property>, more emphasis was put on the enhancement of information security in order to increase the security level of intellectual property rights.

In 2012, the <Act on Promotion of Information and Communications Network Utilization and Information Protection Etc.> had been largely amended to reinforce the personal information protection and to improve the information protection system.

In 2013, indiscriminate usage of national identity number had been restricted under the establishment of <Personal Information Protection Act>, and the National Cybersecurity Management Regulation had been revised to heighten the information protection.

In 2014, for financial security system, an <Electronic Financial Transactions Act> had been amended so that people are not forced to use their Accredited

Certificates for online transactions, and it brought a great success to regulatory reform.

4. Table of Information

Following is the arranged table of process of development of Cybersecurity Legislations in Korea.

The Process of Development of Cybersecurity Legislations in Korea[65]

Year	Rules/Regulations Legislations/Acts	Notes
1964	<Security Operation Regulation> (Presidential Decree) and Association regulation were enacted	
1981	<Intelligence and Security Business Planning, Rules, and Regulations> (Presidential Decree) enacted	Prescribed the plan and adjusted in the method of procedure on national communication security related businesses
1986	<Act on Expansion of Dissemination and Promotion of Utilization of Information System> enacted	
1989	First symposium about information protection	1st Workshop on Information Security and Cryptology (WISC)
1990	Korea Institute of Information Security and Cryptology (KIISC) established	
1994	The Ministry of Information and Communication was established	Expansion and reorganization of the Communications Ministry; Merging/ absorbing of the information and communications related functions of the Ministry of Science-Technology, Bureau of Public Information, and the Ministry of Commerce and Industry
1995	Hosted first NETSEC-KR	

[65] See, 2016 National Information Security White Paper, pp. 68-70.

Year	Rules/Regulations Legislations/Acts	Notes
1996	Korea Internet & Security Agency (KISA) was established	
1998	Korea Information Security Industry Association (KISIA) was established	
	Korea's very first block cryptographic algorithm (SEED) was developed.	
	Evaluation and authentication system of the information security system enforced	
1999	First simulation training of cyber warfare at Ulchi Exercise	
	<Act on Expansion of Dissemination and Promotion of Utilization of Information System> was changed to <Act on Promotion of Utilization of Information and Communications Network>	
	<National Information Communications Security Guidelines> enacted	
	<Digital Signature Act> enacted	
2000	National Security Research Institute (NSR) was established	
2001	<Act on the Protection of Information and Communications Infrastructure> enacted	
	<Promotion of Digitalization of Administration for Materialization of Digital Government Act> enacted	
	<Act on Promotion of Utilization of Information and Communications Network> changed to <Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.>	
	Korea Information Assurance Society (KIAS) was established	
	Korea Information Security Centre was promoted to Korea Information Security Agency (KISA)	
2002	National Information Security White Paper published	
	National Information Security Association (NISA) established	
	Information security system evaluation's Common Criteria (CC) established	

Year	Rules/Regulations Legislations/Acts	Notes
2003	1.25 Internet Crisis	
	KISA established a Korea Internet Security Center (KrCERT)	
	National Block Cipher for Administrative System (ARIA: Academy, Research Institute, Agency) was developed	
2004	National Cybersecurity Center was established	
	<National Cyber Crisis and Emergency Management Manual> (Presidential Decree) was enacted	
2005	<National Cybersecurity Management Regulation> (Presidential Decree) was enacted	
	Held very first Day of Cybersecurity	
2006	Became a member of Certificate Authorizing Participants of Common Criteria Recognition Arrangement (CCRA)	
	Implementation of unified practice on National Cyber Crisis Response ("Unified Counterattack")	
2007	Appointment of private evaluation group for Information Protection Products	
	<Promotion of Digitalization of Administration for Materialization of Digital Government Act> amended to <Electronic Government Act>	
2008	According to the government reorganization, each respective government ministry is now in charge of different functions regarding information security	**Korea Communications Commission** In charge of private sector information protection, such as the common carriers
		Ministry of Public Administration and Security In charge of protection of public service of the e-government; Operation of Administrative Electronic Authentication System; Protection of ICT infrastructure, personal information security of public sectors

Year	Rules/Regulations Legislations/Acts	Notes
		Ministry of Knowledge Economy In charge of promotion and development of techniques of information protection industry; Train professionals in information protection industry
	Built an international level of protection control system	Security control centers were established for 10 core sections such as national defense, diplomacy, or administration
2009	7.7 DDoS infringement incident	
	National Cyber Crisis Comprehensive Countermeasures was established	
	Korea Internet & Security Agency (KISA) was established	Merged version of Korea Information Security Agency, Korea Internet & Security Agency and Korea ICT International Cooperation Agency
	Korea Information Security Industry Association (KISIA) re-established	
2010	Cyber Warfare Command was established	
	Diversification of public certification authority system in electronic financial transaction	
	General revision of <Electronic Government Act>	Merged functions and legislations regarding the e-government
2011	<Personal Information Protection Act> enacted and Personal Information Protection Commission established	
	3.4 DDoS infringement incident	
	National Cybersecurity Master Plan was established and enforced	
2012	Information Protection Day enacted	
	Civil-Government-Military joint response team against cyber threat now in full operation	

Year	Rules/Regulations Legislations/Acts	Notes
2013	3.20 Cyber Terror, 6.25 Cyber-attack occurred	
	A comprehensive plan on cybersecurity measures were announced	
	Limitations on online collection or usage of national identity number enforced	
	Chief Information Security Officer (CISO) Conference established	
2014	Credit card companies and mobile carriers' client information leakage normalization measures announced	
	Korea Hydro & Nuclear Power Co., Ltd. was hacked	
	Cybersecurity Training and Education Center (CSTEC) established	
2015	<Promotion of Information Security Industry Act> enacted	
	Implementation of Personal Information Expiration System	
	Financial Security Institute (FSI) was established exclusively for financial security	
	Announcement of comprehensive countermeasures for heightening of national cybersecurity	

Ⅱ. Regulation and Performance Framework[66]

1. Overview

South Korea, to increase the immediate response system against a cyber-threat, with the Blue House as the control tower of the cybersecurity and the National Intelligence Service (NIS) in charge of the practice, the government has established separate responsible organs for civil, military

[66] See, 2016 National Information Security White Paper, pp. 34-35, 71-76, 159-160, 175, 182-185, 194-200.

and government to ultimately establish a unified counteract structure ("Unified Counterattack").

