INTERNATIONAL TELECOMMUNICATION UNION

ITU WORKSHOP ON CREATING TRUST IN CRITICAL NETWORK INFRASTRUCTURES

Document: CNI/05

20 May 2002

Seoul, Republic of Korea — 20 - 22 May 2002

CREATING TRUST IN CRITICAL NETWORK INFRASTRUCTURES:

KOREAN CASE STUDY

This case study has been prepared by Dr. Chaeho Lim <chlim@if.kaist.ac.kr>. Dr Cho is Visiting Professor at the Korean Institute of Advanced Science & Technology, in the Infosec Education and Hacking, Virus Research Centre. This case study, *Creating Trust in Critical Network Infrastructures: Korean Case Study*, is part of a series of Telecommunication Case Studies produced under the New Initiatives programme of the Office of the Secretary General of the International Telecommunication Union (ITU). Other country case studies on Critical Network Infrastructures can be found at <http://www.itu.int/cni>. The opinions expressed in this study are those of the author and do not necessarily reflect the views of the International Telecommunication Union, its membership or the Korean Government. The author wishes to acknowledge Mr Chinyong Chong <chinyong.chong@itu.int> of the Strategy and Policy Unit of ITU for contributions to the paper. The paper has been edited by the ITU secretariat. The author gratefully acknowledges the generous assistance of all those who have contributed information for this report. In particular, thanks are due to staff of Ministry of Information and Communication and Korean Information Security Agency for their help and suggestions.

TABLE OF CONTENTS

Executive summary

In the modern era, all major infrastructures, such as financial, energy, e-government, military defence, health care, transportation and telecommunication use information technology (IT) and networks. Like other countries, Korea has been upgrading its IT and network capabilities to similar levels to those of other advanced countries.

However, international attacks on these crucial networks, such as the "worm" attacks Code Red and Nimda which took place in 2001, have shown that unauthorized network intrusion can potentially have a huge impact on the whole country, as well as the damage they can inflict on these infrastructures in particular. Where individual networks are connected to public networks such as the Internet, it is clear that the social and economic impacts of such attacks stand to be extremely costly.

In Korea, the telecommunication network has already suffered from Internet-borne attacks, including intrusion and worm viruses. And while the Korean Internet ranks extremely high technologically on a global level, offering very fast communication facilities, intrusions have still occurred.

The problem has led the Korean Ministry of Information and Communication (MIC) to process and pass the "Information and Telecommunication Infrastructure Protection Act". By this law:

- The government can determine what constitutes critical infrastructure, even in commercial networks;
- That infrastructure which is defined as critical should apply strict security principles and should evaluate the potential vulnerabilities;
- If the critical infrastructure is attacked, it should be reported to the law enforcement agencies, or to KISA (Korea Information Security Agency) or ETRI (Electronics and Telecommunications Research Institute);
- Special security companies can be assigned by the government to evaluate the critical infrastructure site;
- ISAC (Information Sharing and Analysis Centre) and ISMS (Information Security Management Systems) are covered by this law.

This case study assesses current threats to network security in Korea and describes current measures taken for the protection of national critical network infrastructures and how these can be defined. Due attention is also given to the importance of regional and international coordination, because sharing attack information may, in many instances, be the first warning of threats to the critical infrastructure. The dynamic nature of hacking and virus worm attacks, and their growing sophistication, mean that ongoing coordination of this nature needs to be developed in parallel to national protection initiatives. Finally, some areas for further study and actions to meet future needs are proposed.

1. Introduction

1.1 The year 2000 can be seen as the start of a new era for information technology in Korea, as it is the year when high-speed Internet services began to spread. The major broadband Internet service providers (ISPs) in Korea are Korea Telecom and Hanaro Telecom (which use asynchronous digital subscriber line technology, or ADSL), Thrunet and Dreamline (which use cable modems), and other private ISPs (which use Internet via satellite, fixed wireless and other technologies). By the end of 2000, the number of users who subscribed to Internet service providers had reached over 4 million, indicating that over 30 per cent of the nation's households have access to high-speed Internet. The expansion of the high-speed network infrastructure enables subscribers to view multimedia contents, setting Korea on the path towards becoming a real information powerhouse. This trend towards greater connectivity and more converged multimedia services, is likely to continue, as the government is forging ahead with a policy to connect at least 90 per cent of the nation's population to the Internet.

1.2 Another striking feature of IT in Korea is that the number of domestic wireless Internet subscribers increased from 2.57 million in February 2000 to 19.01 million in April 2001, or a sevenfold growth. The wireless Internet industry was evaluated as one of the most robust industries in 2000. Since pay-per-view content is possible over the wireless Internet, it could become a profitable new business model.

1.3 In line with this, the year 2000 was a milestone for Korea's effort to enhance security. In December 2000, Acts on the protection of major IT infrastructures from cyber-terrorism were passed. A set of information protection guidelines for IT services was established for raising the awareness of data protection among businesspeople. A regulation was added to the "*Acts on Promotion of information & Telecommunications Network Use*" and was passed to contain the spread of computer viruses. Moreover, a hacking and virus prevention support centre was established to strengthen the virus alert system. Also, by enhancing the support for Consortium of Computer Emergency Response Teams (CONCERT), the government is planning to strengthen information exchanges for hacking attacks and viruses in cooperation with Asian countries such as Japan and China, and to participate actively in the activities of Forum of Incident Response and Security Teams (FIRST).

1.1 Structure of the report

1.4 Following this introductory section, this paper will look into Korea's experience with critical network infrastructures protection as follows:

- In Chapter two, the overall Korean environment is illustrated;
- In Chapter three, the network infrastructures are described through an overview of the Korean telecommunication service market and Internet infrastructure. This section reviews the criteria used to decide which network is "critical" and should thus be treated as such.
- In Chapter four, the report looks at various types of threats to the network infrastructures and their impact on socio-economic life.
- In Chapter five, Korea's approach to the problem is examined. In this chapter, the organization of activities to prevent, detect and respond to potential attacks is described.
- Finally, in Chapter six, future developments in this area will be explored.

2. The Korean environment

2.1 Korea's geographical layout

2.1 Korea is situated on the Korean Peninsula, which spans 1,100 kilometers north to south. The Korean Peninsula lies on the north-eastern section of the Asian continent, where the western-most parts of the Pacific join Korean waters. The peninsula shares its northern border with China and Russia. In addition to the mainland peninsula, Korea includes some 3,000 islands.

2.2 Korea encompasses a total of 222,154 square kilometers—almost the same size as Britain or Romania. Some 45 per cent of this area, or 99,000 square kilometers, is considered cultivatable area, excluding reclaimed land areas. Mountainous terrain accounts for some two-thirds of the territory. The Taebaeksan range runs the full length of the east coast. The western and southern slopes are rather gentle, forming plains and many offshore islands.

2.2 The Korean economy

2.3 Korea recently pulled through the economic storm of the Asian financial crisis that began in late-1997. This crisis, which rocked markets all across Asia, had until recently threatened Korea's economic achievements. However, thanks to the implementation of an International Monetary Fund (IMF) agreement, the strong resolve for reform of the government of Kim Dae-jung, and successful negotiation of foreign debt restructuring with creditor banks, the nation is currently on track to resume economic growth. Since the onset of the crisis, Korea has been rapidly integrating itself into the world economy. The goal of the nation is to overcome problems rooted in the past by creating an economic structure suitable for an advanced economy.

2.4 Korea, once one of the world's poorest agrarian societies, has undertaken economic development in earnest since 1962. In less than four decades, it achieved what has become known as the "economic miracle on the Hangang River", a reference to the river that runs through Seoul—an incredible process that dramatically transformed the Korean economy, while marking a turning point in Korea's history.

