



Competent Government

Establishing a High-Tech Cyber Crime Response System

- The National Police Agency of Korea





Establishing a High-Tech Cyber Crime Response System

Jeongseon Park (Professor, Korea National Police University)

Case Overview

The National Police Agency has established an integrated cyber crime response system in association with cyber crime task force, public organizations, industrial firms, and private and public research centers in order to effectively respond to crimes in cyber space, a new type of crime in digital society, in addition to establishing counter-cyber terror center at the Police headquarters. The establishment of the system was possible with advanced IT technology in Korea. Many countries including France and Thailand dispatched personnel from police and other law enforcement agencies to adopt this system to their countries. The system was recognized as the best government policy adopted by the foreign countries by the Office for Government Policy Coordination in April of 2005.

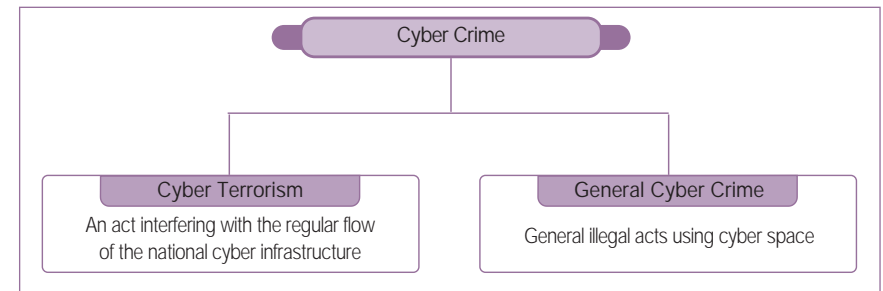
I. Background

The National Police Agency of Korea is currently classifying and coping with cyber crime in two separate categories: cyber terrorism and general cyber crime.

Cyber terrorism represents "electronic invasions into the nation's major information communication infrastructure interfering the regular flow of the nation's electrical, transportation, telecommunication, and government service infrastructure." According to the provisions of the National Police Agency, cyber terrorism is "an illegal act targeting telecommunication networks, attacking computer systems and telecommunication networks by hacking,

disseminating viruses, mail bombs, and network attacks.

<Figure 1> Types of Cyber Crime



General cyber crime is described as "an illegal act using cyber space, such as cyber gambling, cyber stalking and sexual violence, cyber libeling, the issuance of threats, e-commerce fraud, and disclosure of personal information." While cyber terrorism is a crime targeting the nation's major infrastructure, general cyber crime is not limited to attacks on national institutions. Moreover, the machinations of cyber terrorism are not limited to hacking and viruses, but are more extensive and include criminal acts such as operating illegal sites, cyber sexual violence, dissemination of pornographic material, internet fraud, cyber libeling, etc.

To adequately confront the recent surge in cyber terrorism and general cyber crimes, the National Police Agency of Korea (KNPA) has established and is currently operating an integrated Cyber Crime Response System. The Cyber Terror Response Center of the main office is taking a pivotal role and is linked to other cyber crime investigation departments in public institutions, industrial facilities, and research institutions.

With the experience of establishing and operating a high-tech Cyber Crime Response System, the KNPA has held various international conferences such as



the 5th International Computer Crime Conference (2002.10.15-17), the 4th Interpol Asia-Pacific IT Crime Investigation Committee Conference (2002.10.18-19), the 2nd Interpol Asia-Pacific IT Crime Investigation and Drill Seminar (2004.7.18-21), the 1st Interpol Asia-Pacific IT Crime Investigator Training Workshop (2004.11.8-12), and the 2nd Interpol Asia-South Pacific IT Crime Investigation and Drill Seminar (2005.7.19-21). It is taking the lead in disseminating its techniques to other countries. As Korea's cyber crime investigating techniques are gaining recognition abroad, many countries including, France and Thailand, are dispatching police, prosecution, court, and IT personnel to Korea to benchmark the Korean Cyber Crime Response System.

On February of 2004, a U.S. Army computer at SPACECOM was hacked. This case was solved with the help of the Cyber Terror Response Center. In addition, the U.S. deputy director of the FBI visited Korea concerning this matter¹⁾. According to the analyses of foreign countries benchmarking Korea, the KNPA's Cyber Terror Response Center received high praise.

The background for the KNPA to establish such a high-tech cyber crime investigation system is the surge of cyber crimes in the information age, the ever-worsening damage of cyber crimes, and the limits of the private sector to combat cyber crimes. In this context, it was impossible for the KNPA to not establish capacity to combat cyber crimes.

1. The surge of cyber in the information age and the development of internet

South Korea has intensively fostered information communication industries

1) 1) Quote from English article (2004.10.13). Source: www.crime-research.org/news/13.10.2004/709/.

and strongly promoted the informatization of its entire populace since the beginning of the 1980s in order to take the lead in the information age of the 21st century. As a result, the IT industry, which accounted for only 6.2% of the total GDP in 1996, has increased to 15.1% in 2000, surpassed 17.9% in 2003, and approached 20% in 2005. The size of domestic e-commerce has also consistently grown after 2000 and exceeded 300 trillion won in 2004, and has recorded 170 trillion won during the first half of 2005. Of the total number of transactions, the proportion of e-commerce trade has already surpassed 20% in 2005. This means that 1 out of every 5 purchases is made on-line. Furthermore, 31,580,000 people, which is about 70.2% of the population, are using the internet, and the population using broadband internet reached 12,203,290 people in May 2005 with a penetration rate of 25.27%, ranking 1st place in the world. The Republic of Korea is also pioneering the ubiquitous cyber age by combining the internet with mobile phones, PDAs, and DMB satellite terminals.

The development of the internet makes it possible for people scattered all around the world to share information, form communities, and express individuality, and therefore, greatly contributing to the improvement of the quality of life and the development of new industries.

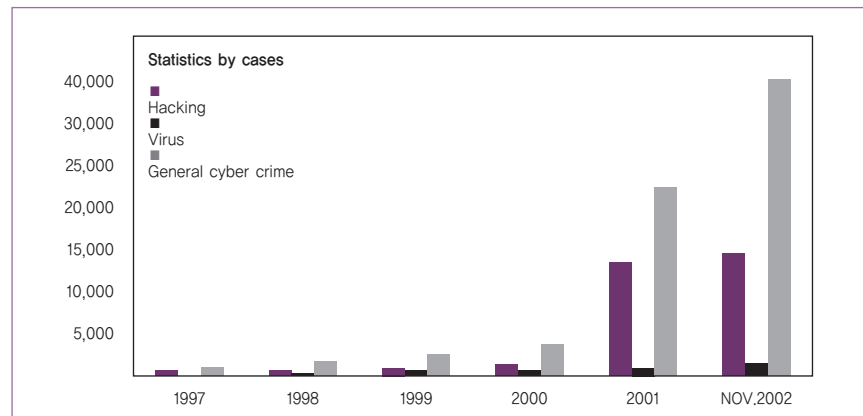
However, notwithstanding these positive outcomes, people are making bad use of it as well, and cyber crime is increasingly more intelligent, sophisticated, and extensive. On top of familiar preexisting problems such as hacking, viruses, and worms, the current situation is infested with various cyber crimes such as phishing²⁾, pharming³⁾, bot-net⁴⁾ and others.