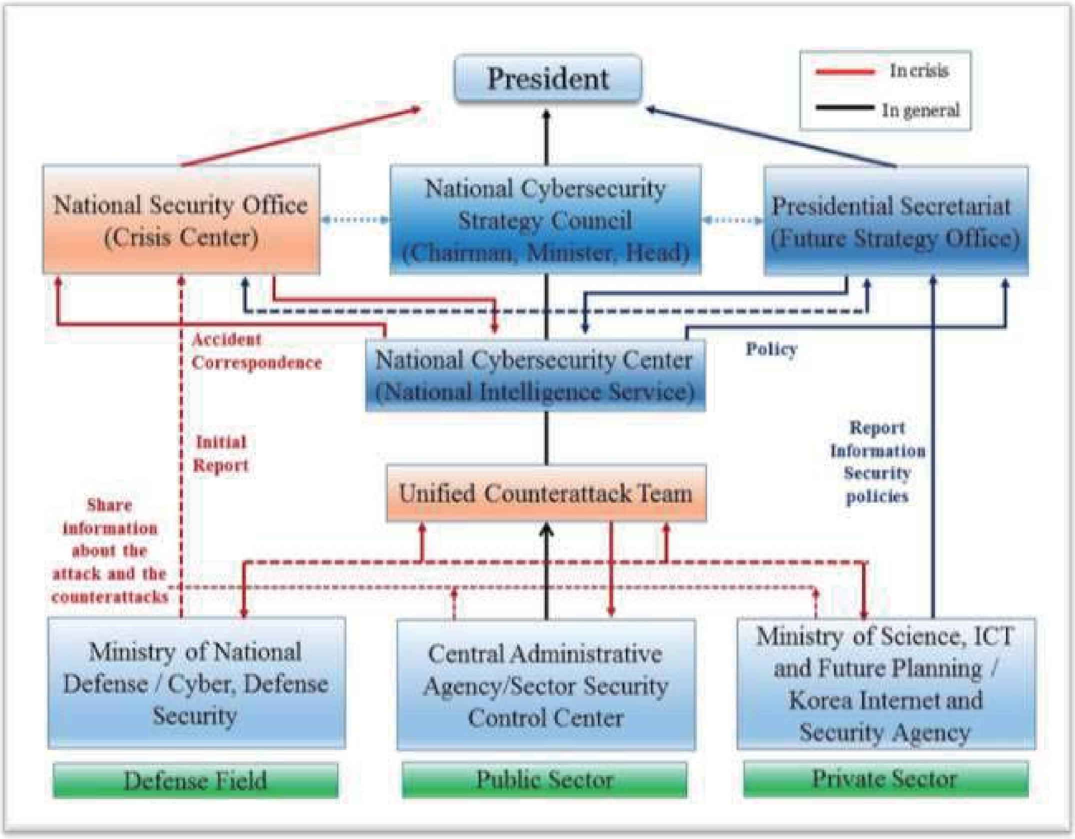
The National Security Office is the control tower at the time of crisis. It reports and diffuses the cyber crisis, and it is in charge of respective counteracts. The Future Strategy Office ("FSO") is the control tower during the normal days and it is in charge of establishment and amendments of statutes, systems, and policies regarding information security. On the other hand, to deliberate the essentials of the matters of national cybersecurity, under the head of the NIS, the National Cybersecurity Strategy Council (the "Council") is held to discuss about the establishment and improvement of the national cybersecurity system, as well as the regulation of respective roles and policies of national security, and also the responsive measures to Presidential decrees regarding the national cybersecurity. The resolution given by the Council is reported to the President after it is consulted by the FSO.

The NIS is the practical manager. With the National Cybersecurity Center, NIS in charge of investigation on national and public level of cyber-attacks and the following preventive measures of those attacks, as well as in charge of investigation/analysis/distribution of information on cyber threats. NIS also operates the National Cybersecurity Strategy Council meetings, establishes Cybersecurity Master Plan, and operates a Unified Counterattack team in National Cybersecurity Center to create an international level of structured counterattacks.

The Ministry of National Defense is in charge of the Defense Security Command and Defense Cyber Command. These Commands prevent and counteract in times of cyber threats in military field, and Commands are also in charge of cyber warfare and also responsible for developing related techniques.

Civil level of cybersecurity is managed by the Ministry of Science, ICT and Future Planning ("MSIP") by preventing and counteracting the civil level cyber-attacks, raising public awareness of cybersecurity, foster information security industry and personnel, and by developing information security techniques. On the other hand, when a cyber-threat or any cyber crisis occurs, each organ or department needs to send an initial report to the National Security Office (Crisis Center) and the NIS (National Cyber Security Center), and the NIS reports to the President through the National Security Office about the counteracts and the casualties from the cyber-attack.

Regulation and Performance System[67]


President
In crisis
In general
National Security Office (Crisis Center)
National Cybersecurity Strategy Council (Chairman, Minister, Head)
Presidential Secretariat (Future Strategy Office)
Accident Correspondence
National Cybersecurity Center (National Intelligence Service)
Policy
Initial Report
Report Information Security policies
Unified Counterattack Team
Share information about the attack and the counterattacks
Ministry of National Defense / Cyber, Defense Security
Central Administrative Agency/Sector Security Control Center
Ministry of Science, ICT and Future Planning / Korea Internet and Security Agency
Defense Field
Public Sector
Private Sector

[67] 2015 National Information Security White Paper, pp. 12.

2. A Public Sector Information Protection Promotion System

Information security promotion system of public sector is composited under the National Cybersecurity Management Regulation. The content is as the following:

Cybersecurity policies and its management is controlled and modified under the consultation of the Chairman of NIS and the Chairman of Central Administrative Agency. Under the control of the Chairman of NIS, a National Cybersecurity Strategy Meeting and National Cybersecurity Countermeasures Meeting are operated. The Chairman of NIS also operates the National Cybersecurity Center.

Central Administrative Agency's Chairman establishes and carries out the cybersecurity measures of his respective area, and directs the measures. Chairman of Central Administrative Agency and the leaders of local governments establish and operate a security control center, and report to the Minister of National Security and the Chairman of Central Administrative Agency if they have acquired any information that may pose threat to cybersecurity.

Chairman of NIS devises counteract based on the information received, and inform the corresponding organizations. When the Chairman spots a cyber-attack, he needs to issue a cyber-attack warning, and when the attack seems critical, he may consult the Minister of National Security and issue a Red alert.

When a crisis from cyber-attack is probable or if a sign of it is hinted, the Chairman of Central Administrative Agency needs to take actions to minimize any possible damage and needs to report to the Chairman of NIS and the Minister of National Security and any other leaders of Central Administrative Agencies. The Chairman of NIS may investigate the causes of the accident/crisis, and if the damage is serious, he may set up a cyber-crisis task force headquarter. The Chairman of NIS studies the damage from the cyber-attack and notifies National Security about the headquarters' countermeasures. Then the Minister of National Security collects all the information and reports to the President. Chairman of NIS then promotes for new policies that are needed for research and development of cybersecurity and the Chairman of Central Administrative Agency permits any research and developments via National Security Research Institute.

3. Private Sector Information Protection Promotion System

Information security promotion system of private sector is composited under the <Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.>. The content is as the following:

The provider of Information and Communication Service may designate the Chief Privacy Officer. For the providers of Information and Communication Services that reach the minimum number of employers and users as decided on the Presidential Decree, the Chief Privacy Officer needs to be designated and should notify the Minister of MSIP. The providers of such services need to properly establish and confirm the level of security and trustworthiness of the information of the service.