2.5 An outward-oriented economic development strategy, which used exports as the engine of growth, contributed greatly to the radical economic transformation of Korea. Based on such a strategy, many successful development programmes were implemented. As a result, from 1962 to 1997, Korea's gross national income (GNI) increased from USD 2.3 billion to USD 474 billion, with its per capita GNI soaring from USD 87 to about USD 10,307. These impressive figures clearly indicate the magnitude of success that these economic programmes have brought about. GNI and per capita GNI drastically dropped to USD 317 billion and USD 6,823 respectively in 1998 due to the fluctuation in foreign exchange rates, but these figures returned to the pre-economic crisis level in 2000.

2.6 Korean imports have steadily grown thanks to the nation's liberalization policy and increasing per capita income levels. As one of the largest import markets in the world, the volume of Korea's imports exceeded those of China in 1995, and was comparable to the imports of Malaysia, Indonesia, and the Philippines combined. Major import items included industrial raw materials such as crude oil and natural minerals, general consumer products, foodstuffs and goods such as machinery, electronic equipment and transportation equipment.

2.7 Korea's rapid development since the 1960s has bee fuelled by high savings and investment rates, and a strong emphasis on education. The Republic of Korea became the 29th member country of the Organization for Economic Cooperation and Development (OECD) in 1996.

2.8 With a history as one of the fastest growing economies in the world, Korea is working to become the focal point of a powerful Asian economic bloc during the 21st century. The North-east Asia region commands a superior pool of essential resources that are the necessary ingredients for economic development. These include a population of 1.5 billion people, abundant natural resources, and large-scale consumer markets.

2.9 The employment structure of Korea has undergone a noticeable transformation since the dawn of industrialization in the early 1960s. In 1960, workers engaged in the agricultural, forestry and fishery sectors accounted for 63 per cent of the total labor force. However, this figure dropped to a mere 11.6 per cent by 1999. By contrast, the weight of the tertiary industry (service sectors) has gone up from 28.3 per cent of the total labour force in 1960 to 68.6 per cent in 1999.

3. Telecommunication network and services in Korea

3.1 Facilities-based telecommunication services

3.1.1 Domestic telecommunication services

3.1 The Korean Government fully recognizes that the establishment of fixed telephone facilities is a means of satisfying the most fundamental communication demands and that, at the same time, the basic infrastructure can provide a wide variety of telecommunication services. Since the 1980s, the government has pursued the development of telecommunication services in preparation for early realization of an information society as well as expansion and modernization of telecommunication facilities. Under these circumstances, more than one million telephone lines have been rolled out every year since 1982. As a result of this effort, there were more than 10 million lines by 1987, ushering in the *one telephone per family* era. The government has been expanding infrastructure continuously with the help of the successful development of a domestic electronic exchange.

3.2 Accordingly, Korea has grown rapidly. Between 1990 and 2000, Korea's total teledensity (fixed lines plus mobile subscribers) rose from 31.1 to 103.1, ranking Korea 27th in the world[1]. The Korean financial crisis had resulted in a drastic reduction in the number of new subscribers. In 1998, the number of subscribers actually fell by 210 thousand. With the revitalization of the economy, there were 22.7 million fixed lines and 29.0 million mobile subscribers as of the end of 2001. As for the domestically developed TDX exchange, there were 12.437 million lines installed at the end of 2000, representing a 51 per cent share of overall exchange facilities usage.

[1] Data from *ITU World Telecommunication Development Report 2002: Reinventing Telecoms,* available at www.itu.int/ti.

3.1.2 International telecommunication service

3.3 International telephone service is available all across the world including the remotest parts of the Sin Po region (water canal construction area) in the North. The number of minutes in outgoing international call in 200- was 1.02 billion, representing an increase of 14 per cent per year since 1995. However, with fewer than 50 minutes of international calls per subscriber, Korea has one of the lowest levels of international calling in the OECD (only Japan is lower)[2] 550 million minutes in 2000 an increase of 12.6 per cent over the previous year.

3.4 The majority of international leased lines are digital lines (above 56/64k) that can handle international voice calls, fax, and data simultaneously. The increased usage of leased lines by service providers has prompted the supply of high-speed Internet services, ranging from 45 to 155 Mbit/s. Three companies (Korea Telecom, Dacom, ONSE Telecom) previously shared the market for international leased line service. In 2001, seven additional companies have entered the market. Various international submarine cable operators (AGC, Level-3, Flag, WorldCom, Concert, Global-One, Equant, KDD, SingTel) are also participating in the market. As a result, this should create strong competition in the international leased line service market. From 2001 to the beginning of 2002, other additional national and international communication companies, in addition to Korea Telecom, have received construction rights for laying down submarine cable lines for international routes, thereby intensifying competition in service costs.

3.1.3 Wireless telecommunication service

3.5 From only 2,658 cellular subscribers in 1984, the number of subscribers has subsequently grown rapidly. In 1990, there were 80,005 mobile subscribers, 1,6 million subscribers in 1995 and by the end of December 2001, the number of subscribers had grown to 29.04 million mobile users, or representing 60.8 subscribers for every 100 inhabitants. The proportion of cellular phone subscribers held by the various service providers at the end of 2000 was SK Telecom (40.8 per cent of total subscribers), KT FreeTel has (19.8 per cent) LG Telecom (14.6 per cent) Shinsegi Telecom (13.2 per cent) and KTM.com (11.8 per cent). Since September of 1999, the number of cellphone subscribers has exceeded fixed telephone subscribers, and this trend will continue.

3.6 In September of 1999, the cellphone companies turned their energies toward providing wireless Internet service through mobile phones using IS-95B and CDMA 2000 1x technology. The number of wireless Internet subscribers in the nation has been rapidly increasing from 2.58 million at the end of February 2000 to 19.01 million at the end of April 2001. As the high growth in the wireless Internet market continues, the trend of competitiveness in the cellphone market will shift from competition in networks to competition in solutions and content. In the near future, wireless Internet service delivered via cellphones will expand into the areas of wireless e-Transactions, such as stock and bank transactions, and cyber shopping. Therefore, cellphone companies have aggressively pursued strategic relationships with Internet providers to develop effective and useful content.

3.7 Three companies (Airmedia, Intec Telecom and Hanse Telecom) acquired the rights to offer wireless data services. Early wireless data service was mainly aimed at the business market, but with the bull market in September 1998, Airmedia began providing interactive stock market service to the general public, resulting in the rapid growth in sales and subscribers. The added convenience of being able to conduct stock market transactions anywhere and 50 per cent lower transaction fees led to greater popularity in wireless data services. However, the market and growth prospects of the wireless data market remain limited, showing 57,038 subscribers at the end of 1999 with an increase to 73,842 by December 2000. The future success of the wireless data market will depend on the ability to differentiate wireless Internet data services through cellphones.

3.8 Third-generation mobile services, or IMT-2000 (International Mobile Telecommunication 2000), promise multimedia services that integrate voice, data and images in various environments, including wired and wireless services, through the use of a personal terminal and user card. In 2001, three IMT-2000 providers were selected to provide high-speed mobile services in the near future. IMT-2000 service can be categorized into multimedia service, wired and wireless integrated services, and global roaming service.

[2] Source: ITU World Telecommunication Indicators Database, available at: www.itu.int/ti.

IMT-2000 enables the transmission and receiving of all kinds of information anytime, anywhere in the world with one terminal. To improve global roaming service, the world's information communication industry is in cooperation with setting standardization levels for IMT-2000 and developing its equipment.

3.2 Non-facilities-based telecommunication service providers

3.2.1 Specially designated telecommunication services

3.9 Specially designated telecommunication services are divided into three different kinds of providers:

- voice resale and Internet phone service through transmitting equipment.
- call convergence, re-billing service, and wireless resale service, without acquiring transmitting equipment.
- telecommunication service using specially-constructed telecommunication facilities.