2) Phishing, a compound word constituted of fishing and private data, is a sort of online fraud. A phishing criminal disguises his identification as a reliable company, uses email or a fake site as an authentication program to collect the user's information, and then uses it to make a profit. It is largely divided into phishing emails and phishing websites, which are hard to distinguish from authentic emails or websites because the graphic, writing style, font, layout, and etc, are very similar and elaborate.



Cyber crime in Korea is increasing. According to Yonhap news, Korea ranks third, following the U.S. and China, in sending spam mail³⁾. Hacking and illegal programs are widespread and antisocial sites, inducing suicide and murder by contract, are also being operated freely. As shown below in (table 1), hacking and general cyber crime, which was a mere few hundred in 1997, has increased annually and began rising rapidly after 2001. The annual increase of general crime was 1.89% for the most recent 4 years, recording 1,860,687 cases in 2001 and 1,968,183 cases in 2004, and the annual increase of cyber crime was 40.94%, almost 20 times the rate of general crime, recording 33,289 cases in 2001 and 77,099 cases in 2004. Comparing it by the type of crime, felonious crime and violent crime has decreased 6.2% and 2.9% respectively in 2004, while cyber crime has made a great leap of 12.6%.

<Figure 2> Increase of cyber crime in Korea



(Source: (Korean) KNPA Cyber Terror Response Center:
http://ctrc.go.kr/English/statistics/statistics_01.jsp)

3) A criminal act in which the domain that a specific site operates under officially is taken over and thus the IDs, passwords, and account information of users who access regularly are usurped.
 4) Bot-net is a malignant program used by worm programmers and cracker groups to usurp private or national security information, or to attack specific sites by remotely controlling network computers infected with the worm.
 5) Comparing the internet penetration rate of the U.S. and the population of China, the statistics reveal the high level of Korea's cyber crime. (Yonhap news 2005. 09. 03)

Korea is now unexpectedly facing the side effects of cyber crime due to the development of the information communication industry and informatization. The increase of cyber crime was a big burden and challenge for Korea, a country trying to develop its information communication industry to enhance national competitiveness and the quality of people's life. Therefore, the establishment of a national institute to comprehensively settle the matter was very much in order.

2. The change of public consciousness in accordance with the seriousness of cyber crime damage

In the early stages, hacking and disclosure of information was done out of the curiosity of hackers who wanted to demonstrate their abilities. However, as hacking techniques advanced and the importance of the disclosed secrets became serious enough to influence national welfare, hacking and information disclosure was no longer a joking matter or mere display of one's ability, but was recognized as a more serious type of crime.

Taking a look at the change of domestic knowledge information infrastructure between 1998 and 2001, governmental e-commerce has surged from a low 21.2% to 80.6%, government e-procurement rate has increased from 19.3% to 87.5%, and online stock trading has increased more than 20 times from 3.7% to 66.6%. Also, all of the nation's major institutions are connected by computers and internet networks.

If cyber terrorism or the hacking of computers occurs through the internet, and thus information is disclosed, it could cause immeasurable danger to the supplying essential resources and services such as energy or water, transportation and communication, finance, and national security, etc. Also, on



an individual level, people suffer from a loss of personal privacy and can incur severe economic damage and loss because of cyber terrorism.

As the gaming industry grew suddenly to a size reaching 1 trillion won, disclosure of personal information, item fraud, illegal trade of items, illegal trade of cyber money, and moreover, critical problems such as tax evasion, are on the rise. During the past 5 years, game-related crimes accounted for 40% of total cyber crime and 90% of the criminals were teenagers. Furthermore, game-related crimes such as game item fraud ranked the highest, taking up 53% of juvenile cyber crime.

It is difficult to find a study in Korea calculating the social cost of cyber crime, but according to research abroad it is estimated to surpass 100 trillion won. The FBI calculated that the social cost of cyber crime is \$400 billion in the U.S., which is 400 trillion won. Assuming that the economic size of Korea is 1/20 of the U.S., this means that the costs of cyber crime here reach about 20 trillion won. However, considering the fact that the scale of e-commerce in the U.S. was only 70 trillion ⁶won (\$70 billion) in 2004 compared to Korea's 300 trillion won, the costs here should be much higher.

The McAfee institute has announced a report containing a few valuable examples such as calculating the costs and techniques of cyber crime on household computers, government computer networks, and business computer systems.⁷⁾ During the 2005 cyber crime investigation, code named "Operational Firewall," government officials in the U.S. and Canada prosecuted global cyber crime organizations operating in 6 different countries, and have arrested 28 offenders. The criminals had stolen 1.7 million credit card numbers and traded card and identification information from which the related institutes

6) McAfee Virtual Criminology Report(2005). This cost appears to have excluded traveling cost, automobile, prescribed medicine, and etc. According to data Jupiter Internet Shopping Model has calculated showing the change of e-commerce size excluding the aforementioned category, it was \$12.3 billion in 1999, \$82.9 billion in 2004, and is expected to reach \$130.3 billion in 2006.

7) McAfee Virtual Criminology Report (<http://mcafee.com/us>)

suffered a \$4.3 million loss. Perhaps only 5% of the total cyber crime is exposed to the law enforcement agencies.

Cyber criminals steal IDs by drawing out personal information from the database of companies or card businesses, and causing damages to thousands of customers. If a virus was a means to boast one's ability in the past, it now functions as a medium to extract information. Computers that are infected by bot viruses are remotely controlled and are thrown into a defenseless state to information disclosure. Some bot-net owners lease the bot-net that they have designed for \$200-300 per hour to illegal users.

Looking at the facts depicted above, it is obvious that cyber crime causes not only economic and social damage but also serious damage to individual privacy, and hence it is of great importance to each of us on a personal level. Worse, this menace is increasing rapidly.

3. The limits of the private sector in response to cyber crime

The primary responsibility for cyber crime in commercial fields such as cyber banking or e-commerce belongs to individual businesses. However, the reality is that it is not possible to place all of the responsibility of cyber crime and security on them. When a cyber crime occurs, it is too difficult for individual businesses in need of judicial power to settle the matter by themselves. The government must step in and devise a proper measure in response to cyber crime.

However, a bigger problem is that cyber crime is not limited to just the private sector. There are no boundaries, no divisions between the government and the people. Good citizens and heinous criminals coexist in the same cyber space. This kind of open information-sharing environment makes potential



criminals able to steal national or industrial secrets and incite chaos by disturbing the country's computer network or destroying the air traffic control network. Moreover, conflict in cyber space has enough destructive power to spark wars between countries. For example, in the Kosovo war Yugoslavia hacked into the U.S. public internet, and the U.S. and China have announced that a cyber war using hacking and virus techniques as weapons will appear in the future. With this situation, it is a matter of great importance for the government to actively establish its position on cyber crime and cyber terrorism.

