NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DEVELOPING A RELIABLE METHODOLOGY FOR ASSESSING THE COMPUTER NETWORK OPERATIONS THREAT OF NORTH KOREA

by

Christopher Brown

September 2004

Thesis Advisor:	Dorothy Denning
Second Reader:	Joanne Kim

Approved for release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of North Korea.			**5. FUNDING NUMBERS**
6. AUTHOR(S) Christopher Brown			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES: The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Computer network operations (CNO) can be considered a relatively new phenomenon being encount modern warfare. Computer network operation is comprised of three components, computer network attack computer network exploitation (CNE), and computer network defense (CND). Computer network attack is def operations to disrupt, deny, degrade, or destroy information resident in computer networks, or the computers and n themselves. Computer network exploitation is the intelligence collection and enabling operations to gather data fro adversary automated information systems (AIS) or networks. Finally, computer network defense are those m internal to the protected entity, taken to protect and defend information, computers, and networks from disruption, degradation, or destruction.

No longer is warfare limited to the use of kinetic weapons and conventional methods of war. Computer network operations have become an integral part of our adversary's arsenal and more attention must be paid to the effects of CNO activities, particularly CNA and CNE being conducted by our adversaries. Of the many states suspected of conducting active CNO activities against the United States and other nations, none warrants more attention than North Korea.

This thesis presents the development of methodology using information available from open sources. This work is intended to prove that a useful methodology for assessing the CNO capabilities and limitations of North Korea can be developed using only open source information.

14. SUBJECT TERMS Computer Network Operations (CNO), Computer Network Exploitation (CNE), Computer Network Attack (CNA), Computer Network Defense (CND), North Korea, and DPRK.	**15. NUMBER OF PAGES** 93
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for release; distribution is unlimited

DEVELOPING A RELIABLE METHODOLOGY FOR ASSESSING THE COMPUTER NETWORK OPERATIONS (CNO) THREAT OF NORTH KOREA

Christopher A. Brown
Lieutenant, United States Navy
B.S., College of Aeronautics, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2004

Author: Christopher Brown

Approved by: Dr. Dorothy Denning
Thesis Advisor

Professor Joanne Kim
Second Reader/Co-Advisor

Dr. Peter Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Computer network operations (CNO) can be considered a relatively new phenomenon being encountered in modern warfare. Computer network operation is comprised of three components: computer network attack (CNA), computer network exploitation (CNE), and computer network defense (CND). Computer network attack is defined as operations to disrupt, deny, degrade, or destroy information resident in computer networks, or the computers and networks themselves. Computer network exploitation is the intelligence collection and enabling operations to gather data from target adversary automated information systems (AIS) or networks. Finally, computer network defense are those measures, internal to the protected entity, taken to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.

No longer is warfare limited to the use of kinetic weapons and conventional methods of war. Computer network operations have become an integral part of our adversary's arsenal and more attention must be paid to the effects of CNO activities, particularly CNA and CNE being conducted by our adversaries. Of the many states suspected of conducting active CNO activities against the United States and other nations, none warrants more attention than North Korea.

This thesis presents the development of methodology using information available from open sources. This work is intended to prove that a useful methodology for assessing the CNO capabilities and limitation of North Korea can be developed using only open source information.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to Dr. Dorothy Denning and Professor Joanne Kim for their inspiration, motivation, and support throughout this meticulous study. I thank you all for your guidance and wisdom in developing this study. This has truly been an invaluable educational experience.

I would like to thank Peter Hayes of the Nautilus Institute for Security and Sustainability for his assistance during the initial stages of my research. Thanks to Mr. Andrew Choi of the Korean Information Security Agency (KISA) for providing access to South Korean CNO subject matter experts.

To my loving wife Karla and my wonderful son Tristan, thank you both for your patience, enthusiasm, and continued understanding throughout this project. Without the both of you the completion of this study would not have been possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Assessing a foreign country's Computer Network Operations (CNO) activities is of high priority in the Intelligence Community (IC), particularly activities relating to Computer Network Attack (CNA) and Computer Network Exploitation (CNE). Although there is extensive classified analysis and reporting in this area, unclassified Internet-oriented research is likely to provide a number of key analytical insights that cannot be obtained from classified work alone.

Modern warfare is changing, and network warfare or cyber-warfare is increasingly becoming more vital to our nation's national interests. With most of the country's infrastructure becoming more automated and network-centric, our adversaries could potentially provide a crippling blow to our nation's infrastructure via the Internet. Although the United States is the world leader in preparing and seriously thinking about cyber-warfare, we should not fall into a level of complacency. We should continue to focus on Computer Network Defense (CND) in an attempt to stay one step ahead of our adversaries.

