THE CURRENT SITUATION AND COUNTERMEASURES TO CYBERCRIME AND CYBER-TERROR IN THE REPUBLIC OF KOREA

*Junsik Jang**

I. INTRODUCTION

The Republic of Korea (hereafter: Korea) is a democratic country with a population of 48.46 million (2007). Korea's stance as a powerhouse in terms of information technology is demonstrated by its vast information communication technologies (ICT) production and exports, development of cutting-edge technology, and also the wide use of Internet and mobile telecommunication devices within the country.

When looking at ICT-related statistics and changes which have occurred in Korean society between 2001 and 2007, the number of broadband Internet subscribers increased from 7.81 million to 14.71 million, while the number of Internet users also increased from 24.38 million to 34.82 million. The number of e-commerce transactions also grew between 2003 and 2006, from 7.2 million transactions to 12.8 million. These figures demonstrate that Korea is one of the most successfully connected places on earth, made possible by the strong driving force of the government.

However, the overwhelming number of cybercrimes and security incidents compared to those of neighbouring countries contrast sharply with the positive aspects of Internet usage in Korea. Some may consider the undesirable phenomena inevitable costs accompanying the acceleration of an information society. In contrast, others may attribute these undesirable phenomena to the lack of social and legal control of online activity in Korea. No one reason can explain the situation. Without waiting to identify the cause, the Korean authorities have made a great effort to tackle cybercrime and other attacks, including the threat of cyber-terror. Here I briefly show the current situation and historic changes in cybercrime with countermeasures to prevent, deter, respond and investigate.

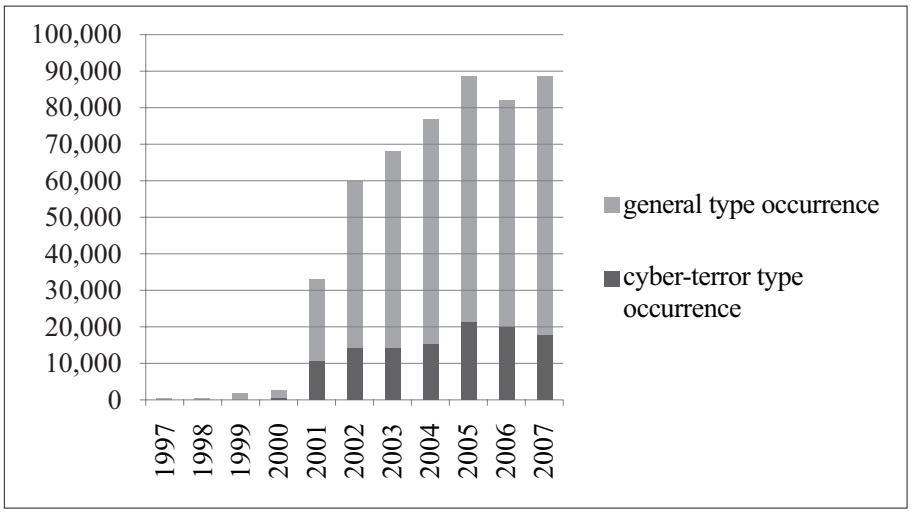
II. THE CURRENT SITUATION OF CYBERCRIME AND CYBER-TERROR IN KOREA

A. Cybercrime Statistics

Korea is one of the most wired countries in the world, but unfortunately statistics show that a variety of cybercrimes also feature in the Korean online environment. Since the Korean National Police Agency (hereafter: KNPA) publicized the first cybercrime statistics in 1997, cybercrime grew at an alarming rate to 2005, as seen in Figure 1. In 2006, we finally saw a decrease in cybercrime for the first time, although this was reversed in 2007.

* Professor/Senior Inspector, Department of Police Science, Korea National Police University, Republic of Korea.