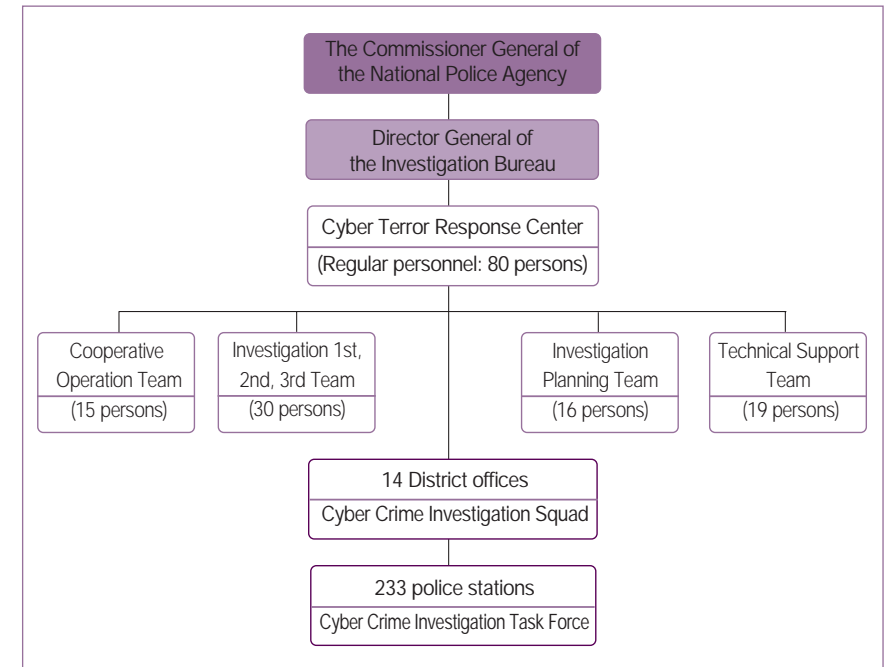
II. The elements of the High-tech Cyber Crime Response System

1. Small and strong organization

The KNPA's Cyber Terror Response Center is in charge of protecting against cyber terror. It also educates cyber investigators nationwide, investigates cooperatively with other countries, carries out initial measures, conducts 24-hour monitoring, investigates major cyber terror cases, develops cyber terror investigating techniques, and gives technical support.

The Cyber Terror Response Center is under the control of the KNPA's investigation bureau. It operates a 3 team/1 lab system constituting the Cooperative Operation Team, Investigation Planning Team, and Technical Support Team, with the Investigation Lab employing three teams (simply enumerated as First, Second, and Third investigation teams)

<Figure 3> Cyber Terror Response Center organization



The Cooperative Operation Team plans and devises overall policies related to cyber crime measures, undertakes the PR role, and manages matters concerned with domestic and foreign cooperation. The Investigation Planning Team plans and directs investigations on cyber crime, and receives/settles related civil complaints. The Technical Support Team makes use of the Digital Evidence Analysis Center and supports the development of related cyber investigation techniques.

8) The Digital Evidence Analysis Center analyzes digitalized evidence, supports investigation, and engages in related research and development. While forensic work traditionally put the emphasis on fingerprints, stolen goods, footprints, on-site traces and so on, digital evidence can be an access record, IP address or any other traceable data that is recorded on the hard disk.



Finally, the Investigation Lab, composed of the three Investigation Teams, is mainly in charge of the direct investigation of cyber crime. The only reason to have divided the Investigation Lab into three teams is to efficiently manage staff. There is no big difference between them. However, tough cases may be given to a specific team where a staff member with advanced techniques is stationed.

2. Securing talented human resources and managing their workflow

The human resources system of the KNPA's Cyber Crime Response System deserves considerable attention. Differing from the traditional concept of investigation, cyber investigation is a very difficult field requiring two types of professionalism: investigative professionalism and technical proficiency in IT. To simultaneously fulfill these two requirements, a special human resource system and flexible workflow formatted is required.

The Cyber Crime Response System currently utilizes a mixed method of securing human resources. Thus, it is recruiting from the private sector and fostering human resources on its own at the same time. Appointing young and talented people is regarded to be of great importance due to the nature of the cyber crime investigation squad, which has to continuously reinforce the human resources of the private sector to secure the necessary talented people and expand new technology. To do this, the cyber crime investigation squad is employing about 20 cyber investigators a year as senior police officers, one rank above a regular police officer. Also, the Cyber Crime Response Center is operating special training programs by which its personnel continuously recharge their cyber knowledge. Human resources secured in this method are posted from coast to coast according to their professionalism and abilities.

This gives Korea an edge over other countries in this particular field.⁹⁾

Meanwhile, the Cyber Terror Response Center is operating a flexible duty system due to the nature of its work. The first-line police officer switches flexibly from a fixed duty system of 3 team 2 shifts (56 working hours per week) to a modified 4 team or 6 team duty system to minimize impasses and improve work efficiency. However, although cyber crime investigators have a fixed commuting time different from the first-line policemen, they also have night-watch duty to ensure coverage.

3. High-tech investigation techniques and program development system

Technique is no less important than human resources in cyber crime investigation. To properly investigate cyber crime, advanced techniques are required and each investigator should possess such abilities. These include many computer techniques such as cyber log analysis, digital evidence analysis, program development ability, and so on.

⁹⁾ According to a study done by EURIM, announced by the House of Commons of England, the police law enforcement institute is in need of trained investigators and digital forensics experts. The need is greater than that of money or legislation. The problem is that notwithstanding the fact that cyber-crime is becoming more common, the ability to trace and analyze cyber-crime is absolutely insufficient because there are not enough police personnel and computer experts. According to the president of EURIM, only 1,000 of the total police force, 140 thousand officers, have received special training on cyber-crime, and only 1/4 of these people can be called an expert. As a result, 6 to 12 months of cyber-crime workload sits untouched, waiting for investigation to start. It is the conclusion of the report to newly open a special educating course related to cyber crime investigation in every school. Meanwhile, Neil Fisher, head of England's Science Technology Security Measures Response Unit, offered a method to use experts of the private sector to reinforce England's cyber-crime response ability. Pointing out that the National Hi-Tech Crime Unit and District Police Agencies are already educating policemen through the help of private businesses for the investigation of digital evidence, and that it is still insufficient, Fisher emphasizes that "We can win the war against cyber criminals only if we educate the police force to analyze digital evidence using talented experts from the private sector."



Korea possesses all of the necessary high-tech techniques and programs for cyber crime investigation. First of all, the techniques and programs the Korean cyber crime investigators possess are by far superior to those of other countries. As previously mentioned, investigation staff and IT technicians are organized in a well-balanced ratio in the law enforcement office, and each team gains a synergy effect through special supplemental education and interactive exchanges with specialists in other fields. Moreover, the specially employed technical experts from the private sector have thorough knowledge of not only the windows series, but also other operating systems such as Linux or Unix and programming languages such as C++, Java, SQL, and they possess unrivaled abilities to independently develop and operate various programs that can ferret out cyber criminals. They are also well-acquainted with databases, network security, not to mention the concept, definition, layout, and establishment of networks, and are computer whizzes possessing computer techniques to track and apprehend hackers.

An elaborate description of the recently developed program cannot be provided for security reasons, but it is known to be a technique of the highest quality. However, such investigative know-how is not possible by just possessing advanced IT technology. If not for the cooperation and assistance of the investigation veterans, who are equipped with many years of practical experience, the KNPA's cyber crime investigations would not be as effective.

In addition, the KNPA founded the Digital Evidence Analysis Center in November 2004, and is developing and complementing the high-tech cyber crime investigation techniques through scientific equipment.¹⁰⁾ The Digital Evidence Analysis System is a technology and a procedure that secures

various evidence to prove the facts constituting an offense when a crime occurs by searching the HDD of a computer or analyzing internet logs. In other words, it designates all technologies and procedures that collect, extract, and reserve all evidence in a crime using a digital medium such as a computer. The KNPA has invested a budget of 1.8 billion won for the Digital Evidence Analysis System, and has secured cutting-edge equipment such as an evidence collecting and analyzing server, HDD replication and initialization equipment, and mobilized forensic equipment. The Digital Evidence Analysis System is used inter alia to analyze digital evidence through the system forensics program and log analysis program.