B. MOTIVATION

Information technology is now an integral part of modern culture and industry. Unfortunately this modernization leaves us vulnerable to cyber attacks. With these weapons of mass disruption, irreparable damage could be inflicted on a country's critical information technology (IT) and civil infrastructures. Several of our nation's critical infrastructure system to include electric power generation, transmission and distribution, mass transit, and oil and gas refining are now being monitored and controlled by networked systems using supervisory control and data acquisition (SCADA) devices [GAO 04]. These SCADA systems are vulnerable to attack as they are often bridged with other IT systems in order to provide remote access to the networks and instant access to critical data regarding the status of systems.

Cyber attacks on critical government and civilian computer systems are becoming more prevalent as more systems are joining the "information superhighway" [Connole

98]. Several foreign states are suspected of conducting CNO against the United States and other nations' IT infrastructures. North Korea has long been suspected of conducting or sponsoring various CNO activities. A methodology for assessing a foreign country's CNO activities could provide invaluable insight into North Korea's CNO capabilities, limitations, and modus operandi.

C. OBJECTIVES

This thesis serves to develop a standard research methodology necessary to assess North Korea's CNO activities from open sources.

Given the history of high diplomatic and political tensions between the United States and North Korea it is most prudent that the Democratic People's Republic of Korea (DPRK) be the focus of this research. For years it has been reported that the DPRK has expressed great interest in the research and development of CNA capabilities.

The goal of this study is to assess North Korea's CNO activities using open sources, including those available through the Internet. This research will identify and analyze relationships between key people and organizations involved in CNO activities, including CNO planning, operations, research, and education. This study will examine CNO activity in government, civilian and military organizations, non-government entities including educational institutions and private industry, non-state organizations the foreign country may be supporting, and CNO-oriented relationships with other foreign countries.

Often times the key indicators and precursors to CNO activities that are state sponsored are unclassified and available on the Internet. This thesis intends to carefully examine several categories of information that directly or indirectly contribute to our understanding of the CNO capabilities, limitations, and intentions of North Korea. This research will develop a methodology for assessing a foreign country's CNO activities. The methodology will identify the critical information points necessary to assess North Korea's CNO capabilities, limitations, and intentions. The Internet is the primary source of information.

D. THESIS ORGANIZATION

Seven chapters comprise this thesis:

- *Chapter I – Introduction:* Establishes the goals for the thesis. Identifies the motivation and purpose behind conducting this research.

- *Chapter II – Background:* Provides information on North Korea's IT infrastructure, capabilities, and limitations. Briefly discusses laws and regulations associated with Internet use.

- *Chapter III – Academic Activity and Public Community:* Discusses the involvement of North Korean academia with respect to CNO activities. Discusses the IT educational opportunities made available to students and the military.

- *Chapter IV – External Information Technology Aid:* Discusses the IT aid provided to North Korea. Briefly discusses the export restrictions that apply to North Korea.

- *Chapter V – Government Activity:* Examines whether North Korea is training cyberwarriors and whether it has incorporated CNA/E in its military doctrine.

- *Chapter VI – Computer Network Attack/Exploitation Activity:* Examines and discusses suspected or reported CNA/E activities associated with North Korea.

- *Chapter VII – Conclusions and Recommendations:* Explains the conclusions and provides recommendations with regard to possible future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. INTRODUCTION

This chapter provides a detailed overview of North Korea's information technology infrastructure, along with a brief discussion of the laws and regulations associated with Internet use in North Korea.

B. INFORMATION TECHNOLOGY INFRASTRUCTURE

Information technology is still relatively new to North Korea. Kim Il Sung first introduced the technology in the early 1980s when the DPRK took the initiative of establishing an integrated circuit (IC) factory that later led to the development of its first indigenous personal computer (PC), the Bongwha 4-1[Hayes 02]. By the mid 1980s the DPRK had established the Pyongyang Informatics Center (PIC) with the primary objective of software research and development. The PIC successfully developed several Korean based software products to include word processing and desktop publishing applications. Fast-forward 16 years to April 2002 when at the Computer Software Expo of DPRKorea in Beijing the DPRK unveiled its domestically developed operating system along with a mix of speech recognition and character recognition software [ITWorld 02].

There have been significant developments in the hardware sector since the development of the 8-bit Bongwha 4-1 PC prototype in 1982. The DPRK is now reported to be manufacturing 16-bit and 32-bit PCs and to have successfully developed 16-megabit IC chips. An IC pilot plant was constructed at the Electronics Research Institute of the Academy of Science and the PIC is currently conducting research and development of a 64-bit microcomputer.