Figure 1: Number of cybercrimes reported to the Korean Police

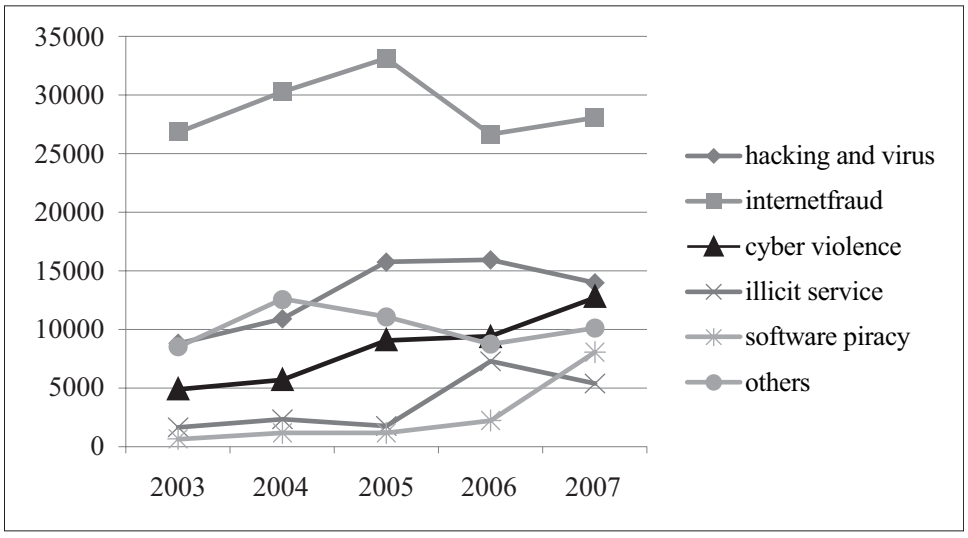


Source : KNPA, March, 2008.

The KNPA has divided cybercrime into two categories;

"Cyber-terror Type Crime" refers to attacks against the information network *per se* such as hacking, mal-ware distribution and Denial-of-Service (DoS) attacks. "General Cybercrime" is crime that uses computers and networks as crime instruments, for example, Internet auction fraud or online child pornography distribution. Each type has several sub-types reflecting the diversity of cybercrime.

Figure 2: Cybercrime occurrence by type



Source : KNPA, March, 2008.

The two most prevalent types of cybercrime are hacking/viruses and Internet fraud. More than half of both types of cases are directly related to online games. Why are there so many cybercrimes? There are a few apparent reasons: digital item trade, anecdotal lack of interest in cyber security, and state-of-the-art Internet infrastructure have all fascinated cyber criminals. Market share of digital items is estimated at more than one billion US dollars in Korea. To improve the situation, legislation prohibiting transactions of virtual money for on-line gambling was activated in 2006.

B. Trends and Issues in Cybercrime

Statistics and cases demonstrate some long-term changes in cybercrime trends. Other changes might occur in a few cases only. These are not exhaustive, but rather representative, examples (cases will be provided separately if appropriate):

- Traditional criminals are hiring tech-savvy cybercriminals internationally. Organized criminal groups have recognized the extent to which they can exploit Internet technology to fulfill their traditional criminal motivations. Their harnessing of technological knowledge makes investigation much harder;
- Mobile Internet devices are replacing Internet cafés as cybercriminals' preferred method of securing their anonymity;
- Collective opinions form on the Internet, stimulate government and are continued into physical movement;
- Cyber rumours and bullying threaten innocent victims;
- Online banking equipped with Public Key Infrastructure was revealed not to guarantee perfect security of customers;
- Korea is losing its negative reputation as one of the greatest sources of cyber attacks worldwide;
- We need to find a solution to the problem of Chinese hackers who speak Korean and target Koreans;
- Identity theft is at the top of the list of serious cybercrimes in Korea. In recent cases, the personal details of more than 10 million people were stolen;
- Virtual Private Networks for secure communications provide criminals with a cybercrime heaven;
- The majority of criminals are not teenagers.

C. Cyber-terror in Korea

Although the term "cyber-terror" has been in use since the late 1990's, vagueness of the concept still remains. Distinguishing characteristics of terror are the violent manners and socio-political intentions of the perpetrators. Even though some attacks seemed to be explicit cyber-terror, the two features are not easy to recognize, even for experts in a specific cyber attack. Rather, nowadays, cyber-terror seems to be noted in regard to the information security of governmental and other critical infrastructures.

Table 1: Number of security incidents reported to the National Intelligence Agency