Fifteen notable experts, all post-doctoral specialists and veteran cyber investigators who are well-acquainted with IT and investigation technique, are set up at the Digital Evidence Analysis Center to support high-tech scientific investigation by restoring/searching, analyzing/breaking ciphers on the digital evidence procured during the process of crime investigation. Also, to prepare for modern crime, the center studies each field's technique for analyzing evidence such as system evidence analysis and network evidence analysis. It also carries out activities to standardize and propagate the evidence analysis procedure, aiming for a multi-factor development goal, in order to engage in practical investigations and academic research at the same time. Just as the National Institute of Scientific Investigation has played a central role in offline crime investigation, the Digital Evidence Analysis Center will lead scientific investigations in the future cyber age.

The KNPA will expand the Center for Digital Evidence Analysis to the front lines. To that end, the KNPA is working hard to dispatch personnel and vehicles to local agencies to gather information used in the analysis, and to provide facilities for better mobilization to police stations so that they can swiftly carry out the time-sensitive task of securing evidence at the scene.

¹⁰⁾ Other than the police, the Supreme Prosecutor's Office and the National Intelligence Service are also interested in the Digital Evidence Analysis Center and have tried to introduce it, but the police established and operated theirs first, serving as an opportunity to greatly improve the KNPA's cyber-crime investigation ability.



4. The Local Cooperation Network and Hub of Around-the-clock International Cooperation

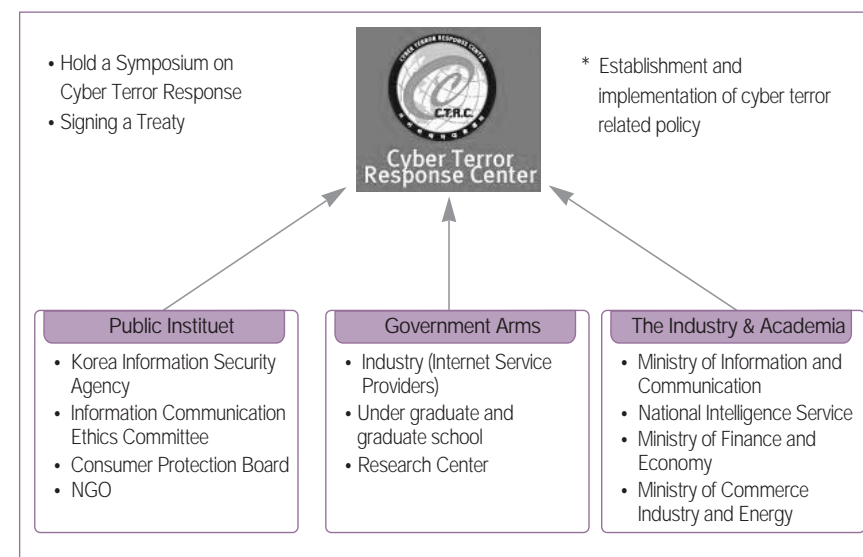
Cyber crime is none other than a war of information. Just as it is no exaggeration to conclude that the way to deal with information dictates victory in a war of information, how to share and facilitate various ideas and information related to cyber crimes inevitably constitutes one pillar of the innovative steps taken to respond to cyber crimes. Based on such awareness, the Cyber Terror Response Center has established a close network with relevant government bodies and a database on cyber crimes. These steps solidified the cooperative system against hacking and cyber terror

First, the Cyber Terror Response Center controls the cyber crime investigation network with 14 local agencies. By establishing a “security network” with 14 local agencies, the Headquarters currently holds network communications with every local agency in: Seoul, Pusan, Daegu, Incheon, Ulsan, Kyunggi, Kangwon, North & South Chungchung, North & South Cholla, North & South Kyungsang and Che-ju. The network goes far beyond a simple network of computers. It is an efficient investigation tool separated from existing “electronic payments networks” or “administrative networks” in that it can detect infiltrators and trace their origin. The system retains up-to-date technology that guarantees air-tight security from outside access for investigation without site constraints.

Second, cyber crimes can be safely subdued and controlled only when proactive and abundant cooperation from public institutions, government bureaus, industry, and academia strike a full balance.

As seen in the above picture, the Cyber Crime Response Center is in close cooperation to maximize its cyber security capabilities with public institutes, such as the Korea Information Security Agency, the Information

<Figure 4> Local Cooperation Bodies



Communication Ethics Committee, the Consumer Protection Board, and NGOs. It also works with government agencies, such as the Ministry of Information and Communication, the National Intelligence Service, the Cyber Investigation team of Supreme Public Prosecutor’s Office and with corporate research centers, universities and internet service providers.

Finally, the Cyber Terror Response Center is working as a hub of international cooperation around the clock. It gained the reputation of being the ‘most advanced cyber crime investigation’ unit, boasting cooperation with 89 countries: 43 in Europe, 13 in Africa and the Middle East, 16 in Asia and 17 in North and South America. Cooperation among investigation agencies is especially important since cyber crimes know no boundaries. In these circumstances the Cyber Terror Response Center is faring well as a hub of international cooperation in anti-cyber crime activities. The MOUs signed with Britain and France, in the late 2004 and Nov. 2005, respectively, gave more



momentum to Korea's role as the hub of international investigation cooperation.

III. Modern Anti-Cyber Crime System Development and Conquest of Problems

1. System Development

Faced with an ever-changing modus operandi of cyber crimes, the KNPA has been preparing effective measures through innovative reforms of personnel and organizational systems. It has consistently expanded its cyber crime team according to the rapid changes since they first launched the Hacker Investigation squad in 1995. And it is working on building the next generation investigation system.

The first step in anti-cyber crime activities, launching the Hacker Investigation squad, was taken to respond to hacking, which was the most damaging among various cyber crimes at that time. Crimes in cyber space, however, were unfolding in various aspects, without being confined to hacking. In addition, changes in network and growing internet usage constantly pushed criminal to adapt their techniques. Investigation methods followed. In step with these changes, the KNPA's anti-cybercrime investigation skills became more diverse and specialized, while changing its names: from Hacker Investigation squad (1995); to Computer Crime Investigation squad (1997); and to Cyber Crime Investigation squad (1999). The transformation to the Cyber Terror Response Center in 2000 brought about more development. And, while going through these changes and cases such as the "Internet

chaos" of 2003, Korea's cyber crime investigation team is finally proud of its top dog status. The history is summarized in the table below.

(Table 1) History of the KNPA's anti-cyber crime unit

Name	Organizational Command	Launch Date	Chief & Rank	Composition	Reference
Hacker Investigation squad	Director general of the Foreign Affairs Bureau	Oct. 1995	Chief of Foreign Affairs Division : Senior Superintendent	2	The first cyber crime investigation unit
Computer Crime Investigation squad	Intellectual crime division of the Criminal Investigation Bureau	Aug. 1997	Investigation Chief: Superintendent	10	Upgrade to respond to increasing computer crime
Cyber Crime Investigation squad	Intellectual crime division, Investigation Bureau	Dec. 1999	Investigation Chief: Superintendent	16	Upgrade to respond to increasing cyber crimes
Cyber Terror Response Center	Investigation Bureau	July 2000	Chief of the Center: Senior Superintendent	69	Upgrade to a national and comprehensive body against cyber crimes

(1) The First Step in Cyber-Crime Investigation: Hacker Investigation Squad (Oct. 1995 – Aug. 1997)

Cyber-crime was not a matter of great social awareness and did not draw attention from the law enforcement officers in Korea in the early 90s, when modem based on-line communications, provided by Hitel, Nowcom, and others was growing. On the 3rd of Nov, 1993, however, shocking news changed the atmosphere. An young male English hacker stole various information and data from the Korea Atomic Energy Research Institute. The incident raised the alarm about the damage that can be caused by cyber-crime. Therefore, with the awareness of the rising risk of hacking, the KNPA launched the Hacker Investigation Squad (HIS) in 1995.