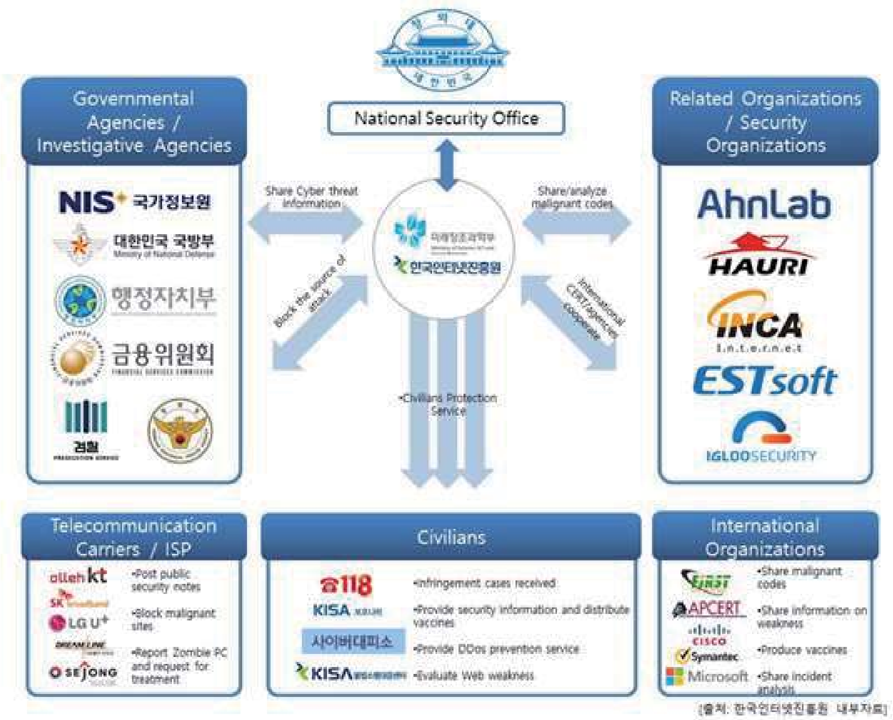
Also, the providers of Accumulated Information and Communication Institutions for provision of information communications need to properly establish and confirm the protective actions for a stable operation of service.

The Minister of MSIP may, on the basis of information protection, advise protective actions according to information security pre-check standard, rate the information security managements, certify the managers of information security management system.

The providers of Information and Communications Service and the operators of the accumulated Information Communication facility need to provide information on infringement accidents to the Minister of MSIP or to the KISA. The Minister of MSIP handles the emergency measures such as collecting data and information about the infringement, informing others of such infringement, forecasting/warning of the infringement, and in times of need, the minister helps the KISA to handle the infringement.

The providers of Information Communications Service and the operators of the accumulated Information communication facility need to immediately report to the minister of MSIP or to the KISA. In times of serious attacks on information network system of the providers, the minister of MSIP may bring in a civil-military joint investigation team to analyze the causation of the attack together.

Countermeasures to Infringement[68]


National Security Office
Governmental Agencies / Investigative Agencies
NIS 국가정보원
대한민국 국방부
Ministry of National Defense
행정자치부
금융위원회
검찰
Related Organizations / Security Organizations
AhnLab
HAURI
INCA Internet
ESTsoft
IGLOOSECURITY
Share Cyber threat information
Share/analyze malignant codes
Block the source of attack
International CERT/agencies cooperate
미래창조과학부
한국인터넷진흥원
•Civilians Protection Service
Telecommunication Carriers / ISP
olleh kt
SK broadband
LG U+
DREAMLINE
SEJONG
•Post public security notes
•Block malignant sites
•Report Zombie PC and request for treatment
Civilians
118
KISA
사이버대피소
KISA
•Infringement cases received
•Provide security information and distribute vaccines
•Provide DDos prevention service
•Evaluate Web weakness
International Organizations
FIRST
APCERT
CISCO
Symantec
Microsoft
•Share malignant codes
•Share information on weakness
•Produce vaccines
•Share incident analysis

[출처: 한국인터넷진흥원 내부자료]

4. A Major ICT Infrastructure Based Information Security Promotion System

An ICT infrastructure related information security bases on <Act on the Protection of Information and Communications Infrastructure>. The content is as the following:

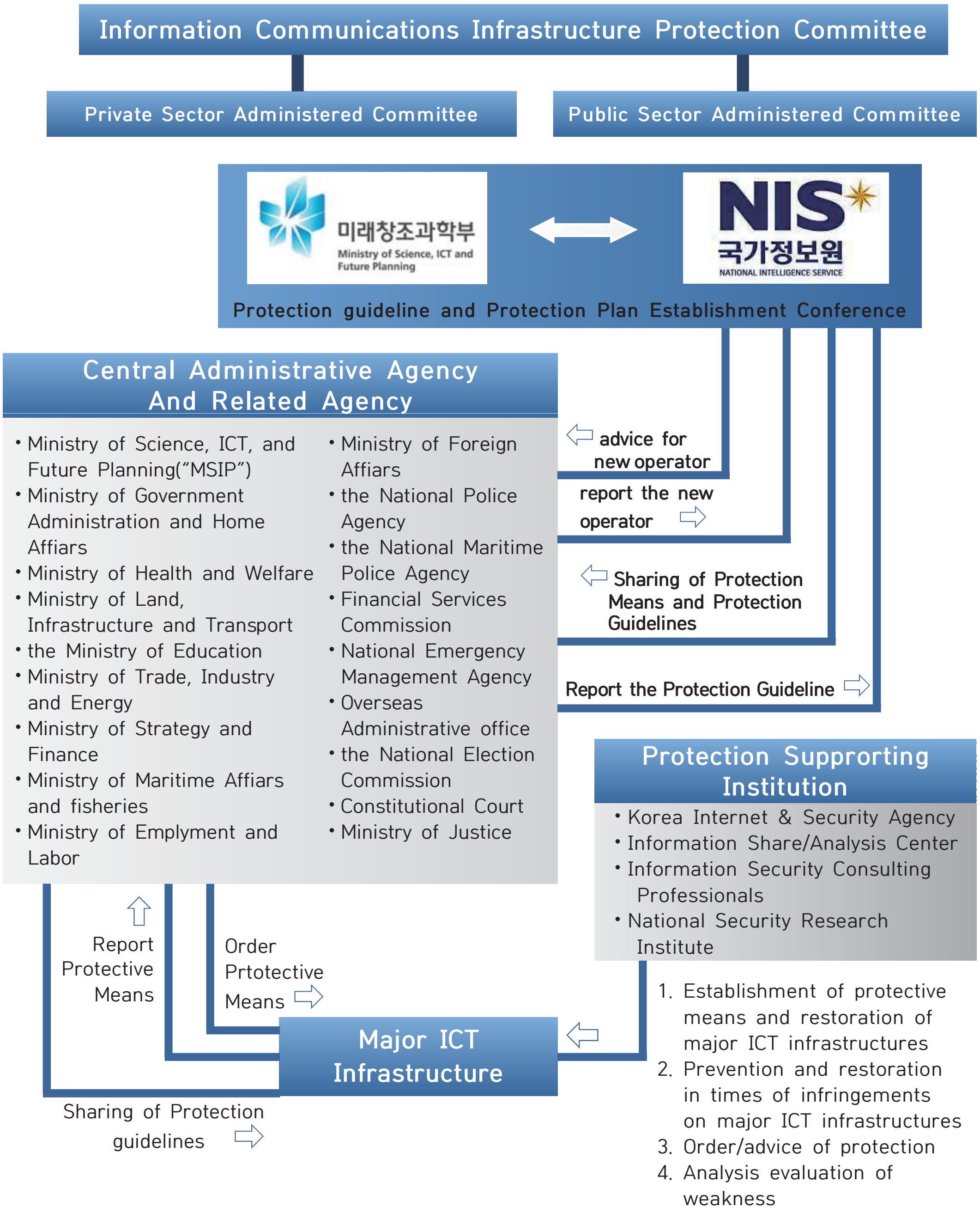
The Information Communications Infrastructure Protection Committee deliberates the matters related with the protection of ICT infrastructures. The head of the office for Government Coordination is the chairman of the Committee, and the chairman of the committee is appointed by the Central Administrative Agency's vice president level official or its chairman.

[68] 2016 National Information Security White Paper, pp. 160.