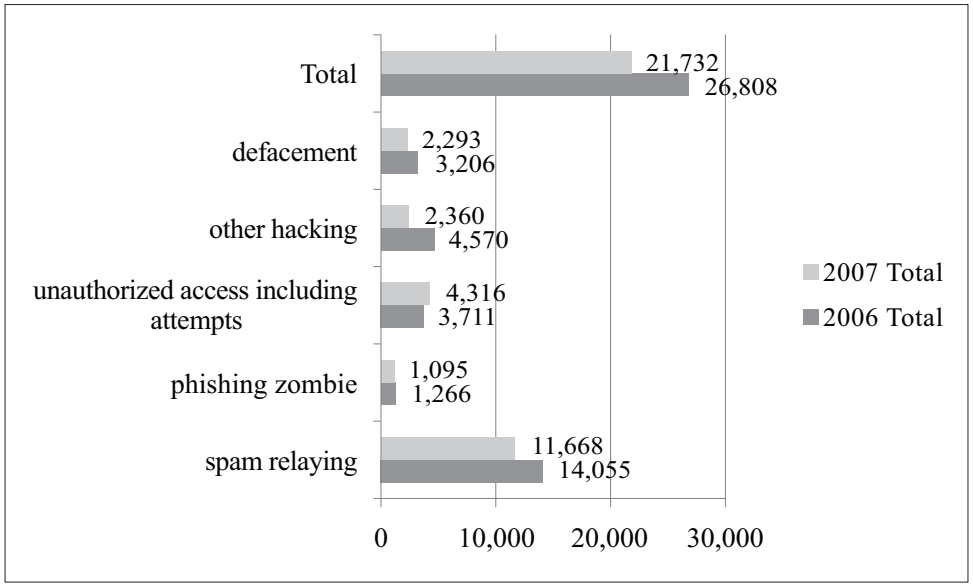
Organization type	Total	Malware Infection	Zombie	Defacement	Impaired or Leaked Data	Others
government	625	498	29	21	55	22
local administrations	3,827	3,583	94	111	24	15
research institutes	198	145	20	8	19	6
education institutes	2,148	1,504	513	91	18	22
affiliated organizations	706	448	85	143	26	4
others	84	16	26	5	34	3
total	7,588	6,194	767	379	176	72

Source: the NIA, April, 2008.

According to the White Paper on National Information Security 2008 by the National Intelligence Agency and Korea Communications Commission, the number of cyber incidents reported in the public domain in 2007 was 7,588 which almost doubled from 4,286 in 2006. The main source of the incidents is infection by Internet worms and viruses.

In contrast, the number of hacking incidents in the private sector which were handled by the Korea Information Security Agency was 21,732. This was a decrease of 18.9% in comparison to 2006.

Figure 3: Number of security incidents reported to the Korea Information Security Agency



Source: the KISA, April, 2008.

Ten important issues concerning cyber security in Korea were selected by the National Intelligence Agency as follows:

- increase in distributed denial-of-service to intimidate for profit;
- promotion of electronic passports containing biometric information;
- incompliance between Windows Vista and domestic security solutions;
- appointment of the first private information security products accreditation body;
- leakage of personal information from public organizations and huge Internet Service Providers;
- issued certificates for public-key infrastructure exceeded 15 million;
- rapid increase in mobile phone spam;
- User Created Content (UCC) became a new security threat;
- Universal Serial Bus (USB) vulnerability is severe;
- obstinate Voice Phishing.

III. THE LEGAL RESPONSE TO CYBERCRIME AND CYBER-TERROR IN KOREA

A. Overview of the Criminal Justice System of Korea

The Korean legal system combines some elements of European civil law systems, Anglo-American law, and classical Chinese philosophies. Constitutional power is divided into three branches; the administration, the legislature and the judiciary. The constitution provides for an independent judiciary.

The judiciary is composed of the Supreme Court, the High Courts, the District Courts, the Family Court, and the Branch Courts. Since 1988 constitutional challenges go to the Constitutional Court. To become a lawyer in Korea, one must pass the Judicial Examination and complete a two-year training course at the Judicial Research and Training Institute.

The Ministry of Justice belongs to the administration. Prosecutors, who have the authority to investigate criminal cases, belong to the Ministry of Justice. As of March 2008, the total number of prosecutors in Korea, which is growing year by year, is approximately 1,655 and they are assisted by a staff of about 7,524 including investigators, administrative clerks and secretaries. Prosecutors' offices correspond to the counterpart court.

Under the Criminal Procedure Act, the judicial police conduct investigations under the supervision of prosecutors. When most crimes (more than 90%) are recognized, however, the judicial police usually initiate and conduct the investigation. The judicial police consist of general judicial police, dealing with criminal

cases in general and special judicial police, in charge of cases specifically related to railway facilities, forests, fire fighting, the sea, etc. General judicial police belong to the Korean National Police, which has 97,700 full-time employees (sworn-officers and civilian), and about 47,000 auxiliary police, who fulfill their constitutional duty of military service by assisting police. According to the White Paper on the police by the KNPA, the number of crimes reported to the police was 1,719,075 in 2006, including 1,073 murders and 4,838 robberies.

In applying the universality principle to cybercrime, the major international treaty that may become the threshold of domestic laws is the Council of Europe Convention on Cybercrime of 2001. Korea has yet to sign the Convention on Cybercrime, but governmental organizations have begun discussing it.