In the beginning the squad was supposed to be attached to the Intellectual Crimes Investigation Section of the Investigation Division. At that time, overhaul of Investigation Bureau was called for because of the emergence of new crimes, e.g. counterfeiting using color printers and the illegal distribution of pornographic CDs. Many suggested that hacking be tackled along with the new crimes. As seen in the table, the Hacker Investigation squad was attached to the Director General of Foreign Affairs Bureau because hacking's international character was highlighted.

The squad was a small unit of two members under the Chief of the 3rd Foreign Affairs Division.

(2) Establishing the Basic Framework on Cyber Crime Investigation: the Computer Crime Investigation Squad (Aug. 1997 – Dec. 1999)

After 1997, when the squad was launched, computer-based crime skyrocketed, as more people used computers and internet usage soared. Cyber-crime naturally gained attention from the media. Law enforcement officers recognized that cyber-crime was expanding its boundaries from hacking to computer viruses, on-line fraud, and all sectors related to computers. Such enhanced awareness called for a stronger and well-prepared investigative body.

Under such circumstances, the Computer Crime Investigation Squad, a task force for the prevention and investigation of cyber crimes like hacking, manipulation of financial networks and cyber terrorism, was created and backed by Senior Superintendent K, head of the Intellectual Crime Section, and Senior Inspector Y, who headed the Anti-hacking Team. The inaugural ceremony was held at the KNPA on 4th Aug. 1997 in the presence of then-Commissioner General Hwang, Yong-ha.

The hacker Investigation squad, which was in charge of hacking and virus related crimes, was merged into the Intellectual Crime Section of the Criminal Investigation Bureau, which was in charge of "general computer crimes", e.g. on-line fraud, to create the new Computer Crime Investigation Squad.

The Computer Crime Investigation Squad warded off computer crimes around-the-clock by monitoring the usual suspects of inbound and outbound hacking, virus distribution and manipulation of network data. The squad itself also investigated the manipulation of financial networks, computer-based forgery and fabrication of bills & credit cards. With all these efforts, the investigation team, which was composed of ten computer experts, played a key role in the investigational plan and education training.

(3) The further development of cyber crime investigation: The Cyber-Crime Investigation Squad (CIS) (Dec. 1999 –July 2000)

The kinds of cyber-crime varied as internet penetration increased and IT technology progressed. Especially after 1999, the term "cyber-crime" covered broader irregularities as almost all the computers were connected to a certain network or to the internet. This change called for another reform of the role and function of "cyber-crime prevention and investigation." This was because the CIS, which was divided into the investigation team and the cooperation officer, had only one investigation team, and the cooperation officer gave help only on a strictly required basis. Furthermore, the squad had only ten full-time employees, which was too few to respond to escalating cyber crimes.

To overcome such limits, the Computer Crime Investigation Squad geared up for another leap forward through the expansion of members and budget. This led to the creation of the cyber-crime Investigation squad, backed by then Commissioner General Lee, Moo-young. The numbers of the work force



increased from ten to sixteen, although the squad had requested 25.

During the restructuring, the Computer Crime Investigation squad was expanded to Cyber Crime Investigation Squad (CIS) with the 1st Investigation Division and 2nd Investigation Division under its umbrella. The CIS was attached to the Investigation Bureau as the Criminal Investigation Bureau had been merged into the Investigation Bureau during the process. Recognizing that cyber-crime is not concentrated in a certain area, the necessity of the CIS in 14 local agencies was raised. Starting from the CIS in the Seoul Metropolitan Police Agency (Feb. 2002), the CIS in each of local agencies were organized to meet the need.

With the expansion of anti-cyber crime units across the nation, the Cyber Terror Response Center in Headquarters mainly investigated “cyber terror,” such as hacking and infiltration into national agencies. On the other hand, the Cyber Crime Investigation squads in local agencies focused their investigations on general cyber crime such as on-line fraud, libel and private information theft.

(4) The leap-forward of cyber crime investigation and the new philosophy: The Cyber Terror Response Center (July. 2000 – Present)

The perception of cyber-crime has changed. With the recognition that cyber crime might paralyze the national cyber network, people started to call for more fundamental and comprehensive strategies. An incident in January 2000 raised more fear about cyber-crimes. Major US portal sites (CNN and Yahoo) were totally paralyzed by a cyber terror attack reportedly carried out by “Mafiaboy” who was then only 15 and living in Montreal, Canada. The unprecedented Distributed Denial of Service (DDOS) attack was enough to

astonish cyber-crime experts and public servants in and outside of Korea.

The cyber terror attack caused America to be cautious about the likelihood that the aftermath of a hacker’s attack might paralyze the whole system. This changed awareness about the issue to the extent that even then President Clinton urged for the creation of a national strategy against cyber terror. As a result the US made full-fledged efforts against cyber-crime, which had been previously confined to the FBI and NIPC, on a Department of Homeland Security level.

The media coverage of the cyber terror attack also changed the notion of cyber terror and ignited a series of changes. The “Mafiaboy” incident re-emphasized the damages cyber terror can cause at home due to the Korean government’s promotion of the country’s IT industry, and also because internet usage was gaining rapidly.

“Cyber felony” was brimming in Korea. Hacking into regional broadcasting stations, Worm-virus distribution terror attacks, and the first local hacking of a cyber securities company are just a few examples of what was going on in this tense atmosphere.

The CIS, however, settled five “cyber terror type” cases in a seamless manner, even causing Prime Minister Park Tae-jun to commend the CIS for its work and promise additional budgetary support. With this support, the potential for reform was great and, subsequently, the squad began a step by step drive toward creating the Cyber Terror Response Center.

To create such a team, a request was made for a budget of 40 billion won and an additional 130 employees. Two other requests followed. The first one was to regard the cyber investigation team as a venture company not as a



common governmental body. The second one was to provide the highest level of incentives in terms of remuneration and welfare. These requests were necessary to compete with the generous compensation packages available to top IT personnel who were much in demand during the IT boom in Korea at that time.

Despite such strong request, the Cyber Crime Investigation squad had no choice but to accept a budget of just 4.4 billion won and 69 employees. This was due to the demanding approval procedure of the Ministry of Government Administration and Home Affairs, and disapproval of The Ministry of Planning and Budget. The change, albeit small, was the cornerstone of the Cyber Crime Response Center, which was launched in July 2000.

The newly launched body was different from its predecessor. It acquired independent status as an investigation center under the Investigation Bureau and its top officer would be one rank higher than before to give it more clout. The center is now a “division” level body in the KNPA hierarchy. The Cyber Crime Center hired more employees and began innovative steps. As a result, the center is now working with 80 investigation personnel dispatched from four teams. The present status of the Cyber Crime Center is as explained above.