Central Administrative Agency need to set the ICT infrastructure with the need of protection from prospective electronic infringement as a major ICT infrastructure. The Minister of MSIP and the head of NIS may advice the Central Administrative Agency as to which infrastructure to set as the major infrastructure based on their judgments. Also, in order to protect various fields of ICT infrastructures, the Central Administrative Agency may also share its information on the weaknesses, infringement causes, live alerts, and its analysis with analysis center and run the center.

The operator of the major ICT infrastructure analyzes and evaluates its affiliated ICT infrastructures' weaknesses, and it may also entrust the analysis and evaluation process to the National Security Research Institute, Korea Internet & Security Agency, Information Share/Analysis Center or the Information Security Consulting professionals. Based on the analysis and the evaluation, the operator establishes and enacts any protection provisions, and reports it to the head of Central Administrative Agency. Related Central Administrative Agencies establish and enact protection provisions of its affiliated ICT infrastructures, establish information protection guidelines, and it may order or advise related offices to take protective actions.

Major ICT Infrastructure[69)]


Information Communications Infrastructure Protection Committee
Private Sector Administered Committee
Public Sector Administered Committee
미래창조과학부
Ministry of Science, ICT and Future Planning
NIS
국가정보원
NATIONAL INTELLIGENCE SERVICE
Protection guideline and Protection Plan Establishment Conference
Central Administrative Agency And Related Agency
• Ministry of Science, ICT, and Future Planning("MSIP")
• Ministry of Government Administration and Home Affairs
• Ministry of Health and Welfare
• Ministry of Land, Infrastructure and Transport
• the Ministry of Education
• Ministry of Trade, Industry and Energy
• Ministry of Strategy and Finance
• Ministry of Maritime Affairs and fisheries
• Ministry of Emplyment and Labor
• Ministry of Foreign Affairs
• the National Police Agency
• the National Maritime Police Agency
• Financial Services Commission
• National Emergency Management Agency
• Overseas Administrative office
• the National Election Commission
• Constitutional Court
• Ministry of Justice
advice for new operator
report the new operator
Sharing of Protection Means and Protection Guidelines
Report the Protection Guideline
Protection Supporting Institution
• Korea Internet & Security Agency
• Information Share/Analysis Center
• Information Security Consulting Professionals
• National Security Research Institute
Report Protective Means
Order Prtotective Means
Major ICT Infrastructure
Sharing of Protection guidelines
1. Establishment of protective means and restoration of major ICT infrastructures
2. Prevention and restoration in times of infringements on major ICT infrastructures
3. Order/advice of protection
4. Analysis evaluation of weakness

[69)] 2016 National Information Security White Paper, pp. 151, from .KISA ICT Security Guide (2016).

The minister of MSIP and the head of NIS may notify the head of related Central Administrative Agency about the protective measures and its guidelines of the major ICT infrastructures, and it also may check for the compliances of those protective measures. The minister of MSIP, the head of NIS, National Security Research Institute, Korea Internet & Security Agency, the Information Share/Analysis Center, and Information Security Consulting Professionals provide technical resources to acceptance of major ICT infrastructure protective measures, prevention of infringement and its restoration, ordering/advising/enactment of protective measures.

Related agencies shall report to the related administrative agencies in times of infringement incidents, and may request for restoration or protective measures. The Information Communications Infrastructure Protection Committee may set an ICT infrastructure infringement countermeasure headquarter in times of broad infringement on major ICT infrastructures.

5. Needed Improvements

In order to heighten the security of our cyberspace, since the April of 2015, the government has developed a comprehensive nationwide cybersecurity plan and put it into practice. The plan includes elements such as heightened government level cybersecurity, development of relevant techniques, education of people, increased international investigation, strengthened control tower, and more.

Therefore, to reinforce the cybersecurity centered control tower in the National Security Office, the government has established a Secretary of Cybersecurity under the National Security Office, in effort to unify the making, enforcing and evaluating of the process of the nationwide cybersecurity policies.

Also, in order to amplify the security capabilities of the Central Administrative Agencies, local governments, and the infrastructure management agency, an establishment and expansion of exclusive cybersecurity organization is encouraged. Through this process, the Central Administrative Agency, local governments and the metropolitan office of education come in charge of security management of its respective field. Moreover, separate budget for information security is allocated for different agencies of various levels; vulnerability analysis assessment is supported; signs of cyber-attacks are detected; response organizations are managed; funding for separation of business network from general internet network is expanded; Unified Counterattack training is strengthened; and cyber threat information system is reinforced by collectively gathering, analyzing and sharing the system.

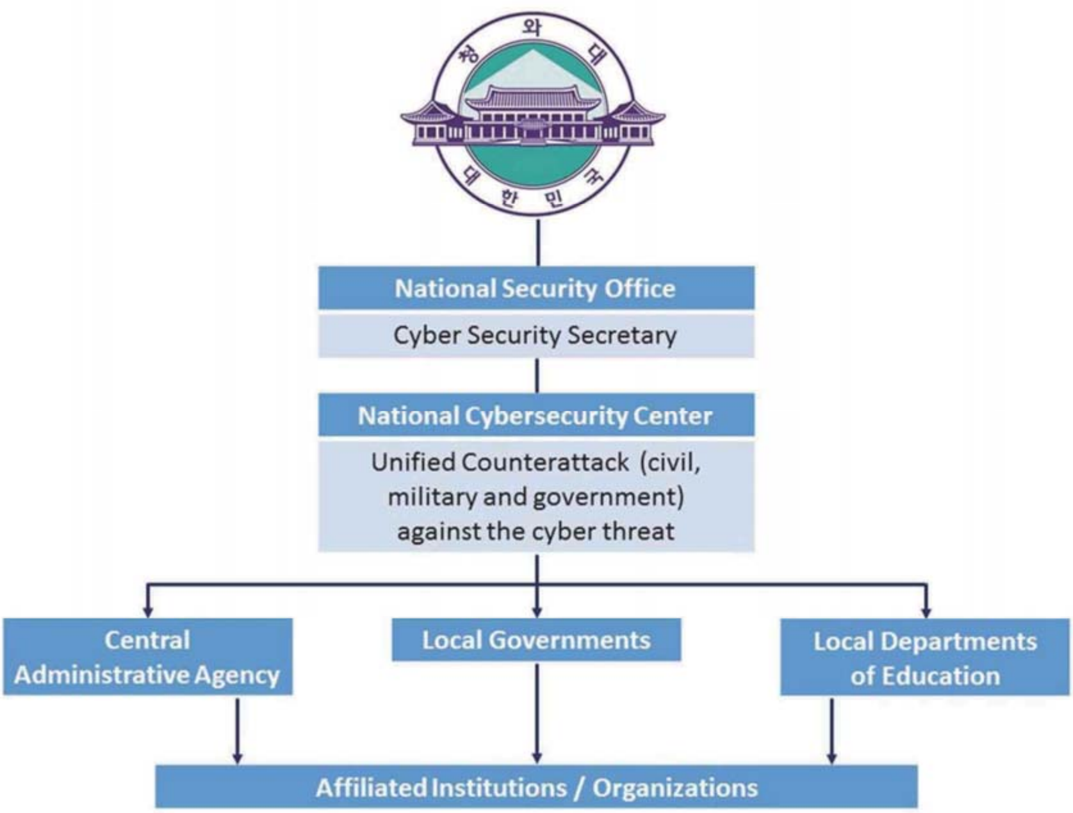
For developments of critical technologies and trainings of top agents in cybersecurity field, increase in number of high schools and universities that are specialized in cyber-related abilities are encouraged. Also, a system where ex-soldiers may work at all strata of society after their military services had been created. Expansion of investment on technology development of cybersecurity specialized institutions, along with the expansion of corporal funding and government assisted businesses are also strongly encouraged.