B. Substantive Cybercrime Laws

Currently, Korea provides for the punishment of cybercrimes in the Criminal Act concerning traditional crimes committed by means of a computer, and in various other laws. The most relevant of these are the Act on the Promotions of Information and Communications Network Utilization and Information Protection, etc. (hereafter: Information and Communications Network Act) and the Information and Communications Infrastructure Protection Act, which are special additions to the Criminal Act.

Besides, the following laws are also relevant: the Framework Act on Electronic Commerce and the Digital Signature Act, concerning e-commerce; the Act on the Punishment of Sexual Crimes and the Protection of the Victims Thereof, concerning cyber-sexual harassment; the Act on the Protection of Juveniles' Sex, etc., concerning child pornography; the Copyright Act or Computer Program Protection Act, concerning on-line copyright infringement; the Act on Promotion of the Game Industry, and the Act on Special Cases Concerning Regulation and Punishment of Speculative Acts, etc., concerning on-line games.

1. Criminal Act (revised in 1995)

The Criminal Act was revised in 1995, accommodating social needs and the regulation of emerging types of crime. Most provisions, except those regarding computer fraud, overlapped with those of the Information and Communications Network Act and the sentences defined in the latter are heavier, so the overlapped provisions are not applicable in most cases. Some features of the Act are:

- Manipulating public electromagnetic records (Art. 227-2, max 10 years) and private electromagnetic records (Art. 232-2, max five years or fine of up to 10 million won);
- Computer fraud (fraud by means of computers): Art. 347-2, max 10 years or fine of up to 20 million won;
- Computer interference with business: Art. 314.2, max 5 years or fine of up to 15 million won;
- Impairment of electromagnetic records: public records (Art. 141.1, max 7 years or fine of up to 10 million won); any other records (Art. 366, max 3 years or fine of up to 7 million won).

2. Information and Communication Network Act (revised in 2008)

- Unauthorized access: Art. 63.1.1 and 48.2, max three years or fine of up to 30 million won;
  - ○ making such attempts is also punishable;

- Transmitting or distributing malicious programmes: Art. 71.9 and 48.2, max five years or fine of up to 50 million won;
  - ○ writing malicious programme *per se* is not punishable;

- Denial-of-service attack (sending a large volume of signals or data for the purpose of hindering the stable operation of a network): Art. 71.10 and 48.3, max five years or fine of up to 50 million won;

- Cyber-pornography (distributing, selling, renting, or openly displaying lascivious codes, letters, sounds, visuals, or films through information and communications network): Art 74.2 and 44.7.1.1, max one year or fine of up to 10 million won;

- Cyber-stalking (repeatedly sending words, sounds, letters, visuals, or films inciting fears and uneasiness to any other person through information and communications network): Art 74.3 and 44.7.1.3, max one year or fine of up to 10 million won;

- Others:
  - cyber-defamation with alleging facts (max three years or of up fine to 20 million won) or openly alleging false facts (max seven years or fine of up to 50 million won);
  - transmission of advertisement information for illegal acts (max one year or fine of up to 10 million won);
  - collecting e-mail addresses without permission by technical means (max one year or fine of up to 10 million won);

C. Procedural Cybercrime Laws

The attitude of the judicial system in the application of law to a new legal issue is to interpret current law or to amend or add new provisions to meet emerging needs. Digital evidence is the most widely used term to depict the new type of evidence consisting of zeros and ones, which signify the greatest challenges concerning criminal procedural law in cybercrime investigations and in court.

Legitimacy of the procedures followed during the collection of digital evidence is the top issue. The most significant method of doing this is a search and seizure operation as defined in the Criminal Procedure Act which is the foundational law for all criminal procedure. There is almost no provision allowing for the statement of digitalized evidence; therefore, the search and seizure issue is basically an interpretation problem. Special procedures, including wiretapping electronic communication to collect specific types of data from specific sources, are defined in a few different laws as outlined below. In court, there are also numerous legal issues.

However, the legal issues concerning digital evidence have been challenged in only a few cases. That is why many investigators are still confused as to how to apply the law in their cases.

1. Search and Seizure

Search and seizure is one of the most important procedures used to acquire evidence. For the search and seizure of electromagnetic records stored in a computer, the cybercrime investigative organizations should first obtain warrants under the legal conditions in force, just like they do in cases of other crimes, unless there exists an exceptional situation, including circumstances in which an emergency arrest is appropriate. Therefore, in response to the Constitution, the suspicion, the scope and the place of the search, as well as the target of the seizure, etc., must be specified by the search and seizure warrant for electromagnetic records.