(5) Paradigm Shift in Cyber Crime Investigation: Cyber Security Management Center (Future plan)

The KNPA has a plan to upgrade the Cyber Terror Response Center into the Cyber Security Management Center (CSMC) to launch a future-oriented cyber-crime investigation system. This is a paradigm shift in “cyber-crime investigation.” The existing Cyber Terror Response Center is an “end-of-pipe” style where one reacts only after a cyber crime is detected. The CSMC, on the

other hand, will focus on preventive measures such as getting rid of crime-causing factors and weakening the evil intention of potential criminals. The KNPA also has a plan to expand the Cyber Terror Response Center by shifting it upward in the organizational hierarchy and to spur cooperation with outside bodies to fulfill the goal of building a reliable anti-cyber-crime body which can design and enforce comprehensive measures.

2. Impediments and conquests

(1) Obstacles to improving the organization structure, budget, workforce and equipment.

Insufficient budget, workforce, and equipment emerged as major problems when the Cyber Crime Investigation squad was transformed into the Cyber Terror Response Center. Since the new center was to be a comprehensive anti-cyber crime body which would also tackle “cyber terror style” crimes, the transformation was not a matter of workforce and equipment increase but a philosophical leap-forward. Therefore, huge changes were inevitable.

The transformation into the Cyber Terror Response Center required sanctions from the Ministry of Government Administration and Home Affairs and the Ministry of Planning and Budget for organizational changes and budget approval. Contrary to expectations, it was difficult to get the approvals. Internal bickering with high ranking officials only aggravated matters. The Ministry of Planning and Budget only approved one tenth of the requested amount. On top of that, it asked for those plans to be put off until the coming year, citing a lack of funds. Despite such lukewarm responses, the leaders of the Cyber Terror Response Center were driven to make the importance of the Cyber Terror Response Center understood.



Luck was on their side. The Korean Government poured huge amounts of reserve funds to take action against a forest fire, which hit Mt. Go-sung in April, right before the general election. This was a typical case underlining how reserve funds can be fully utilized. The leaders in the Center did not let this chance pass. They were able to obtain much of the government's remaining reserve funds by showing how much more damage could be caused from a cyber attack as compared to the fire or other natural disaster. They won their battle, saw their budget increase, and were able to increase and restructure the organization.

The Cyber Terror Response Center proved its worth, despite hostility from other budget centers within the government administration. Their successes in and outside of Korea resulting from constant crime resolution, an aggressive foreign relations strategy, and studies, were rewarded with a budget increase in 2006. Mr. Y., who heads the center, testifies that the Cyber Terror Response Center of the KNPA garnered a 100% budget increase despite a belt-tightening policy which made other national agencies lose 7% of their budget on average. Such a dramatic budget increase was possible because the Ministry of Planning and Budget had faith in the Center, which had been reporting its achievements and demonstrating the value of the expenditure.

(2) Difficulties in Technology Accumulation

Investigation methods tend to be used over a long period of time. Some conventional methods, such as using fingerprints and blood samples, are highly likely to remain valuable in the future. On the other hand, cyber-crime investigation methods are unique in that technology accumulation is tricky. IT or Web-engineering technologies are advancing even at this moment. As a result we often see newly developed cyber-crime investigation methods suddenly become outdated and useless. Without a constant upgrade of new

technologies and investigation methods, cyber-crime investigators cannot outsmart criminals because such nimble technological changes make technology accumulation nearly impossible. Current "cyber cops" know they will lose track of the cyber-crimes if they lose focus even for a short period of time. Constant investment and the provision of continuous education and skills upgrading for the staff is imperative.

Currently, the main focus is only put on securing talented resources and not on providing enough training and education for existing members. Progress in private sector improvements of the cyber infrastructure and expansion of the "cyber culture" do not guarantee progress in cyber-crime investigation. This shows that the infrastructure for cyber-crime investigation is still inadequate as compared to other cyber-infrastructure. Hence the police have struggled to develop and expand programs, training, and research methods for cyber-crime investigation on their own.

Facing these challenges, the police invested more budgetary and personnel resources to expand the cyber infrastructure and have tied to cooperate more with the private sector. However few ways there may be to learn tips on cyber-crime investigation, the private sector in Korea is equipped with an abundant infrastructure to help resolve basic online problems.

This environment triggered an invisible rivalry among cyber cops. Personal development became a race for prestige and seniority. It is remarkable that such competition contributed to the progress of the organization, with many of the members being specially promoted on a merit basis. This is all the more noteworthy since 78-80% of the cyber cops got specially promoted in two or three years on a merit basis, while only 10% of special promotions were given to other police officers in a year, and is a testament to their efforts to learn new investigation technologies.



III. Achievements of the High-tech Cyber-Crime Response System.

With an inadequate budget and organizational structure, and too few personnel, the Cyber Terror Response Center strived to be reborn as a small but strong organization. As a result of such tactics, it has been a reliable guardian of cyber space, which was not previously possible even with an enormous budget and workforce.

1. International achievement- Resolving the 'Brazil Hacker' case

Brazil is notorious as a hot bed of computer hacking and cyber-crimes. According to the BBC's report on Sept. 14, 2004, eight out of ten hackers in the world are Brazil-based. It is also reported that internet financial fraud in Brazil does more financial damage than bank robbers, and two thirds of the worldwide child pornography sites stem from Brazil. Brazil is called the heaven of hacking as hacking itself does not constitute any crime in the country. Consequently, many international hacking groups make their home in Brazil. One of them, called CYBERLORDS, was the culprit in the so called 'Brazil Hacker' case, where 1,032 web sites, including 58 sites in Korea, China, Japan, Indonesia, Brazil were hacked. Those hackers attacked weaknesses in the Window's operating system and manipulated homepages. They used "Proxy servers" to avoid connector tracing and crime analysis, using remote computer servers in remote places such as the United States or European countries as intermediate points.

Facing this challenge, the Cyber Terror Response Center developed a dedicated program for cyber crime investigation and cooperated with its

Japanese counterpart to successfully bring the hacking ring down after six months.

This remarkable accomplishment drew international attention. An American cyber cop, in a private conversation, described the accomplishment as a miracle, pointing out that even the US failed to root out the ring despite better financial, legal, and system-related resources.

2. Thorough Investigation into Hacking Damage at State-run Institutes

A group of Chinese hackers infiltrated key Korean networks in June 2004. They attacked 222 computers in more than ten of Korea's key research institutes and governing bodies, such as the National Assembly. Later 79 additional victims were found in the private sector, increasing the total number to 301. The Korean Government paid much attention to this case for the sake of national security because it was tantamount to "cyber war" given the prominence of the main targets.

The investigation of this case started when a Korean researcher reported that he got a camouflaged e-mail written by an unidentified man who stole the e-mail account of a Korean man working for a military supplier. The center found out that information stored in a PC can be remote-controlled because the Trojan horse virus is automatically installed when opening the attached file. After tracking the hackers, the center also found out that the Back-Door in question is a mutated "Peep," similar to the one that overwhelmed Taiwan in early 2004, whose function is to enable the remote control of available data. Through this hacking technique, the hackers deflected the infiltration blocking system using TCP 80, a port used at the moment of connection, and



successfully stole the data by inducing trackers to go to a remote intermediate point.

The Cyber Terror Response Center created a joint investigation team with related government bodies after the case. The newly created team came up with the correct analysis on the status and security measures, and distributed a “back-door vaccine” they had created. As a next step, they promptly restored the damaged systems, investigated the leaked classified information, and blocked the access to the intermediate point.