To increase the cyber confrontational ability, increase in research and development funding and the expansion of respective organization and manpower are strongly suggested. Also, regarding major information network system, development of security techniques or components such as the hacking prevention system, and development of related industries are also strongly carried out.

Additionally, for cooperated counterattacks against cyber-attacks, a scope of sharing of information of cybersecurity policies have been expanded, and a close cooperation with the international organizations will enhance deterrence and establishment of an international norm.

Lastly, for the unification on decision-making regarding the national cybersecurity policies, current laws and acts regarding cybersecurity will be amended and the system of implementation of business will also be continually modified.

National Cybersecurity Performance System Changes and Directions[70]


청와대
대한민국
National Security Office
Cyber Security Secretary
National Cybersecurity Center
Unified Counterattack (civil, military and government) against the cyber threat
Central Administrative Agency
Local Governments
Local Departments of Education
Affiliated Institutions / Organizations

[70] 2016 National Information Security White Paper, pp. 34.

Ⅲ. Current State of Related Law and Regulations

1. Overview

Current Korean legal system is categorized according to each regulation's functional and purpose differences. For example, laws are categorized into *protection of national intelligence related* laws, *prevention of outflow of critical information* related laws, *digital signatures and authentication* related laws, *information network and information system's protection* related laws, *punishment on infringement acts* related laws, or *personal information protection* related laws. The following is a table of laws categorized under big branches:

Category	Laws / Regulations
Information and Communications Network and System's Safe Usage	<Framework Act on National Informatization> <Act on the Protection of Information and Communications Infrastructure> <Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.> <Electronic Government Act> <Digital Signature Act> <National Cybersecurity Management Regulation>
Punishment on Infringement	<Act on the Protection of Information and Communications Infrastructure> <Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.> <Electronic Trade Facilitation Act> <Criminal Act>

Category	Laws / Regulations
Protection of National Intelligence and Prevention of Outflow of Critical Information	<Military Secret Protection Act> <Security Operation Regulation> <Military Criminal Act> <Act on Prevention of Divulgence and Protection of Divulgence and Protection of Industrial Technology> <Technology Transfer and Commercialization Promotion Act> <Promotion of Technology Projects for Joint Civilian and Military Use Act>
Establishment of Information Security Conditions	<Promotion of Information Security Industry Act> <Act on the Protection of Information and Communications Infrastructure> <National Cybersecurity Management Regulation>
Personal Information Protection	<Personal Information Protection Act> <Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.> <Credit Information Use and Protection Act>

2. Information and Communications Network and Information and Communications System's Safe Usage Related Laws

Cyber infringements and cyber threats such as hacking or planting virus has increased in the national and individual level information system, which required a systematic national level protection means. Laws on protection of information network and information system include <Framework Act on National Informatization>, <Act on the Protection of Information and Communications Infrastructure>, <Act on Promotion of Information

and Communications Network Utilization and Information Protection, Etc.>, <Electronic Government Act> and <National Cybersecurity Management Regulations>.

A vitalization of remote transactions and businesses increased due to the actively developing information system and information network system, and this vitalization called for a necessity of protection in securing electronic documents to increase the trust level and to further activate such usages. Hence a digital signature and its authentication related laws were prepared. Related laws are such as <Digital Signature Act> that validates the safety and trust of the electronic documents, or <Electronic Government Act> that regulates the Government Public Key Infrastructure ("GPKI").

(1) Information Security Management System Authentication

As we can wee in the July 2009 DDoS attack, the 2011 bank computer network breakdown, the 2012 telecommunication services' massive personal information leakage, cyber-attacks are becoming smarter and more enhanced in targeting particular information such as corporation's confidential information, personal information and so on.

The damages by the cyber-attacks are not only the results in corporations' cutting-edge technology leakage, loss of credibility and consumers of the corporation, but also affect the stock market and create societal and economic issues such as class action suits or massive damage compensations. In order to resolve these problems, it required more than a mere technological measures, one-time management, or a partial solution. There needed to be a fundamental solution.

The Information Security Management System ("ISMS") is a system that allows information security activities by appointing the highest officer for information security to link a corporation's business management system, and establish an information security policy through a risk analysis. In addition, ISMS monitors and reviews, and continuously requests improvement on information security activities followed by the information security policy.

Through these series of processes, organizations that adopt the ISMS will be able to establish an effective information security system through information security policy and consistent activities. As explained previously the ISMS certification system is a system that evaluates whether a corporation or organization searches the information asset risk and subsequently the established risk management strategy and plans for the series of information security activities are in accordance with the certificatory standard of the ISMS, and grants certification.

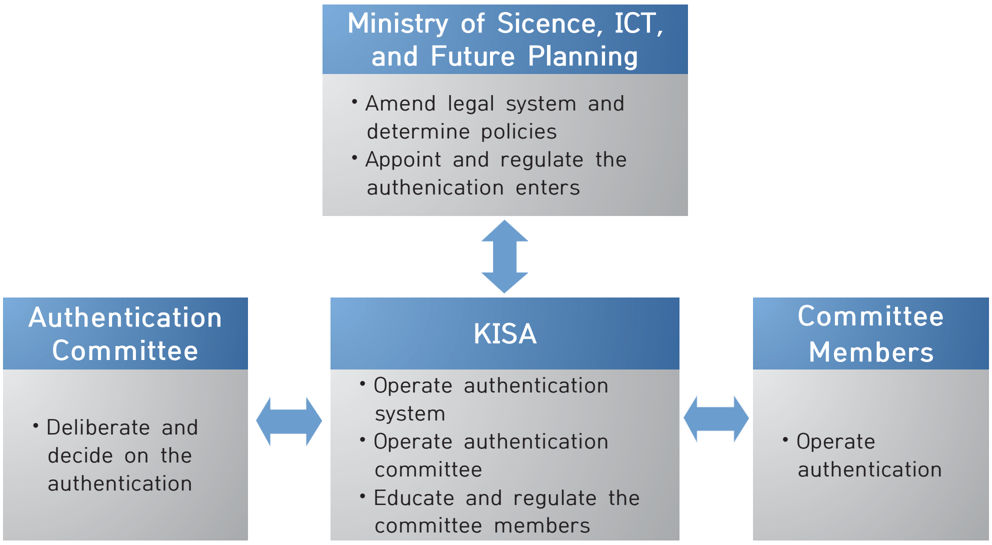
(2) Authentication System

The ISMS authentication system follows the <Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.>, in which a third party authentication institution, independently and objectively, evaluates and certifies whether corporations or organizations' ISMS are in accordance with the certification standard, and suggests a model standard for the ISMS.

Korea Internet & Security Agency ("KISA") is working as an authentication institution to provide fairness and objectively to the authentication system.

As for the authentication institution, Korea Association for ICT Promotion ("KAIT"), Korea Association for Information and Communications Technologies, and Financial Security Institute (“FSI”) were additionally appointed, and the effort to maximize efficiency of the authentication system is in progress.

Authentication Process[71)]


Ministry of Sicence, ICT, and Future Planning
• Amend legal system and determine policies
• Appoint and regulate the authenication enters
Authentication Committee
• Deliberate and decide on the authentication
KISA
• Operate authentication system
• Operate authentication committee
• Educate and regulate the committee members
Committee Members
• Operate authentication

3. Punishments on Infringement Act Related Laws

In order to prevent national and social damages from infringements on the information network system such as hacking, virus, or declination of service, and also from extortion or fraud on information, penal provisions are enacted.