2. Telecommunication Information

The Telecommunications Business Act (revised in 2006) regulates the procedure of acquiring account and other basic information from the Telecommunications Business Operator. The objects of the request include:

- Names of users;
- Resident registration numbers of users;
- Addresses of users;
- Phone numbers of users;
- IDs (referring to the identification codes of users which are used to identify the rightful users of computer systems or communications networks);
- Dates on which users subscribed or terminated their subscriptions.

The request should be made by way of a written document of a court, a prosecutor or the head of the investigation agency.

3. Transaction Records

Transaction records are defined as "communication confirmation data" in the Protection of Communications Secrets Act (revised in 2008). An investigative authority may ask any operator of the telecommunications business for the perusal or the provision of the communication confirmation data. The records of telecommunications falling under any one of the following items are communication confirmation data:

- The date of telecommunication by subscribers;
- The time that the telecommunication commenced and ended;
- The number of outgoing and incoming calls, etc. and the subscriber's number of the other party;
- The frequency of use;

- The computer communications or Internet log-records relating to facts of using the telecommunications services by the users of computer communications or the Internet;
- The data on tracing a location of information communications apparatus connecting to the information communications networks;
- The data on tracing the location of connectors capable of confirming the location of information communications apparatus used to connect with the information communications networks.

When an investigative authority officer asks for the provision of the communication confirmation data, he or she must obtain permission from the court, with a document. If urgent grounds exist, he or she shall obtain permission immediately after asking for the provision of the communication confirmation data. Provision of real-time records is executed by the same articles in practice. Asking other parties, including non-public information holders, for the same type of data is executed under search and seizure clauses.

The co-operative obligations of operators of telecommunications businesses for wiretapping and acquiring transaction records and the minimum three-month mandatory period of keeping transaction records are defined in law, but operators are not compelled by any other measure to follow the necessary provisions.

4. Wiretap

Wiretapping telecommunications is strictly confined by the Protection of Communications Secrets Act (revised in 2008). Most importantly, wiretapping can be permitted by a court only for prevention and investigation of serious crimes enumerated in the law. There is no typical cybercrime included in the serious crime types. Therefore, in practice, monitoring, surveillance, or packet capturing for the purposes of cybercrime investigation must be conducted without accessing the content of the communication.

5. Digital Evidence in Court

Electromagnetic records seized by warrant are not made readable until printed. The admissibility of the records thus printed, if submitted as evidence, may be questioned. There is no written regulation on this matter, but the Supreme Court adjudicated on a recent case requiring high level reliability of the programme used, the person who dealt with the evidence, the chain of custody, procedures, etc., to admit authentication and admissibility of digital evidence.

Regarding the identity of the electromagnetic records and the printed document, the person who printed out the electromagnetic records by means of a certain programme should have to testify to the authenticity of the printed document at the trial. In addition, to the extent that the electromagnetic record is deemed identical to the printed document, the latter should be deemed original.

On the other hand, if the document that is made visible and readable by printing the electromagnetic records is used as evidence of a crime, this document may be deemed statement evidence made by extracting a human idea through an electronic method, i.e., hearsay evidence without cross-examination. Therefore, the rule of hearsay evidence under Article 311 of the Criminal Procedure Act and the provisions that follow shall be applied in determining the admissibility of such documents.

IV. THE COUNTERMEASURES TO CYBERCRIME AND CYBER-TERROR IN KOREA

A. Framework for National Cyber Security

The Framework for National Cyber Security has been formulated not by design, rather it has developed by trial and error. A few critical cases, including Slammer Worm hits in 2003 which caused catastrophic interference to country-wide Internet connections, and alleged organizational attacks targeted at major governmental networks found in 2004, served as a crucial momentum to reform past frameworks.

The main focus of the reforms was to integrate distributed resources and capabilities within a single framework and make strict ties between the spots to draw a bigger picture. The current National Cyber Security can be divided into three sub-systems: General Cyber Security responsibility; Critical Infrastructure Protection systems; and Cyber Security Management systems.