Finally, the joint investigation team detected that the connecting point was in China and asked for cooperation from the Chinese government via Korea’s Ministry of Foreign Affairs and Trade. After the investigation, the culprits were found to be hackers belonging to the People’s Liberation Army.

3. Clean and fair elections through controlling election irregularities

Many election irregularities occurred due to the increase in number of Internet users and diversified participation in politics through the Internet. The Internet was used as an important method of election campaigning in local elections (6.13), educational committee election (7.11) and the National Assembly and by-elections (8.8) in 2002. Moreover, after realizing the significance of netizens in the 16th presidential election, candidates and voters actively used the internet in subsequent election campaigns. Especially in during the 17th National Assembly election (April 15, 2004), the number of cyber election irregularities showed a rapid increase. Pre-election campaigning such as leaving feedback online, slandering opposition candidates, or supporting specific candidates were the most common form of the cyber

election irregularities.

In response to these activities, the Cyber Terror Response Center prepared a 24-hour surveillance structure for the web sites. Also a 24-hour surveillance system was constructed by committing 600 cyber surveillance agents in order to block illegal election campaigning on the Internet. At the same time, 112 centers were set up to quickly arrest anyone involved with election irregularities using PC cafes. As a result, 1066 cases were uncovered and 1152 people, accounting for 20.8% of the total 5548 election irregularities, were arrested for cyber election irregularities during the election. Also 3000 web sites that were related to parties and candidates were under surveillance for 24-hours in order to regulate false reporting on candidates. This contributed to a cleaner and fairer election atmosphere and cyber election culture.

4. Securing the safety of the internet through solving cases and consistent academic research

Other than the facts mentioned above, the cyber terror response center secured the safety of the internet by solving numerous types of cases. The details are as follows:

- Apprehension of 30 domestic Commercial communication network Hackers (1997, August)
- Apprehension of members of CVC, the biggest domestic computer virus producer (1998, February)
- Apprehension of suspects who hacked into the KAIST network and leaked confidential data regarding “Woori byul” (1999, March)
- Apprehension of suspects who produced a worm virus for the purpose of cyber terror (2000, February)



- Apprehension of international cyber gambler worth 90 billion dollars (2002, July)
- Apprehension of 13 members of biggest domestic hacking group who hacked into about 80 government-related web sites.

In addition, the Cyber Terror Response Center participated actively in academic research and public relations to increase awareness of the dangers of cyber terrorism. A typical example was The Cyber terror response symposium that was held on October 13, 2005.

IV. Primary success factors for construction of the cyber crime response system.

There are many factors that contributed to the construction of the advanced Cyber Terror Response Center. However, the following aspects stand out.

1. Development of Korea's IT industry and employing its best talent

The human resources at the KNPA dedicated to this job are the key success factor. Due to the characteristics of cyber-crime, investigation required IT experts and people with expertise in general investigative methods.

A number of schemes to secure such talented people were suggested in order to react quickly to the demand of the labor force during the take off stage from cyber-crime investigation to the Cyber Terror Response Center. The first option was to educate prior investigators on new IT technologies. The

second option was to educate IT experts about criminal law. Third, was to implement special appointments by employing a hybrid team of IT experts and seasoned investigators. By selecting the third scheme, it was possible to invest efficiently in education as well as garner significant synergy effects. It was also possible to put together the team in a short time.

This solution was possible due to the development of the IT industry. For four years, from 1997 to 2001, the government invested 2.15 billion dollars in supporting Korea's IT venture industry, which resulted in an increase in the number of IT enterprises from 9,397 in 1997 to 17,719 in 2001. Especially in 2001, 44.5% was IT-related. That is equivalent to approximately 5,073 among the total venture industry. Also, the employees who worked for the IT venture industry increased almost 3 times from 77,720 in 1999 to 229,401 in 2001.

Therefore the necessary talent could be attracted due to the development of the IT industry in Korea and the KNPA could use these competent and creative IT experts. Since the procedure of selecting these elites was very strict, only experts who had experience in IT related fields for over two years or those who possessed a certification of qualification in safeguarding information, or knew how to operate UNIX, NETWORK, or security related issues were admitted. It was also helpful that Koreans tend to prefer jobs in government or public organizations due to career stability. According to a survey, becoming a "cyber cop" is now seen as a prestige career route to take within the organization.

The Cyber Terror Response Center also implemented a strategy to centralize education for this elite force. The focal point was to concentrate on educating them so that they could be re-located to local districts. Korean governance has recently trended toward decentralization but, in this case, due to the fast developing technologies, it was more appropriate to educate



personnel centrally.

IT and engineering technologies are improving day by day. The degree of integration is doubling every 18 months and, recently, the development cycle for IT products has been shortened to 12 months. In case of Samsung Electronics, it developed 256MB NAND flash memory in 1999. Since then, it created 512MB in 2000, 1GB in 2001, 2GB in 2002 and 4GB in 2003.. As for communication technologies, the bandwidth of fiber optics is increasing three times as fast as before and as a result the speed of internet communication is becoming faster and the size of information storage is getting bigger. Moreover, mobile broadband service is being rapidly deployed, so it is suggested that 4th generation broadband services and Wireless Mobile Broadband Service will be the mainstream in the coming years, outpacing the 3rd generation broadband service, "IMT2000".

In order to respond to these fast changing technologies, the centralization of education is far more efficient and economical than the decentralization. This maximizes the decentralized educational system consistently updates technologies by educating the staff at the Police Headquarters and re-locating them to local districts. The reason that this type of strategy could be successful was due to the from great connectivity and interaction between Police Headquarters and local district headquarters.

2. Futuristic leadership and the enthusiasm of the members

In order to actively and positively adapt to a new environment which is changing endlessly, you need leaders who understand those changes, can predict the future with keen insight, and develop essential technologies.

The Police had already begun preparing for the impact that cyber terrorism

would have on society even when cyber crime was not a serious issue. According to a high-ranking official, the experience of staying in foreign countries as a resident officer helped to predict the problems of the cyber terror. This opportunity to experience the communication technologies and informatization of other countries made the officer realize the importance of cyber safety and the seriousness cyber terror attacks. This consciousness became a foundation for future cyber-crime investigations.

Problems become serious when the foundational structures of society are compromised in densely populated areas. Disturbances, crimes, and riots are likely to occur when key infrastructure, such as transportation, communication and energy, become paralyzed due to hacking. Especially in Korea, it is easy for cyber crimes to circulate due to the existence of a complex housing system, such as the reliance on apartments. At the same time, this type of housing structure can also respond to cyber-crime easily by connection through the network. This kind of infrastructure can be easily affected by cyber terror in the presence of advanced IT.

Considering this, Police Headquarters concentrated on developing a cyber-crime response structure that most suits the circumstances in Korea. That required forward looking leaders who could respond to the serious consequences of cyber terror. Absent that, and the present cyber-crime response system would not exist.

Leaders also needed a technological mindset. One mid-ranking official, who was also the cooperation team leader, was a member of the domestic cyber-crime investigation team. Almost all the cases that were reported in the media were due to his efforts and he is unrivaled in this department. Through precise analysis, he proved that international hackers hacked into 11,222 institutions in 95 countries via imitated servers in Korea. The present cyber terror response



center exists because he became a model to the members of the cyber terror response center for his tenacity, reasoning, and passion.¹¹⁾

There was also good cooperation from a high authority who supported and understood the role of the police and stood behind professional mid-rank officials in order to confront cyber-crime. Fortunately, high-ranking officials at the Police Headquarters, with ability to quickly respond to altered circumstances, supported changing the organizational structure, man power, and functions according to the types of crimes in order to create the best cyber-crime investigation system possible.