Specially designated telecommunication services began operation in January 1998. In that year alone, 180 companies registered as special service providers. Since then, the number of new companies participating in the market has slowed down, reaching 268 companies as of March 2001. The majority of the early specially designated telecommunication service providers have experienced rapid growth by entering the international call market through a voice resale service and Internet phone service. The market for special services has expanded dramatically being worth 248.7 billion won in 1999 to 792.3 billion won in 2000.

3.2.2 Value-added telecommunication services

3.10 According to Article 4 of the Telecommunications Business Act, value-added telecommunication service combines computer functions with the basic transmitting function of telecommunication. Value-added service providers provide telecommunication services, excluding designated basic telecommunications services, that include PC communication, computer reservations, telephone mail box service, Internet, electronic mail, EDI and credit card request by renting telecommunication network facilities from facilities-based service providers.

3.11 Domestic value-added telecommunication services have maintained higher growth rates due to the expansion of existing markets and the development of new business areas, creating a favourable environment for the entry of additional value-added service providers. As of the end of 2000, there was a five-fold increase over 1996 with 2,885 value-added telecommunication service providers present in the market. This rapid growth was due to government support in promoting the industry, innovative and effective management, large-scale information systems in larger companies, and greater public awareness of information technologies in our society. The majority of value-added telecommunication service providers are running integrated systems that provide more than two services. Korea Telecom and Dacom are leading providers in this industry, while ISPs are gaining more ground due to the increased number of Internet users. The value-added telecommunication service market accomplished gross sales exceeding approximately one trillion won in 1998, and reached 2.533 trillion won in 2000, achieving an average annual growth rate of 32.8 per cent. Its gross sales are predicted to be 6.3 trillion won in 2004 due to the increasing number of Internet users, electronic transactions and the great demand for high-speed networks.

3.2.3 Internet connection services

3.12 The population of Internet users has been increasing tremendously, from 3.1 million in 1998 to 24.12 million at the end of September 2001. The first commercial Internet connection service was launched in 1994. There were 36,644 Internet hosts in 1995, rising to 440,000 as of 2001. There were only 11 Internet service providers and related businesses in 1994. This grew to 83 by 2000. The Internet market has been growing at full speed due to the remarkable developments in IT technology, huge increase of e-Trade, acceleration of small-office-home-office (SOHO) and the IP industry. Now, ISPs have a new concept of business that goes beyond simply connecting to the Internet. By putting forth their best efforts to provide additional services to draw customers, they also focus on outsourcing that is designed to consign and manage additional services. The rate of growth of the Internet market has averaged 184 per cent annually and continues to grow rapidly.

3.3 Internet infrastructures in Korea

3.3.1 Internet eXchange (IX)

3.13 Domestic IXs are operated by NCA (KINX), KT (KT-IX), Dacom (DACOM-IX) and Korea Internet Neutral eXchange (KINX). The nonprofit public networks peer via KIX while commercial ISPs peer via KINX, KT-IX, and DACOM-IX.

3.3.2 Internet backbone network

3.14 Currently, the number of commercial networks is about 80, including KT, Onse Telecom, Hanaro Telecom, and Thrunet, while the number of nonprofit ISPs is 7, making it a total of 87 ISPs in Korea. Considering the fact that the number of ISPs in 1999 was 40, this is a rapid growth. Below, the state of the domestic Internet backbone network is presented by looking at the major carrier providers that have large-scale exchanges with the nationwide network:

- **KII Network (**PUBNET - Korea Telecom). KT has been providing services by establishing a router-oriented network at the end of 1997 in order to meet the rapidly increasing demands in the public sectors. However, by establishing an ATM switched network since the end of the 1999, KT is converting users on the existing PUBNET into ATM networks, This process of migration was due to be complete by the end of 2001. Moreover, KT is providing a nationwide service through leased lines, frame relay, and ATM lines, and through diversification of the types of access speed and forms of Internet networks. The Internet backbone network has been constructed in dual system by installing ATM switches and relay/backbone routers at seven major cities across the country (Seoul, Inchon, Suwon, Taejon, Pusan, Taegu, and Kwangju), and ATM subscriber access switches are installed in 130 areas across the country, providing access of 155-622 Mbit/s between major cities within the backbone sector, and 155 Mbit/s between medium and small cities.
- **PUBNETPLUS** – DACOM is establishing a KII-G infrastructure construction project that connects the national and public agencies with ATM switches and optical cables. At the same time, Dacom is propelling a project for consolidating the infrastructure of high-speed IT networks, such as promoting the use of KII-G through investments on multimedia application services and contents. DACOM is preparing for interconnectivity between terrestrial and wireless IT networks, and installation of a next-generation intelligent network. High-speed ATM switch networks have been established, and DACOM has been providing ATM service, FR-ATM exchange service since July 2000, and Internet service since September 1999. Currently DACOM is providing services such as leased line, packet exchange, FR, and Internet service to about 6,000 agencies, and is planning to provide various services for activating the high-speed IT networks, such as ATM, FR, Internet service, and other application services in 2001. In the section between main nodes, transfer lines of 2.5-5 Gbit/s are offered, whereas between small cities, 45-155 Mbit/s, while maintaining stable service in case of accidents by dualizing the routes between the nationwide nodes.
- **HPCNet/KREONET – KISTI** HPCNet is a supercomputer user group, whereas KREONET is a research network user group. HPCNet and KREONET share major domestic backbone networks, and provide services through 155-300 Mbit/s backbone networks between major nodes and 45 Mbit/s between middle and small nodes. HPCNet is a backbone network constructed in order to provide KISTI's supercomputer infrastructure to all supercomputer users. HPCNet is promoting the use of supercomputers by researchers in each subscribed agencies, public and private company laboratories, and educational institutions, and at the same time, is continuously enhancing the domestic network backbone for high-speed use. The main network advancement project in 2001 was to promote the increase of all local network node speeds to 45-155 Mbit/s. Also, in order to strengthen the characteristic as a national research network, and to promote the transition into a leading network, the establishment of a next-generation network through connection with KT's KOREN is being prepared. KREONET is one of the five national backbone networks, a noncommercial ISP that aims to enhance research productivity, by mutually connecting the network with the researchers of domestic government laboratories, science technology related public agencies, and university company-attached laboratories, and to activate the share of domestic and overseas computer resources, and the mutual exchange of research data. Moreover, in order to specialize enhance KREONET into KREONET2, a plan of high

speed exchange (45 Mbit/s) with STAR-TAP, the American NSF's high performance research network, in cooperation with MIC's APII testbed, is under way.

- **KOSINET – NCA.** Since 1994, KOSINET has been serving as a part of the establishment of an infrastructure for sharing information and activating Internet use in government, public agencies and other using agencies, providing a connection service with the non-commercial networks (educational, research networks, etc) through KIX, which is currently operated by NCA, and also an overseas Internet service. By using KII-G as an exclusive high speed network, cost reduction in communication fee is being promoted, while NCA is providing services using the KII-G by universally managing the communication lines of the related agencies. For Internet networks for government and public agencies, the Seoul-Yongin section is covered by a 45 Mbit/s line, which has been established and operated with a view to activating Internet use in government and public agencies.
- **EDUNET – KERIS.** Korea Education & Research Information Service (KERIS) is promoting projects such as establishing a general education information service for students and teachers, establishing EDUNET in order to provide various information, establishing a research information service system, and establishing a research information system in order to provide original academic DB services. KERIS is also promoting projects such as IT-based education, and researching the policies in IT-education. EDUNET consists of 12 nodes across the country, connected with 4-6 Mbit/s lines between major nodes, and 512 Kbit/s-2 Mbit/s, between intermediate and small nodes.