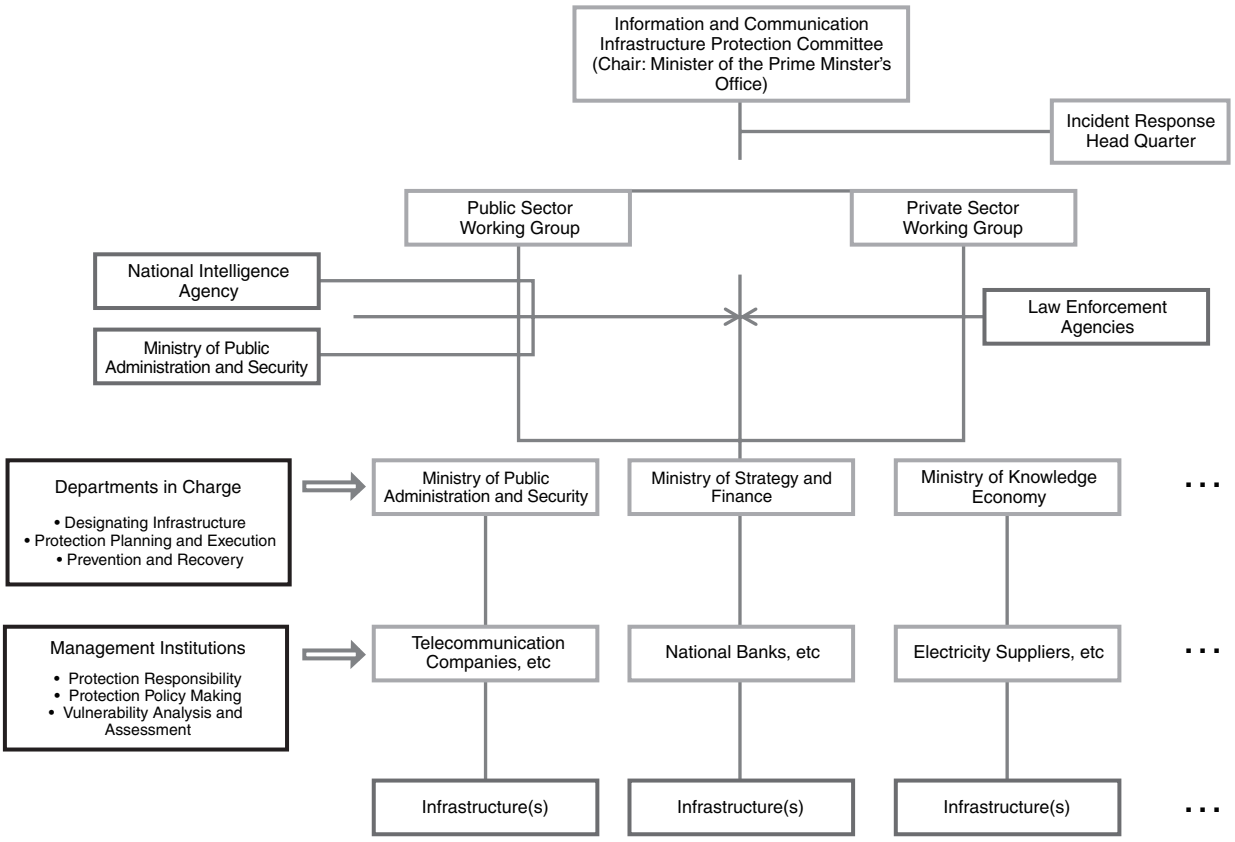
B. General Cyber Security

As an extension of traditional national security management, each governmental organization is responsible for its own assets and affiliated organizations. The National Intelligence Agency Act and the Regulations on Intelligence and Security Affairs Co-ordination (Presidential Decree No. 16211) are legal grounds for this responsibility.

C. Critical Infrastructure Protection

In 2001, Korea enacted the Act on Information and Communications Infrastructure Protection to make a framework to protect highly important networks such as military, communications, finance and so forth. Once designated, a governmental administrative organization that is responsible for the network has to form an effective information security policy followed by vulnerability analysis and assessment. The punishments for an attack and attempt to damage the Critical Infrastructure are more severe than those for similar actions directed towards the other systems and networks.

Figure 4: Organization Chart for Critical Infrastructure Protection



The chairman of the Information and Communication Infrastructure Protection Committee, which directs government organizations which manage infrastructure under its supervision, answers to the minister of the prime minister's office. Once a major incident happens in any critical infrastructure, a temporal incident response headquarters is set up. Law enforcement agencies are responsible for investigation of the incidents.