Main examples of these penal codes are: <Act on the Protection of Information and Communications Infrastructure> holds penal codes against infringements on major ICT infrastructures, <Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.> holds penal codes against infringements on information network system. Also, <Electronic Trade Facilitation Act> has codes about accessing digital

[71)] 2016 National Information Security White Paper, pp. 185.

computer files of related trade organizations, and codes about falsification of trade documents in database about trade information. In <Criminal Act>, there are penal codes against digital fraud.

4. Protection of National Intelligence and Prevention of Outflow of Critical National Information Related Laws

Laws regarding protecting national intelligence include: prohibition and punishments on outflow of information that might threaten the nation's existence, safety and democratic orders, categorization of secrecy, defining of documents, resources or facilities that belongs to national intelligence, or regional security tasks. For example, <Military Secret Protection Act> deals with classification of military secret, protective means of military secret, and means to be taken in times of exposure of military secrets. <Criminal Act> includes regulations on espionage, leakage of diplomatic secrets, or leakage of official secrets.

On the other hand, developments in information network and its telecommunication means or digital transactions also increased the usage of passwords, which, amendments on laws had followed. Regulations in relation to the usage of passwords include, <Security Operation Regulation>, <Framework Act on National Information>, and <Framework Act on Electronic Documents and Transactions>. About the illegal usage of password, there is a <Military Criminal Act>.

<Act on Prevention of Divulgence and Protection of Industrial Technology> is a major regulation on prevention of outflow of information regarding advanced technologies developed within Korea or any information that may threat national security or advancement of civilian economy. There

also are regulations such as <Technology Transfer and Commercialization Promotion Act> and <Promotion of Technology Projects for Joint Civilian and Military Use Act> with similar goals.

5. Establishment of Information Security Conditions Related Laws

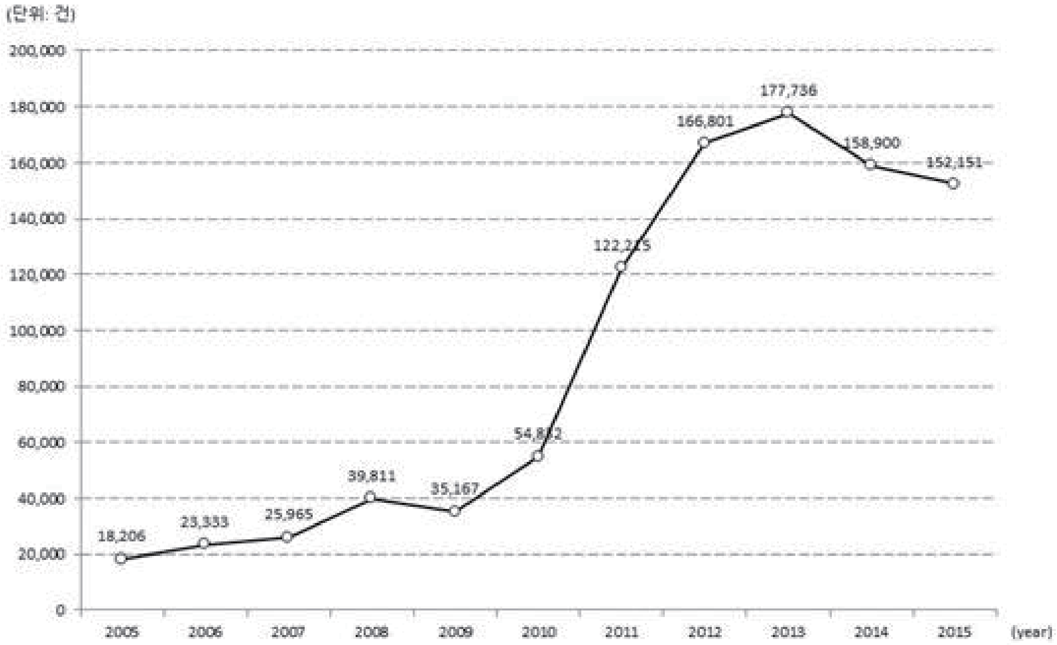
Development of necessary technologies for an enactment of information protection is important in terms that it prepares a practical field of information security. Regarding these condition establishments, the <Promotion of Information Security Industry Act> is a major regulation. This regulation determines the factors necessary for information security industry, prepare the basis for information security industry, strengthen its competitiveness, and ultimately create a safe information communication usage conditions and also dedicate itself in strengthening of economy. It also determines the basis factors for activation of information security industry, and promotion of the industry. On the other hand, <Act on the Protection of Information and Communications Infrastructure> determines the factors of technology developments and joint international research and developments, and the <National Cybersecurity Management Regulation> also deals with regulations about technology developments.

6. Personal Information Protection Related Laws

The nature of Korean personal information protection is rapidly changing with the development of information communication technology. Technologies such as Internet of Things (“IoT”) or Information and Communications Technology (“ICT”) have worked as a major economic growth. As the time of IoT or Big Data has properly begun, ICT technologies such as wearable devices, smart TV or connected car are being produced. These advancements in technologies will drastically change the paradigm of our daily lives.

These developments in ICT have made our lives more convenient and smart. However, an instant collection and usage of information has grown, and each individual are in an easier environment for violation of their privacies. Not only their personal information is collected and used in a massive scale, but sensitive information such as their real time location, their interests, their physical information or their history are also exposed.

Infringement of Personal Information[72]



[72] 2016 National Information Security White Paper, pp. 170.

Above are yearly reports on infringement of personal information. As seen above, the number of reports has drastically increased over the years. Therefore, amendments on related regulations were necessary in order to suffice the increased interest on this matter.

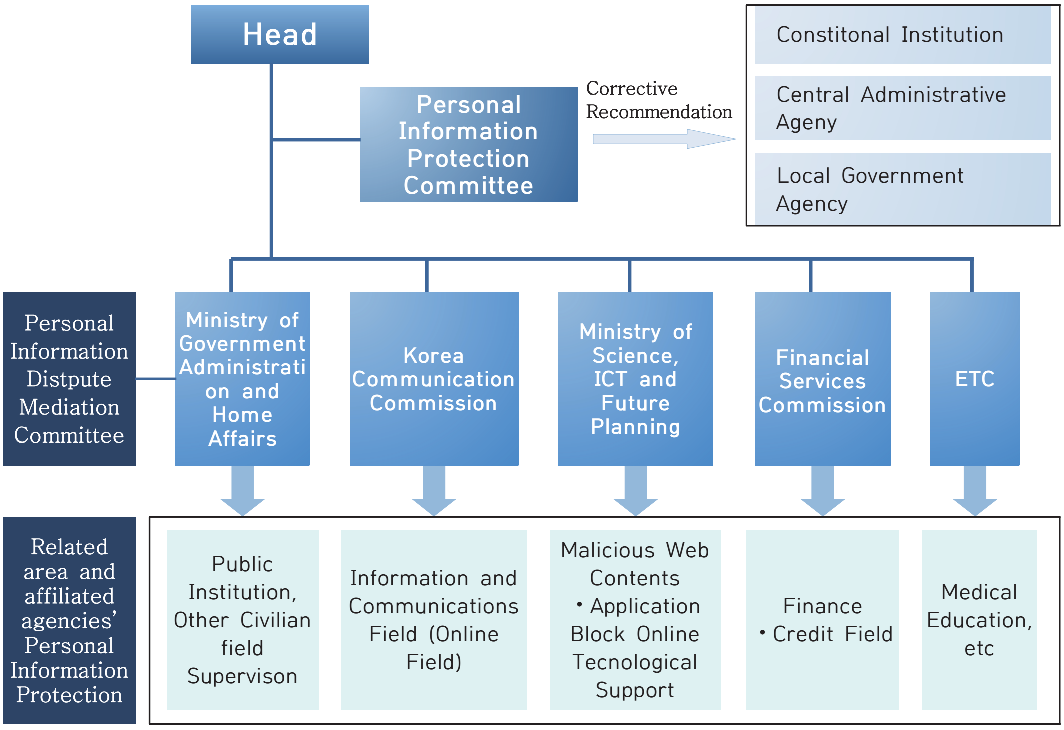
<Personal Information Protection Act> is a general regulation that deals with both public and private sectors' personal information which was established in March of 2011, enacted since September of the same year. The Act was first enacted in order to minimize the damages of leakage of personal information. The Act has regulations regarding the information holder's means of handling the information, or the request of accessing/correcting/deleting one's information, which are ultimately the factors that protects the individual right over their own information. The Act required any holders of personal information (especially the national security number) to codify the national security number. Following, in order to strengthen the capacity of personal choice, the Act was amended to include the necessary confirmation step for the holders to acquire the individual's personal information.