1. Telecommunications

Automatic switching networks were introduced in North Korea in the 1970's with limited use in Pyongyang, Siniju, Hamhng, and Hyesan. In 1985 there were a reported 30,000 telephones in use in the DPRK compared to the 1.1 million in use today [CIA 04]. These telephones were primarily available at factories, government offices, cooperatives, and other workplaces [LOC 93]. Satellite communication was also introduced in the mid 1980's with the construction of a satellite ground station near Pyongyang utilizing the

International Telecommunications Satellite Corporation (Intelsat) Indian Ocean satellite and one Russian satellite, with the French providing most of the technical support [LOC 93]. Due to the close monitoring and control by the government, many ordinary citizens do not have the privilege of a private telephone line. International connections routed through Moscow and Beijing were available to high-ranking party officials and by 1989 international direct dialing via Hong Kong became available. By 1990 a few public phone booths began appearing in Pyongyang and an agreement had been reached with Japan to share Japan's telecommunications satellites.

Title	The Number of Telephone Lines (Unit: 10,000)			Telephone Lines Diffusion Rate (Unit: %)		
Year	**1983**	**1992**	**1996**	**1983**	**1992**	**1996**
North Korea (DPRK)	54.0	108.9	110.0	2.8	4.8	5.0
South Korea (ROK)	481.0	1559.4	2008.9	12.1	35.7	43.2

Table 2.1: ROK and DPRK Telephone Diffusion Rate Comparison

[From: Ho-Song 01]

Title	The Number of Telephone Lines and Cellular Subscribers per 100 Population		
Year	**1990**	**1999**	**2000**
North Korea (DPRK)	2.46	2.18	2.15
South Korea (ROK)	30.78	96.20	106.01

Table 2.2: ROK and DPRK Main Telephone Lines and Cellular Subscriber Comparison

[From: UN 04]

Year	Country	The Number of Main Telephone Lines and Cellular Subscribers per 100 Population
2002	South Korea (ROK)	116.80
2002	North Korea (DPRK)	2.11
2002	China	32.78
2002	Japan	119.49
2002	Russia	36.23
2002	United States (USA)	113.40

Table 2.3: Sample Main Telephone Line Comparison

[From: UN 04]

Until banned (see below), cellular telephones were becoming more prolific in North Korea, especially in Pyongyang and Rason where they were initially introduced in November 2003. Mobile phone users are reported to be approximately 3,000, as the cellular infrastructure is still in its early stages of development and the costs associated with the sign up and usage fees are extremely high. According to Hwang Chol Pung, president of the Korea Communications Company, plans are underway to extend cellular phone service to all the provinces. The company currently offers various service plans for cellular phones including those for a prepaid system, homepage, and E-mail services connected to computer websites. The cellular phone infrastructure in the DPRK follows the Global System for Mobile Communication (GSM) system, which is a mainstream in Europe. There are plans to introduce the Code Division Multiple Access (CDMA) system, which is currently being used in South Korea [Beal 03].

As of May 25, 2004 all mobile phones were banned in North Korea [AFP 04]. It is widely believed that North Korean officials eager to introduce mobile technology to the reclusive country did not foresee North Koreans being exposed to foreign culture and influences. We have not seen any discussion as to the reinstatement of mobile technology in North Korea.

Figure 2.1: Cellular phone models being sold in the DPRK

[From: DPRKNTA 02]

In 1997 a 27-year contracted joint venture between the Thai company Loxley Public Co. and the Korea Post and Telecommunication Corporation (KPTC) created the Northeast Asia Telephone and Telecommunications Company Limited (NEAT&T) to provide telecommunication services to the Rajin-Sonbong area. NEAT&T intended to provide telecommunication services that covered all ranges of frequencies, communication lines, and media formats in the Raijin-Sonbong Free Economic and Trade Zone. These services include a projected 15,000 user lines, an international gateway, mobile phone services, cross border China and Russia connections, and DPRK long distance services via Chongjin/Pyongyang. The company also planned on the installation of 5,000 new telephone lines, 80 payphones, and cellular service. Although cellular phones and payphones were becoming more popular in Pyongyang, it is still unclear whether NEAT&T completed all their objectives given the embargoes on certain technical equipment, the shortage of power supplies and fuel, and the lack of international banking facilities. In addition, the ban imposed on cellular phones in May 2004 could adversely affect future expansion.

Figure 2.2: Cellular users in the city of Pyongyang
[From: TPK 03]

2. The Internet and the DPRK

With a population of approximately 22.5 million, the reported number of North Koreans currently connected to the Internet remains unknown. As of the year 2000, the DPRK was reported to have only one Internet Service Provider (ISP) and it was state run. Although the DPRK has two assigned Class C Internet Protocol (IP) address blocks with

131,072 addresses and a registered top-level domain (kp), no activity has been reported to originate from these assigned IP addresses. In July 2003 the website http://www.stic.ac.kp was reported to be up [Williams 03]. However, when we attempted to connect to it on several occasions we found it inaccessible.