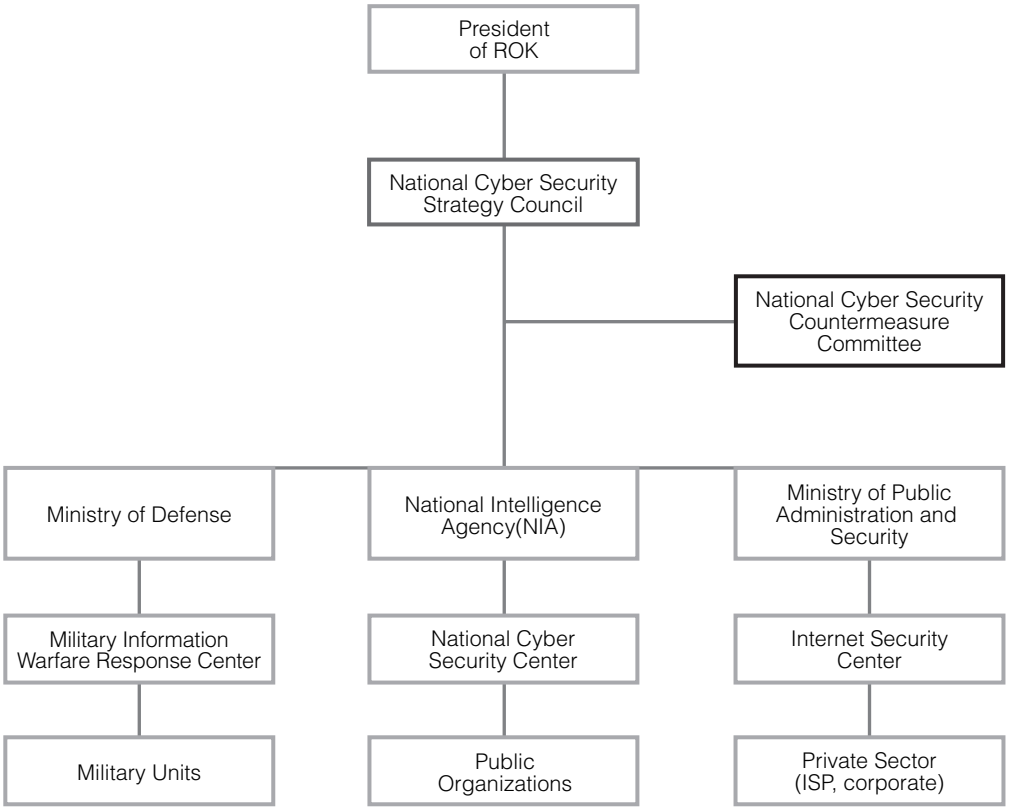
1. Cyber Security Management

A Cyber Security Management system was established to enhance mainly the capability to respond to incidents in three comprehensive parts; public, private and military. Major operations of Cyber Security Management are:

- Integration and implementation of national-level cyber security policies;
- Cyber-security proactive actions;

- Collecting, analyzing and disseminating information on cyber threats;
- Emergency response, investigation, and recovery support during intrusion incidents.

Figure 5: Organization Chart for Cyber Security Management



Among these agencies listed above, investigation is responsibility of law enforcement agencies. Presidential Directive No. 141, the National Cyber Security Management Regulation, is the main legal source. Several important organizations implement the policies directed by each central administrative agency.

(i) National Cyber Security Center

The National Cyber Security Center is the central point of government for identifying, preventing and responding to cyber attacks. The NCSC is responsible for analysing cyber threats and vulnerabilities and disseminating threat warning information.

(ii) Military Information Warfare Response Center

The Military Information Warfare Response Center is responsible for protection of military infrastructure and response against attacks on the network.

(iii) Korea Internet Security Center

The Korea Internet Security Center is one of the divisions of the Korea Information Security Agency (KISA). The mission of the KISC is collecting information and detecting attacks, major network monitoring, disseminating alerts, incident analysis and technical support, mainly for the private sector.

(iv) Other Specialized Organizations

- National Security Research Institute: Researching and developing technologies concerning cryptography, counter-attack, and other security technologies;
- Korea Information Security Agency: Reacting to security threats properly at the national level, and providing integrated and systematic information security services. It includes the Internet Security Center;

- Electronics and Telecommunications Research Institute: Non-profit government-funded research organization that has been at the forefront of excellence on information technologies;
- Financial Security Agency: Being established by entire financial industry to provide proper security service for member corporations and customers.

2. Prosecutor as an Investigative Authority

Not only are public prosecutors responsible for prosecution, but also they have authority to investigate all kinds of crime through investigative units within prosecutor's offices. The public prosecutors' offices of Korea have a hierarchical structure consisting of the Supreme Public Prosecutors' Office (SPO), five High Public Prosecutors' Offices (HPPO), thirteen District Public Prosecutors' Offices (DPO), and forty branch offices of the District Public Prosecutors' Offices. Among them, the SPO and the Seoul District Public Prosecutor's Office have units designated for high-tech crime investigation, including cybercrime. Those units are the High-tech and Financial Crimes Investigation Division in the SPO and the High-tech and Financial Crimes Investigation Department in the Seoul District Public Prosecutor's Office.