However, a more important factor than the leadership is the passion and active participation from the members. If the members do not follow the leader, the project will collapse. Fortunately the members of the Cyber Terror Response Center were selected through close examination and a long period of verification and they all worked hard to develop themselves after being hired. It is very significant to notice that this effort to improve their abilities and educate themselves by holding self-seminars was all voluntary. As a result of this effort, experimental investigation methods, such as remote investigations were possible.

3. Investigation strategy using central control

Among the factors that brought success to the cyber crime investigation team was the centralized investigation strategy. In the case of cyber-crime, jurisdiction and technological problems can easily arise. However, they can be

resolved if things are centralized in Police headquarters where superior technologies are located. What made this strategy possible was the cyber investigation network. This is only possible within national police structure with practical work experiences and technologies.

The cyber investigation network is based on what has been called the Virtual Private Network, which is a secure system of communication that connects the center with the remote sites. It is secure, but nonetheless uses the public network, which means that many different districts can access it and exchange information and contacts with the Police headquarters and other local district. There are some problems with the system, because it is based on older technologies. For example, signaling speed and the necessary bandwidth may not be secured. That necessitates encryption and electronic authentication, and this may require certain personnel who can handle that task on a regular basis. At present, Police headquarters is utilizing the cyber investigation network under the maximized security through encryption and electronic authentication.

The synergy effect of investigation strategy using central control can be seen by combining this network with a police supporting system, such as the C3 system. The C3 system refers to command, control, and communication. The patrol unit needs to arrive at the crime scene in a short time and quickly deliver accurate information back to the center. In order to execute the investigation efficiently, the cyber investigation network needs to be connected to the C3 system. The unification by centralization strategy makes this possible, and is another reason why the KNPA's cyber investigation has been so successful.

¹¹⁾ As a result of this effort, he was elected unanimously as a vice-president of Interpol's Asia-Pacific Cyber-Crime Consortium.



4. The principle of equality and mutual strategic organization culture

The structure of police forces, which are completely different from other organizations, is such that generalists rather than specialists are preferred. Also, police forces are more familiar with the rank distinction principle rather than the principle of equality. This rank distinction principle is understood as being indispensable in order to respond to crimes quickly and efficiently. However, CTRS tries to maintain the principle of equality. It also focuses on expertise rather than hierarchy as the CTRS members are from younger generations and the cyber business itself has special and professional traits.

That structure is hard to set up in Korea, and some members of the cyber terror response center had difficulty adjusting to the lack of hierarchy. On the other hand, the ones who are engaged in the IT field, tend to work without authoritarian or obsolete ways of thinking. Therefore, the Cyber-Crime Response Center cultivated an environment in which the young technical stars could work in harmony with the older, more experienced investigators. Of course, this new culture incurred conflicts and problems with other departments. However, in the end, cooperation and understanding was possible by focusing on the strategic investment that was being made.

Many conflicts arose because of the differing backgrounds. But they developed a cooperative culture where members understand and cooperate with one another through the principle of reciprocity and professionalism. The structure also depended on their strong will to upgrade their skills and be curious enough about the others to learn from them as well.

5. Site appointments and consistent investment on education

In order to continue to respond to the evermore sophisticated instances of cyber-crime and cyber terror, it is not necessary to explain that professionalism in the field is a must. Sometimes an officer is sent out into the field for lengthy periods of time, but that opens the possibility for improper relationships with civilians. For these reasons, the organizational culture of long-service site appointment was settled down along with the experts in this field.

Non-Koreans may not be able to understand the fact that long service in the field of cyber crime investigation is a factor for successes because long service in the field of cyber-crime has been taken for granted. On the other hand, it is worth noticing that long service in the field of cyber crime investigation can be differentiated from the long service for the continuation of business. The core point of the differentiation is a steady investment in education in order to acquire professionalism.

Privately commissioned educational training is currently being carried out at the cyber-crime investigation center in order to maintain the abilities of cyber-crime investigators at maximum levels. 30 to 50 investigators receive intensive reeducation frequently. The subjects are diverse, but the focus is on professionalism and practical skills upgrades. There are 16 courses and the duration of the program is between 4 to 6 months. In order to maximize its effect, participants are asked to focus on the course and nothing else. Police headquarters is trying to secure a budget which can educate 200 to 300 people every year.

In addition to the education program, the cyber terror response system is doing its best to exchange information and develop its own core technologies. The technical support team, which consists of 12 members, is maximizing its professionalism by engaging in problem solving seminars on a weekly basis.



By actively participating in seminars and sharing their research and data, they find new avenues to create new information. There is no similar process elsewhere in the KNPA. And, this academic research is not limited to the domestic arena. Much is also accomplished in the international sphere. And in these sessions, the principle of equality among the members is most noticeably in effect. It works for a smooth transaction of opinions and enables extracurricular activities. This creates a synergy effect that makes the present cyber crime investigation structure possible.

VI. Lessons

As seen above, the KNPA is now equipped with world class cyber-crime investigation skills. These are reflected in its prompt reaction to the rapidly changing needs of the digital age. Behind these top-tier investigation skills was the KNPA's new slogan, "Reform is the only way to survive." KNPA wisely overcame obstacles and fully utilized whatever support it could garner during its reform drives. Without any complacency, the KNPA and its anti-cyber-crime team are making constant efforts to assure world-class cyberspace security.

To establish a next-generation cyber crime investigation system is necessary to successfully achieve this goal. To that end, the KNPA plans to expand the current Cyber Terror Response Center to the Cyber Terror Correspondence Center; create task forces for each category of cyber-crime; and, provide specialized and distinguished security services by intensively fostering new policy, strategy and digital evidence analysis sectors. A stepped-up recruitment plan will accompany those goals: an additional 65-80 investigators will be employed, and five doctoral researchers, whose job it will be to

permanently focus on research, will be recruited.

Next, laws and regulations related to cyber-crimes should be amended. The goal is to maintain cyber policies that can satisfy the people and assure national cyber security in the long term by keeping consistent and well-planned policies. Ideal circumstances for cyber-crime prevention, investigation, and consultation can be fostered as long as scientific policies are the target of the efforts to amend the law.

In addition, the cooperative networks inside and outside of Korea should be reinforced. It is necessary to maximize the capacity to respond to cooperative investigations and to assure a solid reputation as the leader of cyber-crime investigation by establishing a cooperative network. To this end, the dispatch of cooperation officers should be expanded not only to international organizations like Interpol, but also to local entities related to cyber-crime investigation. The importance of this can be seen in the fact that the current number of cases Korea deals with on an cooperative basis internationally exceeds 100.

The best quality cyber security service will be provided when next-generation cyber-crime investigation systems are established, when laws and regulations on cyber-crimes are amended, and when cooperative networks inside and outside of Korea are reinforced.

Dynamics of Government Innovation and Decentralization in Korea

COMPETENT GOVERNMENT

Date of issue	December 31, 2005
Publisher	Presidential Committee on Government Innovation and Decentralization
Address	Simunro 1-ga, Jongro-Gu, Seoul 110-786, Korea
TEL / FAX	82-2-3703-6500 / 82-2-3703-6576
Homepage	www.innovation.go.kr
Edit & Print	HYUNDAI MOONHWA Co.
Design	SUS4 Co.