3.3.3 Access networks

Wired services

3.15 The types of broadband wired services that spread rapidly after 1998 include xDSL, Home PNA and LAN. The number of high-speed Internet subscriber have increased monthly by an average of 21 per cent, from 870,000 in April 2000 to 4 million by December 2000.[3]

- **Dial-up modem and ISDN services.** The dial-up modem and ISDN services are now legacy services that are mostly used by those users who use the Internet for a rather short time and do not download large files. Online service started commercially in December 1993. Recently, in spite of the increase of high-speed Internet services such as ADSL and cable modems, the number of online service users increased from 9 million in 1999 to 16 million in December 2000, and this seems to result from the increase of various forms of "free service", rather than an increase of subscriptions. By using ISDN (Integrated Services Digital Network), users can access the Internet at speeds of between 64 kbit/s and 128 kbit/s.
- **Cable modems.** The CATV Internet network is a Hybrid Fibre/Coax (HFC) network, using optical cable between broadcasting stations and the main distribution frame, and coaxial cable between MDFs and subscribers. Commercial services have been provided since Thrunet's service began on 1 July, 1998. Currently, in December 2000, Hanaro Telecom, DACOM, Dreamline, Thrunet, Onse Telecom, and SK Telecom are providing the service.
- **XDSL.** The number of ADSL (Asymmetric Digital Subscriber Line) subscriber has increased rapidly since Hanaro's commercial service was introduced in April 1994. Hanaro Telecom is providing Internet access through FTTC (Fiber to the Curb)-type digital optical local loop by bringing the optical cable to the apartment doorway. Korea Telecom provides Internet access under its "Megapass" brand name. Each Megapass service is divided according to its connection speed, fixed IP, and number of users; light (for download speed of 1.5 Mbit/s), premium (for download speed of 8 Mbit/s), My-IP, and Multi IP. Other xDSL services are HDSL (high bit rate digital subscriber line) service and VDSL (very high bit rate digital subscriber line) service. HDSL is being used mostly by consumers living in commercial buildings and apartments because it can support a large number of subscribers. VDSL has been under trial in 50 households within Seoul since August 2000. Commercial VDSL service was due to begin in areas near Seoul in 2001. The service will be expanded in the second half of 2002.

[3] For the latest data, see the: Ministry of Information and Communication website at: http://www. mic.go.kr

Wireless Internet

- **Internet via cellular mobile communications.** The Internet service using mobile communications was originally provided on the basis of the existing IS-95 standard, with an access speed of 9.6 kbit/s. IS-95A offers 14.4 Kbit/s speeds and the commercial service of IS-95B in Seoul provides speeds of 64 kbit/s. Recently, the commercialization of IS-95C provided access speeds of up to 144 Kbit/s. While there are currently many problems in providing the service, such as the methods of use, and charging policies, providers are plotting strategies in order to grab the leading edge in the wireless multimedia business, which leads to IMT-2000.
- **B-WLL** (broadband wireless local loop) is a wireless telecommunication system offering high-speed Internet transmission within a radius of 2-3 km by using a frequency of 26 Ghz. In March 1999, Korea Telecom and Hanaro Telecom were selected as the providers of B-WLL, and in June 1999, Dacom was additionally selected. Hanaro Telecom had started its service in July 2000, and was planning to provide commercial service of 1-2 Mbit/s, in 2001.
- **Satellite Internet.** Internet via satellite enables telecommunications in areas where on-line services or Internet access are impossible, such as islands or mountain areas where terrestrial lines cannot be built. The transmission speed is 56-80 Kbit/s for uploading data and 400 Kbit/s-1 Mbit/s for downloading. Korea Telecom started its service in May 1999 and Samsung SDS is also providing services via the Mugungwha satellite launched in 1996. Also, GCT Korea and Mirae on-line have been offering services since the second half of 2000.

3.3.4 International submarine cables

3.16 The current international submarine optical cable network connected to Korea is composed of a total of ten undersea cables (JKC, HJK, RJK, CKC, APCN, FLAG, SMW-3, CUCN, Across the Pacific, and APCN-2), and its total capacity amounts to 1,402.6 Gbit/s. The domestic submarine cable relay stations are distributed in eight areas (Pusan, Cheju, Geoje, Taean, Goheung, Namhae, Hosan, and Ulleung), and its total capacity amounts to 13.48 Gbit/s. After 2002, it is expected that the submarine optical cables will account for 95 per cent of all Internet traffic, and that the usage of submarine optical cable lines will exceed reliance on satellite telecommunications.

3.4 Overview of Korean network infrastructures

3.17 Like PDD 63 in the United States, Korea now has an information and telecommunication infrastructure protection Act. This law allows the president of the central government cabinet to designate certain infrastructures as critical and gives powers to require their repair and rapid recovery in the event of damage from intrusions and virus attacks

3.18 The law covers the following areas:

- E-government and general administration;
- Financial networks;
- Military and defence;
- Gas and energy;
- Transportation;
- Telecommunications.

3.19 The General Administration Network is intended for the interoperability of government and public services. The Assemblies, Law and Administration of the government are interconnected by this network with the commercial Internet, and with the networks of other public and private agencies. It is run on a non-profit basis. General Administration Networks are operated by five major nodes, central, Gwacheon, Taejon, Honam and Youngnam center. In order to provide service to the general public, the central node is interconnected to public Internets, like KORNET, BORANET, Pubnet and KREONet.

4. Types and impact of threats to critical network infrastructures

4.1 The year of the Internet worm, 2001

4.1 The year 2001 was known as the "Internet worm" year, with worms such as Remen, Li0n, Sadmin/IIS, Chees and Red Worm all appearing in the first part of the year. In the second half of the year, worms infecting Windows NT, including CodeRed I/II and Nimda attacked Korean networks, affecting businesses and home PCs, especially those with broadband connections (see Table 4.1).

4.2 Recent worms like CodeRed and Nimda increased network traffic by up to ten times the normal rate, putting a heavy burden on the ISPs, which, at peak usage times, had difficulty maintaining their networks. The entire communication infrastructure was under strain and recovery was difficult. A worm typically operates in the following manner:

1. It scans systems chosen at random;
2. If it finds a vulnerable system, it attacks and installs the worm program;
3. It opens a specific port as a backdoor;
4. It sends to the originator, by e-mail, specific files like passwords;
5. Alternatively, it replaces the homepage;
6. It continues to repeat numbers 1 to 5, *ad infinitum*.

4.3 These worms then shifted from UNIX server to Microsoft Windows PCs :

- It appears that attackers regard Windows as a particular challenge because of the "fame" they achieve in the hacker community for demonstrating vulnerabilities in the operating system.
- Personal computers using Microsoft Windows have the equivalent power to a server.
- Security on personal computers is not usually high.
- General users can open attached files as normal.

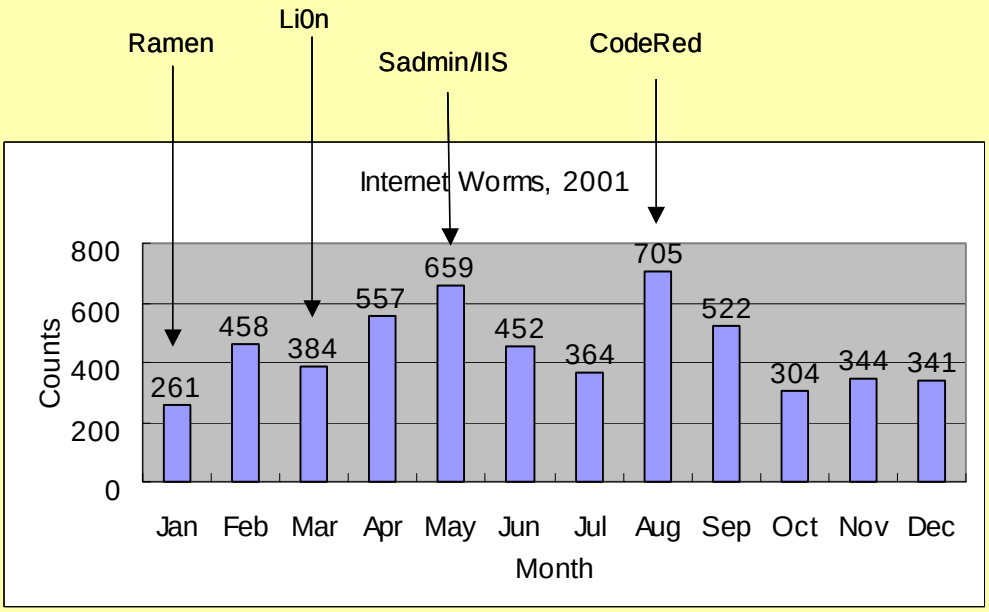
4.4 As illustrated already, worms infiltrate vulnerable systems that do not use anti-virus scanning or patches. All commercial systems have some areas of vulnerability, for instance:

- The vulnerabilities of Unicode;
- The buffer overflow of ISAPI;
- The attacks to IIS RDS;
- Common network using NETBIOS;
- Information disclosure using NULL session ;
- LN Hash vulnerable in SAM ;
- The overflow vulnerabilities in RPC;
- The vulnerabilities of sendmail ;
- The vulnerabilities of BIND;
- The vulnerabilities of LPD;
- Sadmin and mountd ;
- Default SNMP string.

4.2 Internet attack statistics

4.5 Figure 4.1 shows the Internet worms that affected Korean networks in 2001, by month.

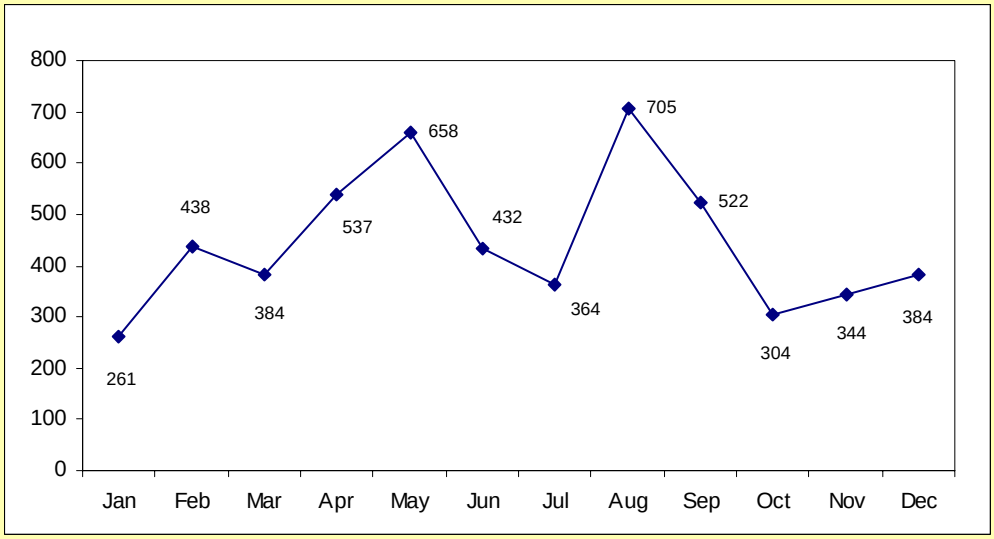
Figure 4.1: Internet worms in Korea in 2001
Counts per month



Source: Case study research

4.6 Figure 4.2, showing the security incidents reported to KISA in 2001, includes statistics for the Sadmin/IIS worm in March, Code Red I in July and Code Red II in September 2001. By the end of 2001, security breach reports fell as many enterprises were better prepared to prevent attacks. However, in the longer term, the increase over time is evident. Table 4.1 shows the number of sites reporting incidents between 1996 and 2001.

Figure 4.2: Monthly statistics of security incidents reported to KISA in 2001



Source: KISA.

Table 4. 1 The number of affected sites between 1996 and 2001

	1996	**1997**	**1998**	**1999**	**2000**	**2001**
AC.KR	95	32	80	262	260	554
CO.KR	46	25	69	248	818	2’509
OR.KR	2	2	3	18	6	63
RE.KR	0	3	4	11	3	11
{geo}.KR	0	0	0	0	48	225
Other	4	2	2	33	808	1,971
Total	**147**	**6’4**	**158**	**572**	**1’943**	**5’333**

Note: The reason why “other” has the highest number is because that category includes personal computers.
Source: KISA.

4.7 Table 4.2 illustrates the need for security incidents to be dealt with by an international security incident response team.

4.8 Table 4.3 shows which countries are connected to the security incidents. Table 4.4 shows the intrusion statistics by style of attack. Table 4.5 shows the impact and outcome of security incidents in 2001. Table 4.6 shows the intrusion statistics since 1996. As shown in that table, incidents increased almost every year. The reasons for this increase were probably:

- The vast increase in the number of Internet users;
- The extension of the boundaries and limits of technical capabilities.

Table 4.2: International security incidents

Direction of attack	Domestic	Attacks launched from Korea	Attacks from abroad		Direction of attack not known	Total
			Direct	Indirect		
Number	285	175	289	408	4’351	5’508
%	5.1%	3.2%	5.3%	7.4%	79.0%	100%

Table 4.4: Attacks broken down by supposed place of origin

Economy	**Number**	**Economy**	**Number**
Australia	600	Italy	1
Austria	7	Japan	615
Brazil	310	Malaysia	76
Canada	21	Netherlands	24
Chile	1	Poland	30
United Kingdom	107	Slovenia	3
France	707	Spain	5
Germany	220	Thailand	61
Hong Kong SAR	1	USA	51

Table 4.5: Breakdown of intrusions by type

Classification	**Numbers**	**Remarks**
Impersonation	299	Sniffer, password cracker
S/W Security bug	150	IIS Unicode
Buffer overflow	323	popd, imapd, mountd, named, amd, ftpd, rpc.statd & automountd, rpc.ttdbserver, rpc.cmsd, RPC
Configuration error	17	System configuration error
Malicious codes	1’571	Back Orifice, NetBus, rootkit, backdoor, worm
Protocol error	1	IP spoofing, session hijacking
DOS	57	carko, syn flood
Attacks with e-mail	64	Mail relay, mail bomb, spam
Scan probe	2’853	Port scan, network scan
Social engineering	4	

Source: KISA.

Table 4.6: Breakdown of intrusions by outcome

Impact	Number	Remarks
Scan Probe	3’664	Scan
Compromised	1’240	Gained access to root
Disclosure	7	Disclosure of information
Data Removal	59	Removal of log files
Unauthorized Access	86	Unauthorized access to the system or files
Homepage Defaced	212	Homepage replaced
System interruption	2	System down
System Bug	5	System non-operational
DOS	58	DoS attack

Table 4.7: Intrusion statistics - Changes since 1996

Year	**‘96**	**‘97**	**‘98**	**‘99**	**‘00**	**‘01**
Counts	147	64	158	572	1’943	5’333
% growth	n.a.	-44%	147%	262%	240%	174%

Source: KISA

4.3 Computer virus attacks

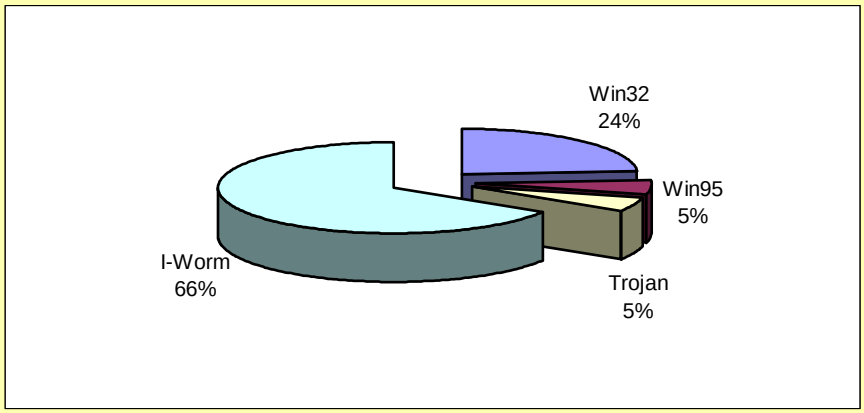
4.9 In 2001, numerous foreign viruses attacked Korea’s networks. Worm viruses like Nimda and SirCam were attached to e-mails and spread rapidly. Table 4.7 shows the may viruses found in Korea. This data is an example of the kind of information that can be helpful to anti-virus companies, such as Ahn-Lab, Hauri, Symantech Korea, Micro Trend Korea.