(i) Investigation by Prosecutors

Most cybercrime investigations are initiated by the police. Prosecutors conduct continuing investigation after the transfer of each case to decide whether or not to file for prosecution. Prosecutors also conduct investigations *ex officio*. The cases initiated by prosecutors are commonly distinguishable from those investigated by police. Prosecutors tend to focus on cases having a bigger social impact. Most of them are not dynamic but static. Theft or leakage of trade secrets is a typical investigation initiated by prosecutors. This creates natural divide in types of crime investigated by the police and prosecutors.

The High-tech and Financial Crimes Investigation Division is also responsible for co-operation concerning Internet crime and is the contact point of the G8 24/7 High-Tech Crime Network in Korea.

(ii) Digital Forensics for Prosecutors

Digital forensics is a key element in solving a variety of types of crime today. The effectiveness of digital forensics have been proven in a number of financial, high-tech, corruption cases. To integrate and improve digital forensic capability, a comprehensive digital forensic lab is under construction.

3. The Cyber Terror Response Center and Cyber Policing in Korea

The Korean National Police has devoted its efforts to securing safety in cyberspace with the establishment of the Cyber Terror Response Center in 2000, which was initiated from establishment of the Computer Crime Investigation Squad at the National Police Agency in 1997.

In regard to the outstanding activities gaining renown in the global law enforcement society, the Korean government selected the brand name "*Cyber cop NETAN*", a compound of "Net" and "An", meaning "safety" in Korean, as one of the renovation symbols of cybercrime investigation in 2007.

(i) Organization and Human Resources

The Cyber Terror Response Center (CTRC) is the cyber division of the Korean National Police Agency (KNPA), operated within the Agency's Investigation Bureau. The object of the CTRC's investigation includes, but is not limited to, cyber attacks against the Republic of Korea and its people. It is headquartered within the KNPA main building; at present the Center's administrative wing commands and controls all cybercrime investigation teams nationwide, which are installed in each of the investigation functions of the 16 provincial police agencies and 238 local police agencies. The CTRC consists of six teams:

- Administration and Co-operation Team: Plans policies against cybercrime, training and co-ordination of domestic and international co-operation;
- Three Investigative Teams: Conduct major, national-level cybercrime investigations, including cyber-terror type attacks;
- Investigative Planning Team: Receives crime reports, analyses trends of cybercrime and plans a nationwide crackdown operation on special issues;
- Technical Assistance Team: Researches and develops investigative techniques, provides digital forensic services to all law enforcement agencies through the Digital Forensic Center.

As of July 2008, about 900 sworn officers and civilians are exclusively dedicated to cybercrime investigation and support. The majority are police officers working as cybercrime investigators. Among them, 168 officers have been recruited through a special hiring process for ICT specialists possessing adequate academic education and work experience. Most forensic examiners in the Digital Forensic Center are qualified civilian experts.

(ii) Cybercrime Response Activities

(a) Strengthen investigation capability with professionalism

The top priority to enhance investigative capability is to encourage specialized personnel to join and train. The CTRC provides initial training, domestic and international continuing education, and on-the-job training.

(b) Satisfying citizens by rapid responses and a strategic approach

A 24/7 complaints procedure which receives and responds to complaints through an exclusive website and a cybercrime call centre linked with the police emergency network are being maintained. The reports are saved in a data warehouse called e-CRM (Customer Relationship Management) and are analysed by dedicated specialists.

(c) Domestic co-operation and crime prevention activity

No fewer than 125 private enterprises and 85 organizations including academia and non-governmental organizations are tied with a single contact point and hotline. Educational activities and an alert system are playing a crucial role in preventing cybercrime and reducing the number of teenage criminals. *Nuri-cops*, civilian supporters, are not only enhancing mutual understanding, but they are sometimes helpful enough to notify police of unknown but important events on the net.

(d) International co-operation in cybercrime investigation

The CTRC has hosted several international events related to cybercrime and cyber-terrorism, including the Annual Symposium on Cyber Terror. Instructors are frequently dispatched for international training programmes or to deliver specially designed instruction to requesting countries. Through the Interpol network or other channels such as the Cybercrime Technology Information Network System (CTINS), the CTRC maintains a hotline with more than 110 countries. The CTRC has so far contracted a Memorandum of Understanding (MOU) with leading agencies on cybercrime investigation in 15 countries.