The Central Administrative Agency deals with administrative tasks of its affiliated areas or related specified regulations. Therefore, they establish enactment procedures as to personal information protection, and make sure that the related regulations meet the criteria of <Personal Information Protection Act>. The Personal Information Protection Committee established directly under the President under the <Personal Information Protection Act> come up with trial plans of personal information protection, review and vote for relative law, regulation or policies, and advice on violation of regulation of the local government, court, or constitutional institutions.

On top of this general regulations, there are more specified regulations such as <Act on the Protection, Use, Etc. of Location Information>, <Credit Information Use and Protection Act>, <Protection of Communications Secrets Act>, <Act on the Protection of Information and Communications Infrastructure> or the <Act on Real Name Financial Transactions and Confidentiality>.

On the other hand, regulations regarding personal information protection in public sectors include, <Electronic Government Act>, <Resident Registration Act>, and <Passport Act>. In private sectors, there are specific regulations such as <Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.>, <Credit Information Use and Protection Act>, <Act on Real Name Financial Transactions and Confidentiality>, <Internet Address Resources Act>, <Framework Act on Electronic Documents and Transactions> and <Digital Signature Act>.

Personal Information Protection Promotion Precess[73)]


Head
Personal Information Protection Committee
Corrective Recommendation
Constitonal Institution
Central Administrative Ageny
Local Government Agency
Personal Information Distpute Mediation Committee
Ministry of Government Administration and Home Affairs
Korea Communication Commission
Ministry of Science, ICT and Future Planning
Financial Services Commission
ETC
Related area and affiliated agencies' Personal Information Protection
Public Institution, Other Civilian field Supervison
Information and Communications Field (Online Field)
Malicious Web Contents • Application Block Online Tecnological Support
Finance • Credit Field
Medical Education, etc

Ministry of Government Administration and Home Affairs	• <Personal Information Protection Act>
Personal Information Protection Committee	• Personal Information Protection Related Case · Review Deliberation(Head Division) • Personal Information, Protection basic plan, Policy, system, ordinance, etc. Related case review · deliberation
Korea Communication Commission	• In charge of INS regulation related personal information protection • Research and collect data regarding personal information, investigate, and charge and regulate
Ministry of Science, ICT and Future Planning	• In charge of Information Protection Cyber Security (Online Information Protection) Work • Malicious Web Contents · Application Block, etc. online techonogy support, etc.

[73)] 2016 National Information Security White Paper, pp. 198.

Chapter 4. Conclusion

Based on the comparative analysis of Mongolian and Korean cybersecurity related legislations in Chapter 2 and 3, we compare the characteristics of each legislation, and look for the implication points of policy making and legislative improvements.

In case of South Korea, who possesses longer history of cybersecurity related legislation, we can see that there has been an exponential growth in Information and Communications Technologies (ICT), and a rapid arrangement of institutional framework and related legislations to support such exponential growth. In particular, Korea shows a high dependency on Information Communications, and Korea also has a highest Internet usage rate and the largest number of Internet users in the world. In 2015, the Internet usage rate of Korea was 85.1% with 86.4% of Smartphone possession rate. Moreover, the amount of transactions in online and mobile markets are also exponentially increasing, which again shows the high dependency rate of Korean people on Korean ICT. In the near future, the importance of ICT will only grow bigger with the emergence of new level of ICTs such as Internet of the Things, Cloud Computing, Smart Platform and Big Data.

On the other hand, the risks of injurious behaviors or infringements of basic human rights that happen in cyberspace such as infringement of personal data, leakage of business information, cybercrime, or cyber terror also increase along with the exponential growth of dependency on cyberspace. On top of this, in case of South Korea, the possibility of cyber terror by North Korea stands as a very serious danger factor.

Especially after the 2014 cyber hacking of Korea Hydro & Nuclear Power Co., a full-scale discussion emerged on improving cyber security systems of major national facilities such as nuclear power. Likewise, Korean cybersecurity legislation has developed in reaction to the advancement of Information Communication and its related technologies and infrastructures, as well as the counteracts to increasing cyber danger factors. The occasional cybersecurity related incidents and accidents, and the following frequent enactments and revisions of legislation directly show the progress of rapid maturation of Korean cybersecurity legislation.

Amongst all, one aspect to pay attention to in Korean cybersecurity legislation is the governance encompassing public as well as private sector. Because private sector leads the ICT and its application, a public-sector-centered governance will have difficulty securing the effectiveness of enforcing the law. Therefore, establishing a governance that leads out private sector's capacity and voluntary compliance is crucial, and Korean cybersecurity legislation seems to have a strong suit in this aspect. Although the unified decision-making regarding the national cybersecurity policies is also an important assignment, it seems more ideal to establish an enforcement system based on the usual correspondence of the major actors of cyberspace.

Meanwhile, in spite of the short history of development of cybersecurity legislation, Mongolia puts much effort in counteracting to international cybercrime or cyber terror in cooperation with the related countries. Also, it is worth paying attention to the systematization of legislation based on the concept of National Security Concept, and its subcategories: Confidentiality of Information, Integrity of Information, and Availability of Information. A broader and more systematized cybersecurity legislation is expected once the Law of Data Protection Act, which is in the process of enactment, and legislations such as Law Information Security enact.

Establishment of governance to enforce the law and securing of its capacity, however, is where the focus needs to be on as well as the development of substantial legislation. In reality, despite the substantial growth in current Mongolian cybersecurity legislation for the past 14 years since the revision of Criminal law in 2002, only a few number of information crimes under the Criminal Law were registered with the police or investigation departments due to the lack of knowledge among the majority of law enforcement officers, judicial officers, and judges on what information, data, or cybersecurity is, or how an investigation should be conducted. For the effective enforcement of other cybersecurity related laws apart from the Criminal Law, a cultivation of capacity and a concentration of resources for considerable period of time seems necessary. Therefore, a determination and continuing effort at the decision-making level will have a significant meaning in the whole process.