Table 4.8: Computer viruses in 2001

Rank	Computer virus	Type	Total
1	Win32/Nimda	I-Worm	16’665
2	Win32/Sircam.worm	I-Worm	12’216
3	Win32/Funlove.4099	Win32	11’372
4	I-Worm/Wininit	Trojan	2’827
5	W32/CIH	Win95	2’705
6	Win32/Nimda.D	I-Worm	2’205
7	I-Worm/Hybrids	I-Worm	1’754
8	I-Worm/Hybrid.Spiral	I-Worm	1’190
9	W32/Weird	Win32	1’187
10	I-Worm/Navidad	I-Worm	1’127
other			11’,785
Total			65’033

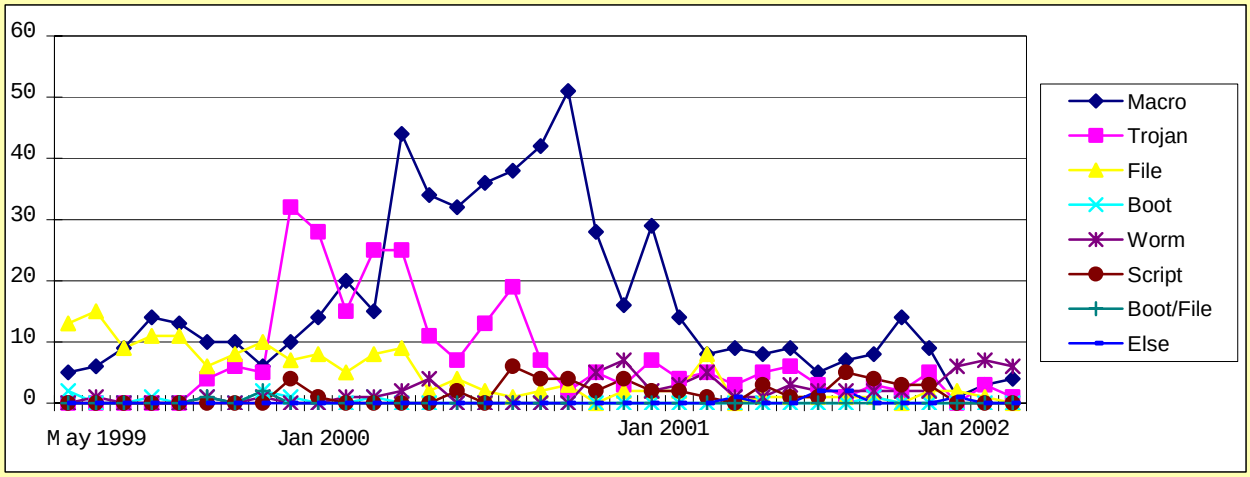
4.10 The data above is also illustrated in the Figures 4.3 and 4.4.

Figure 4.3: Computer viruses found in 2001



Source: KISA.

Figure 4.4: Computer viruses by type since 1999



Source: KISA.

5. Key initiatives to protect critical network infrastructures

5.1 Information and Telecommunication Infrastructure Protection Act

5.1.1 Overview

5.1 Information and telecommunication infrastructure protection began with a review of the current situation of virus and hacking incidents, and how these result in serious problems and damage when this infrastructure supports the underlying systems of the social infrastructure.

5.2 In Korea, national government administration, national finance, national emergency services, national telecommunication and national transport are among the key areas of national security for the information society. These are the systems that are most at risk of successful Internet intrusion and virus attacks. If such attacks against critical infrastructures succeed in bringing public services to a halt, the result would be widespread economic and social disorder, with a high cost of recovery.

5.3 The Telecommunication Infrastructure Protection Committee, a subsidiary of the office of the Prime Minister, was set up to organize a pan-governmental response mechanism to these attacks. The Committee is comprised of the Prime Minister and chief officer of each department, including the Ministry of Government Administration and Home Affairs, the Ministry of Science and Technology, the Ministry of Finance and Economy, the Ministry of Foreign Affairs and Trade, the Ministry of Justice, the Ministry of National Defense, the Ministry of Information and Communication, the Ministry of Commerce, Industry and Energy, the Ministry of Construction and Transportation, the national intelligence service, financial supervisory service, etc. The Committee is chaired by the Prime Minister.

5.4 The Chairman of the Ministry of Information and Communication is responsible for a sub-committee, the Telecommunication Infrastructure Protection working group. This working group is comprised of the Vice-Minister of each ministry.

5.5 The aim of the Joint Working Group for Security Incident Response is to prevent the spread of incidents, to help trace attackers and to restore security.

5.1.2 Designation of critical infrastructures

5.6 What processes and criteria are used to define social facilities, including facilities of the private sector, as a critical information infrastructures? Each administrative organization selects these facilities as a critical information infrastructure according to a base line such as the national importance of the facility, the

level of dependency on the specific facility, and the potential impact of an incident, were such an incident to occur. Examples of these critical information infrastructures include, *inter alia*, subways, airports, power plants, broadcasting facilities, national research centres.

5.7 Each administrative organization establishes protection guidelines, and recommends that other organizations observe these guidelines. Each sub-organization of the administration then carries out its vulnerability analysis and assessment, establishes its protection plan, and reports to the administrative organization. A protection plan might include:

- The result and assessment of the protection plan deployed;
- Comparisons with the previous year;
- A prevention plan against incidents;
- An incident response and recovery plan;
- The protection plan for the next year.

5.8 Furthermore, each executive organization must appraise the threat of electronic infringement that can destroy the confidentiality and integrity of the information related to the operation of the critical information infrastructure. KISA (Korea Information Security Agency), ISAC (Information Sharing and Analysis Center), the Designated Information Security Company, and ETRI support these assessment activities. Organizations responsible for designated critical information infrastructures have to carry out their vulnerability analysis and assessment once within six months, every second year. The steps for vulnerability analysis and assessment are:

1) Establishment of a working group, vulnerability analysis and an assessment plan;
2) Selection of the subject for analysis;
3) Threat and vulnerability analysis;
4) Re-examination of the existing protection plan, and appraisal of vulnerability;
5) Establishment of a new protection plan.

5.9 The following are examples of security incidents:

- Unauthorized persons who access the major infrastructure or authorized persons who manipulate, crack, conceal and outsource;
- The use of malicious programs like computer viruses and others to crack data and to disrupt the operation of the critical infrastructure;
- The use of control messages or inaccurate commands to interfere with the operation of the critical infrastructure.

5.10 Security incidents of any kind may use malicious codes to distribute, install, and execute computer viruses, Trojan horses, worms, back doors and attack scripts. Critical infrastructure systems can be totally disrupted by such attacks. Heads of administrative organizations therefore need to establish protection plans, and to encourage other relevant organizations to adhere to them. The protection plans must also contain security management guidelines, operational guidelines, vulnerability assessment guidelines, security incident prevention, and a response and recovery plan.

5.11 If organizations experience any kind of security incident, they must report this incident to one of the relevant administrative organizations, such as KISA, or a law enforcement organization. If the incident is considered critical, then a protection/prevention working group must be established to prevent the incident from spreading.

5.1.3 ISAC and special security companies

5.12 The ISAC (Information Sharing and Analysis Centre), whose role is to analyse security incidents and report to the relevant organizations, is the system for prevention, detection and response against security

incidents. One useful approach for government might be to establish further ISACs, such as a financial ISAC, a communication ISAC, etc. Ideally, each ISAC should:

- Have at least 15 staff;
- Have a budget of at least 2 million won;
- Be capable of secure information management;
- Establish and observe information security management rules.

5.13 Other special information security companies may be used for testing and analysing. As it becomes increasingly difficult for each organization to ensure protection of its critical information infrastructures on its own, a national information security company may be designated to apply the critical information protection plan. The requirements for such a special information security company are that it should:

- Have at least 15 experts;
- Have a budget of more than 2 million won;
- Own its identification and access control system.

As of November 2001, nine companies were registered as special information security companies.

5.1.4 The penalty

5.14 The following illegal acts under this law are punishable as follows:

- Anyone who disrupts or damages the critical infrastructure with intrusion and computer viruses can be punished with a one hundred million won fine or 10 years imprisonment.
- Anyone working in the organizations who evaluates the vulnerabilities, report and recovery against security incidents and reveals any information about its role may receive at least 5 years' imprisonment or 10 years' qualification suspension, or a 50 thousand won fine.

5.15 The following illegal acts are also punishable by fines:

- If a managerial office doesn't follow instructions from a government office, it may receive a 10 thousand won fine.
- If the ISAC doesn't report within 30 days on its role being implemented or updated, it may receive a 10 thousand won fine.
- If the special information security company fails to report within 30 days any breaks, discontinuation or resumption of their role, it may receive a 10 thousand won fine.
- If the special information security company fails to report, or falsely reports, information at the request of the MIC, it may receive a 10 thousand won fine.
- If the special information security company fails to return any materials related to vulnerabilities assessment and analysis to the managerial office once the SISC's role has been cancelled or abolished, it may receive a 10 thousand won fine.

5.1.5 How to determine critical infrastructures

5.16 Any relevant government body can analyse its network infrastructure in terms of its "critical" characteristics, by understanding its own business and organizational strategic demands. Usually, this would be carried out as a business unit, by assessing the organization's structure vertically and horizontally.

- Vertical level analysis: All businesses can be analysed hierarchically, distinguishing between upper-level and lower-level activities.
- Horizontal level analysis: All businesses are treated at the same level, according to their field of activity.

The details can be identified by considering the following issues:

- If a particular infrastructure has a nationwide control and management system, information system or communication system, then it may be considered critical.
- The analysis could be based on a review of the vulnerability analysis, a protection report, economic aspects and other responsibilities.
- An analysis could be based on the consequences of suffering an electrical brownout.
- An assessment can be made of whether the electrical control and management system, MIS and communication systems are physically connected, or whether these are not physically connected.

Table 5.1: Criteria for determining critical infrastructure

Area	Major items	Remarks
Electrical control and management	Energy production and distribution Aviation Official Regulation System Port Management System Communication Network Management	Failure of these systems could be fatal for social environment services.
Information Systems	Management Information System Rail Road Reservation System Citizen Information Management National Tax Management	Excluding systems used only within organizations.
Communication Systems	Switches, Routers and other Communications Facilities	Excluding systems that are regulated under other laws.

5.1.6 Likelihood of security intrusion

5.17 The possibilities of security incidents affecting critical infrastructures are illustrated in Table 5.2.

5.2 Reviewing the critical networks

5.2.1 General administration networks

5.18 The general administration networks are the largest computer networks comprising government and citizen information services networks, and interconnecting 77 governmental organizations. Within these networks, the sheer number of services means that security incidents can have a huge impact. Examples of such services are electronic documents interchange, national tax system, real estate, citizen and diplomacy information flows with citizen's private information.

5.19 The general administration networks, comprising shared networks and general tax services, general citizen, foreign affairs and real estate networks, should all be considered as critical infrastructures. General administration networks also maintain national territory administration that interconnects the central and local authorities. All 16 cities and local authorities, 232 Kun and Ku, 3'511 Eup, Myun and Dong are connected.

5.20 Regional government networks should also be considered as critical infrastructures.

Table 5.2: The likelihood of security incidents affecting critical infrastructures

Area	Possible security incidents
Energy, Gas	- The central control systems are more secure than others because they may be using dedicated leased lines, without any connection to others in outside networks. - Vulnerability could increase if the central control systems are connected with general networks. - Remote control systems in the general and production system could be vulnerable because that system uses generic system software, or if is connected to the general systems.
Railway, Airplane, Port	- The intrusions from outside networks could be easier because these systems are, in general, migrating from being closed to open networks. - They may be more vulnerable if they use mobile or other frequency-based networks.
Financial	- Generally, financial systems operate via leased lines and have good security. - However, foreign attacks could be mounted via global telecommunication systems, especially in areas such as Internet banking and commercial operations.
Telecom	- The switching systems and carrier line systems should not be easily attacked. - Intranet and Internet-based commercial networks could be attacked relatively easily and voice frequency networks could be vulnerable to frequency interference.
General Admin.	- The government is trying to set up electronic government, so may become more vulnerable to Internet attacks

5.2.2 Diplomatic networks

5.21 Diplomatic networks are interconnected between the Ministry of Foreign Affairs, the Ministry of National Defense and the national intelligence service, in order to share foreign affairs information. This diplomatic network should be considered as critical infrastructure. Other systems, dealt with in the section below, should also not be overlooked as critical infrastructures.

5.2.3 National health and annuity networks

5.22 The National Citizen Health Security Information System is operated by its own managerial organization. It interconnects the 6 central and local departments and 235 agencies via high-speed networks using leased communication links. It should be considered a critical infrastructure because any security problems, for instance for qualification management for all citizens, the details of medical examinations and medical fee management, could cause significant problems.

5.23 National annuity systems are run by their own managerial organizations. They interconnect via high-speed networks and LANs in order to maintain the subscriber information management, annuity decision and collection and annuity fee provision.

5.24 National citizen health networks may also be considered critical infrastructures because some security incidents could result in the over-estimation of annuities or in nonpayments.

5.2.4 Communication and networks

5.25 Telecommunications use the Public Switched Telephone Network (PSTN) for voice communication and Public Switched Data Networks (PSDN) for Internet services. The detail of national backbone, switching systems and user systems is described below.

5.26 The PSDN is growing fast owing to the rapid upgrading of Internet services, national administration services, company information, logistics and financing services. This means that if security problems affect the PSDN system, this will have rapid repercussions for the overall national infrastructure.

5.27 The PSTN system is a basic national service provided to the population. The PSTN has not seen many problems as the switching devices and trunk systems are not visible to the general public.

5.3 Regional level security coordination

5.28 Nowadays, many virus and hacking codes, including worm attacks, have the following features:

- Stealth;
- Importability, platform independent;
- Polymorphism, dynamic update;
- Special mission;
- International scope.

5.29 With the Code Red, Nimda and other worm attacks in 2001, Korea had the highest rate of compromise, insofar as these attacks could be classified by country, as shown in Table 5.1.

Table 5.1: Internet worm attacks that compromised security, ranked worldwide, 2001

CodeRed	%	CodeRedII	%	CodeRed.d	%	Nimda	%
.net	49	.net	46	.net	47	.net	53
Korea	16	Korea	27	Korea	32	Korea	21
.com	11	.com	13	.com	8	.com	11
.edu	6	China	4	China	4	China	5
Germany	2	Germany	3	Germany	3	.edu	2
Italy	2	.edu	3	.edu	2	Germany	2
Brazil	2	France	2	France	2	Taiwan	2
Spain	2	Italy	2	Italy	2	USA	2
Netherlands	2						
China	2						
France	2						
Denmark	2						

5.30 Such worm attacks could cause international damage very quickly. In an effort to address this threat, the Asia Pacific Security Incident Response Coordination (APSIRC) was held by Japan's Computer Emergency Response Team Coordination Center (JPCERT/CC) in February 2002. Most Asian countries, including Australia, China, Hong Kong, China, India, Indonesia, Japan, Korea, Malaysia, Singapore, Taiwan, Province of China, and Vietnam were invited with the support of funds from Japan. At this conference, all countries presented their activities and shared information. In particular, the conference decided that AUSCERT of Australia would be in charge of the APSIRC task force team.