It is very likely that Mongolia will not experience the same process of development of ICTs and related legislations that South Korea has experienced. Therefore, if Mongolia carefully analyzes the technologies and legislations of those countries, as well as Korea, who already established these aspects, Mongolia will be able to find the most suitable legislation and governance in the near future. Especially, considering the high speed of development of ICTs in Mongolia, the cultivation of capacity of legislature and judicial agencies for a timely correspondence is certainly important because there are times where the current law and policy are incapable to problem-solve the advancing of technologies. In those times, it needs to be asked whether the counteract is possible through the interpretation of current law, and if not, a shrewd judgment call is necessary for the counteract through an enactment or revision of law. For such reasons, a cooperation and further research of related countries, especially Mongolia and South Korea whom were subject to this research, are expected.

References

Articles

Annual report 2014 of Information technology, Post and Telecommunication Authority of Mongolia (ITPTA)

Asia-Pacific Cybersecurity Dashboard (A Path to a Secure Global Cyberspace) by Galexia (2015)

Australian Strategic Policy Institute(ASPI), Cyber Maturity in the Asia-Pacific Region (2014)

Brandon Valeriano, Ryan Maness. “Persistent Enemies and Cyberwar: Rivalry Relations in an Age of Information Warfare”. pp. 139-158. Cyberspace and National Security: threats, opportunities, and power in a virtual world / Derek S. Reveron, editor. Georgetown University Press. Washington DC (2012)

Cyber wellness Profile Mongolia. ITU

Cyber wellness Profile Republic of Korea. ITU

Cybersecurity and Cyberwarfare (Preliminary Assessment of National Doctrine and Organization) by Center for Strategic and International Studies (2011)

D.Myagmar. New Institute for Geopolitical Studies, “The Mongolian Journal of Geopolitical Studies”, №1, 2015. Ulaanbaatar (2015)

Dakota L. Wood: 2015 Index of U.S. Military Strength: The Heritage Foundation (2015)

Derek S. Reveron, Editor. Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World. Georgetown University Press (2012)

Derek S. Reveron. “An Introduction to National Security and Cyberspace”. pp.3-20. Cyberspace and National Security: threats, opportunities, and power in a virtual world / Derek S. Reveron, editor. Georgetown University Press. Washington DC (2012)

Electronic database of Mongolian Court Decisions (2015)

Explanatory Report to the Convention on Cybercrime Budapest, 23.XI. (2001)

Ian J. Lloyd. Information Technology Law (Sixth Edition). Oxford University Press (2011)

Il Seok Oh(Luke), A Legal Study on Enhancing Security Authority’s Cyber Security Activities, Vol. 20, No.3, Journal of Law and Science(Hannam University)(October, 2014)

Il Seok Oh(Luke), A Study on the Compensated “Damages” arising from Breach of Duty to Protect Personal Information, Vol. 19, No.3, Ewha Law Journal(Ewha University)(March, 2015)

Il Seok Oh(Luke), Recommendations on Reforming Critical Information Infrastructure Protection Act of Korea with a View from Risk Allocation, Vol. 19, No.1, Ewha Law Journal(Ewha University) 293 (September, 2014)

Il Seok Oh(Luke), Seung Youl Lee, So Jeong KIM: Designing Effective Responding Legal and Political Measures against North

Korea’s Cyber Attacks: Institute for National Security Strategy (IISS) Policy Studies, vol.186 (2015)

International Telecommunication Union (ITU). Measuring the Information Society Report (2015)

James Andrew Lewis, Denise E. Zheng: Significant Cyber Events: Center for Strategic &International Studies(CSIS) (2016)

Korea Institute for National Unification(KINU): North Korea Domestic and Foreign Policy Evaluation and Outlook after Kim Jong-un seizing the Power: 11th KINU Unification Forum(2015)

L.Galbaatar. Resolving a cybercrime case by a court (training handbook). Ulaanbaatar (2015)

List of Offensive Domain Names. Communications Regulatory Committee (CRC) of Mongolia

Main Indicators of Telecommunications Sector by 1st half of 2015. Communications Regulatory Commission of Mongolia.

Michael A. Vatis. The Council of Europe Convention on Cybercrime (2010)

Moon Taek Kwon: A Study on Countermeasures to the North Korean Asymmetric Strategy - ‘Cyber Surprise Attack’: Journal of Information and Security, vol. 10(4) (2010)

National Cybersecurity Master Plan. Republic of Korea (2011)

National Intelliegence Service, etc., 2016 National Information Security White Paper, (2016) Paul N. Stockton &Michele Golabek-Goldman. Prosecuting cyber terrorists: applying traditional jurisdictional frameworks to a modern threat (2014)

Richard A. Clarke, Robert Knake. Cyber War: The Next Threat to National Security and What to Do about It. HarperCollins Publishers. (2010)

Sangdon Park, Injung Kim: A Study on Tasks for the Legal Improvement for the Governance System in Cybersecurity: Journal of Informational and Security, vol. 13. no. 4 (2013)

So Jeong Kim, Sangdon Park: A Study on Cyber Cecurity Policy in the Context of International Security: Journal of Informational and Security, vol. 13. no. 6 (2013)

Sunha Bae, Sangdon Prark, So Jeong Kim: A Study on the Development for the National cyber security Capability Assessment Criteria: Journal of the Korea Institute of Information Security &Cryptology, vol. 25, No. 5 (2015)

Tobias Feakin: Playing Blind-Man's Buff: Estimating North Korea's Cyber Capabilities: International Journal of Korean Unification Studies, vol. 22, no. 2 (2013)

United Nations E-Government Survey 2014 E-Government For The Future We Want (December 8, 2014)

Websites

http://darkmatters.norsecorp.com/2015/11/23/cyber-issues-china-japan-south-korea-talk/

http://english.yonhapnews.co.kr/news/2015/10/13/0200000000AEN20151013004800315.html?b1e08f30

http://english.yonhapnews.co.kr/northkorea/2013/10/04/62/0401000000AEN20131004007400320F.html

http://khnews.kheraldm.com/view.php?ud=20151208000959&md=20151211003712_BL

http://news.mk.co.kr/column/view.php?year=2014&no=3423

http://news.mk.co.kr/newsRead.php?year=2015&no=611797

http://panmore.com/the-cia-triad-confidentiality-integrity-availability

http://ubpost.mongolnews.mn/?p=18801

http://www.databreaches.net/20-million-people-fall-victim-to-south-korea-data-leak-fss-calls-on-financial-institutions-to-improve-protections-against-insider-leaks/

http://www.heritage.org/research/reports/2015/03/the-us-needs-to-respond-to-north-koreas-latest-cyber-attack

http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

http://www.kookje.co.kr/news2011/asp/newsbody.asp?code=0300&key=20150106.22008193319

http://www.mt.co.kr/view/mtview.php?type=1&no=2015012908211802132&outlink=1

http://www.nsc.gov.mn/sites/default/files/images/National%20Security%20Concept%20of%20Mongolia%20EN.pdf http://www.nsc.gov.mn/sites/default/files/images/National%20Security%20Concept%20of%20Mongolia%20EN.pdf

http://www.pcworld.com/article/2032918/us-south-korea-join-forces-to-prevent-cyberattacks-by-north-korea.html

http://www.securityweek.com/20-million-people-fall-victim-south-korea-data-leak

https://en.wikipedia.org/wiki/Internet_fraud

https://en.wikipedia.org/wiki/Pharming

https://en.wikipedia.org/wiki/Phishing

https://en.wiktionary.org/wiki/cyberviolence

https://www.itu.int/net4/wsis/forum/2016/Content/documents/agenda/WSISForum_2016_DraftAgenda_2016-04-07.pdf

https://www.unodc.org/toc/en/crimes/organized-crime.html

https://www.whitehouse.gov/the-press-office/2015/10/16/remarks-president-obama-and-president-park-republic-korea-joint-press