6. Conclusion and possible areas for further study

6.1 Overview

6.1 The MIC of Korea approved the Information and Telecommunication Infrastructure Protection Act in 2001. This law will apply nationwide in 2002. But if this law is to be applied without any problems, supporting organizations such as KISA, ETRI and special security companies need to develop the capability to evaluate the vulnerabilities of a particular critical infrastructure site. To this end, KISA and ETRI have been studying possible methodologies.

6.2 For this, a nationwide information security management system (ISMS) needs to be established. KISA is trying to launch an evaluation process to assess the requirements. Moreover, KISA is also evaluating security requirements for an Internet data centre (IDC).

6.2 Integrated National Information Security System, under construction

6.3 In the "e-KOREA Vision 2006" promoted by the government, implementation of a small-scale and efficient "SMART Government" is projected. The Ministry of National Defense is aware of the dangers that cyber-terrorism poses for the National Defensive Force, and is moving ahead with the "Information Security System Construction Project" to provide an effective response to hacking or virus attacks.

6.4 As the integration of private, public and state organs accelerates, in line with the growth of the Internet, it is necessary to readjust current thinking among the relevant parties. One step is the establishment of GISAC (Government Information Sharing and Analysis Center), which will act as a cyber terror control centre for the National Network.

6.5 The terrorist attacks of 11 September 2001 in the United States have heightened awareness of the need to invest in disaster recovery and to have prepared responses to this type of terror campaign. In the US, Congress is pressing ahead with establishing a "Hi-tech SWAT" team for preventing cyber terror.

6.2.1 National level construction

6.6 For the efficient and strong promotion of Integrated Information Security Management System by government, the establishment of an Information Communication CSO (Chief Security Officer), directly reporting to the President, is necessary. For rapid response to cyber terror, the operation of what might tentatively be called a "CT Emergency Response Team" is necessary.

6.2.2 Integrated security management system

6.7 For the protection of finance, construction, administration, information communication networks and the national defence network, a mutually cooperative integrated security management system needs to be developed.

6.8 For the efficient and systematic operation of information security, a National Information Security Management Standard model, followed by a Information Security Management Standard, is necessary.

6.2.3 Operation of national cyber terror monitoring

6.9 For rapid response to current and future security alarms, the operation of a provisionally named "National Cyber Terror Monitoring Cell" is needed. This will involve creation of a system of private, government and forces cooperation, and an international cooperation system

6.2.4 Training in “mock cyber terror response" and enforcement by each sector

6.10 Under the aegis of the central Ministry of Information and Communication, Korea Information Security Agency and Virus Consult and Support Center, it is necessary to create a mutually cooperative system to anticipate security threats for both the public and private domains.

6.11 Cooperation with relevant agencies, like CONCERT or the Information Security Enterprise, is well advanced. As the operation of major society infrastructure is generally under private management in an advanced country like Korea, an agency for major information communication infrastructure operation is

needed for each sector of the economy: e.g. finance, communication, transportation, energy, etc; and a government agency is needed to provide better cooperation for incident-handling

6.12 As in the USA, the emphasis is now on the creation of a system of private sector and government cooperation for the protection of major information communication infrastructure (PDD63), and on guidelines and support for the establishment of private ISAC (seven ISACs are now operational or are in preparation).

6.2.5 Strengthening private response systems

6.13 Strengthening communication and cooperation between the private sector and government will involve:

- Preparation of secure operations and management system for shared information by private sector and the government.
- Private/public cooperation, to increase the ability to rapidly detect cyber attacks and enact emergency responses.
- As operating major information communication infrastructure is under private management, the Information Security Consultation Organization consists of CEOs of private agencies.
- Organize and operate a forum for increasing private/public cooperation and raising cooperative response ability.

6.3 Establishing common criteria for evaluating security products

6.3.1 Summary

6.14 A plan is urgently required for estimating the response management plan in the case of cyber-terrorism and countermeasures. Existing countermeasures are insufficient in the light of constantly increasing attacks against the vulnerabilities of information systems.

6.15 Furthermore, it is necessary to establish common international criteria, which are globally accepted, for the purpose of building confidence in the reliability of security products. This will require the creation of an evaluation method regarding the level of information security for the development of next-generation information security systems. It will also require the setting up of an information security evaluation system and a certification agency to evaluate numerous information security systems in a timely manner.

6.3.2 Status

6.16 The United States and other developed States have warned against the threat of cyber-terrorism, and have established countermeasures. As the need for mutual recognition of certification schemes between countries has increased, common criteria that can be used to evaluate various information security systems have been developed as an ISO/IEC standard.

6.3.3 Administrative tasks

6.17 It is necessary to evaluate the management of responses to cyber-terrorism. This will require classifying the information communication network and the level of protection according to the following criteria:

- Risk analysis on the national defence network and information super highway;
- Classify the importance of the each infrastructure;
- Establish the level of protection of various information communication networks for the purpose of protecting against information warfare;
- Establish evaluation criteria for evaluating the level of response management against cyber-terrorism.

Table 6.1: Cyber terror level

Attackers	Target	Level of Damage	Classification
Individual (Hacker)	PC	Individual privacy, property loss	D
Organization (Terrorist, Crime Org)	Enterprise network, Financial network, Power infra. Medical info network, National geography, Information system, etc	Damage on enterprise, Public losses (damage on the public)	C
		National commerce loss, Damage public organization (loss to national economy)	B
Country	National defense network, Foreign affair network, Public peace network	Damage on the important national facility	A

Source: Case study research.

6.18 The IT product evaluation criteria will need to be updated by:

- Increasing the capability for evaluating more IT products, and developing suitable evaluation methods for next-generation information security systems;
- Developing automatic evaluation software;
- Establishing a certification mechanism based on CC;
- Establishing information security system evaluation and certification centres;
- Promoting private evaluation centres.

Annex 1 : References

- MIC, Act of the information and telecommunication infrastructure protection guide, Nov 2001
- NCA, 2002 Korea Internet White Paper, Feb 2002-05-12
- MIC, The White Paper of Information and Telecommunication, Nov 2001
- Center for Security Studies and Conflict Research, Swiss Federal Institute of Technology, "The International Critical Infrastructure Protection Handbook", Nov 2001
- KISA, "The form of constructing the act of Information and Telecommunication Infrastructure Protection", July 2000
- KISA, "The forum of constructing the performance of the act of Information and Telecommunication Infrastructure Protection", Mar 2001
- KISA, "The Forum of How to follow up the act of Information and Telecommunication Infrastructure Protection", July 2001
- KISA, "2001 The Survey of the Information System Hacking and Virus", Dec 2001.
- KISA, "The Survey of the Information Security Related Laws ", Oct 2001
- KISA, "The Guidelines of the Response against Hacking and Virus Attack in the season of World Cup Event", Mar 2002-05-12
- The Cyber Monitoring, "2001 White paper of Korea Cyber Crime", Dec 2001
- Abor Networks, "A Snapshot of Global Internet Worm Activity", Nov 2001
- http://www.gcc.go.kr
- http://www.kftc.or.kr/
- http://www.fss.or.kr/
- http://www.mnd.go.kr/
- http://www.nhic.or.kr/
- http://www.mohw.go.kr/
- http://www.moct.go.kr/