The majority of the websites associated with the DPRK on the Internet are hosted in Japan, China, and Australia. The DPRK has only a handful of officially state sponsored published websites, all of which are hosted on servers in China and Japan. The DK Lotto (http://www.dklotto.com) and the Jupae Lotto (http://www.jupae.com) websites are the most sophisticated of these websites [McWilliams 03]. Both websites were developed by South Korean entrepreneur Kim Beom Hoon of Hoonnet Co., Ltd, and the DK Lotto website is the only website to have its server physically located in Pyongyang. Other sites are used solely to spread the Party's "juche" message to the masses, with the Korean Central News Agency (KCNA) (http://www.kcna.co.jp) being the most popular. The Korean Central News Agency is the state-run agency of the Democratic People's Republic of Korea that speaks for the Workers' Party of Korea and the DPRK government [KCNA 03].

In May 2002, a South Korean information technology firm operated by businessman Kim Beom Hoon and the state-owned entity Jangsaeng opened the DPRK's first Internet café in Pyongyang. The approximate cost of sending and receiving email is estimated at $10.00 per hour in June 2002, down from $100.00 per hour previously charged in May 2002. Because the average North Korean earns less than $50.00 per month, mainly visiting businessmen, tourists, and diplomats utilize the café's Internet services. Internet service is also provided in some hotels in Pyongyang; again tourists and diplomats are the main users.

Figure 2.3: International email users are becoming more popular in Pyongyang [From: DPRKNTA 02, TPK 03]

3. The DPRK Intranet

North Korea today remains one of the most disconnected and isolated countries in the world. Notwithstanding the DPRK's disconnect from the Internet, it is reported to possess an extensive and well-developed intranet providing connectivity to government offices throughout the country.

The computer became more prevalent in the DPRK in the early 1990's, with local area networks (LANs) being installed in the Party's Headquarters, research laboratories, and several educational institutions. In 1996 the DPRK began developing the Kwang Myong (Bright Star) network using locally developed software that seems to have striking similarities to the Japanese version of Microsoft's Windows operating system. In June 1997 the network was installed at the Central Scientific and Technological Information Agency (CSTIA) and was brought online shortly after. The network features a sophisticated search engine, an electronic information system, a Japanese based web browser, a homepage search engine, television program guides, email functions, a language translation system, and a data transmission system [Conner 01]. The Kwang Myong Network or Intranet contains mostly scientific and technological information and is reported to have more than 30 million documents posted [Conner 01].

Figure 2.4: Researchers using the Kwang Myong Network
[From: TPK 01]

In 2001 it was reported that North Korea's Pyongyang Information Center (PIC) had begun testing a firewall system installed between the Internet and the Intranet in order to screen and control the information being transmitted between the two networks in anticipation of a permanent linking of the two networks in the future. These tests were facilitated by the installation of a superhighway communication device using a "T-Line" installed by Gigalink Limited at PIC. It was also reported that test emails utilizing "kp" email addresses were also conducted [Kwan 01]. In addition, researchers have begun encrypting information being transmitted via the Intranet. It is believed that the encoding is aimed at blocking outside hacking once the Intranet is finally connected to the Internet [Kwan 01].

4. DPRK Electrical Infrastructure

North Korea's electrical infrastructure is so antiquated and in such a state of disrepair that it is difficult to conceive formidable and sustained computer network operations being conducted in the DPRK. Judging from its current state, it is hard to imagine that North Korea had one of the most developed electrical networks in Asia during calendar year 1980. At the time it could generate 25 billion kilowatt hours (kwh)

annually with a capacity of 5.4 million kilowatts (kw). Today the system is obsolete and operates at less than 50% capacity, falling way short of the demand being dictated by the population [FAS 00].

The DPRK's electrical grid is comprised of 62 power plants, 58 sub-stations, and 11 regional transmission and dispatching centers, all operating without the aid of computer systems or automation. As a result, the power system suffers from poor frequency control, poor power factors, and frequent power outages [Hayes 95]. In Pyongyang the power received is usually weak and intermittent, often times dropping from 220 volts to 140-150 volts [Dubrovin 03]. The DPRK has been soliciting additional electrical power from South Korea since the year 2000, but this effort could prove to be futile given the antiquated electrical grid of the DPRK.

Stable and reliable power is needed not only to conduct computer network operations, but also to manufacture the IT systems and components needed to carry out such operations. Until North Korea solves its electricity supply problems, it will be unable to conduct sustained active computer network operations.

Figure 2.5: Satellite picture of Southeast Asia at night
[From: NASA 00]

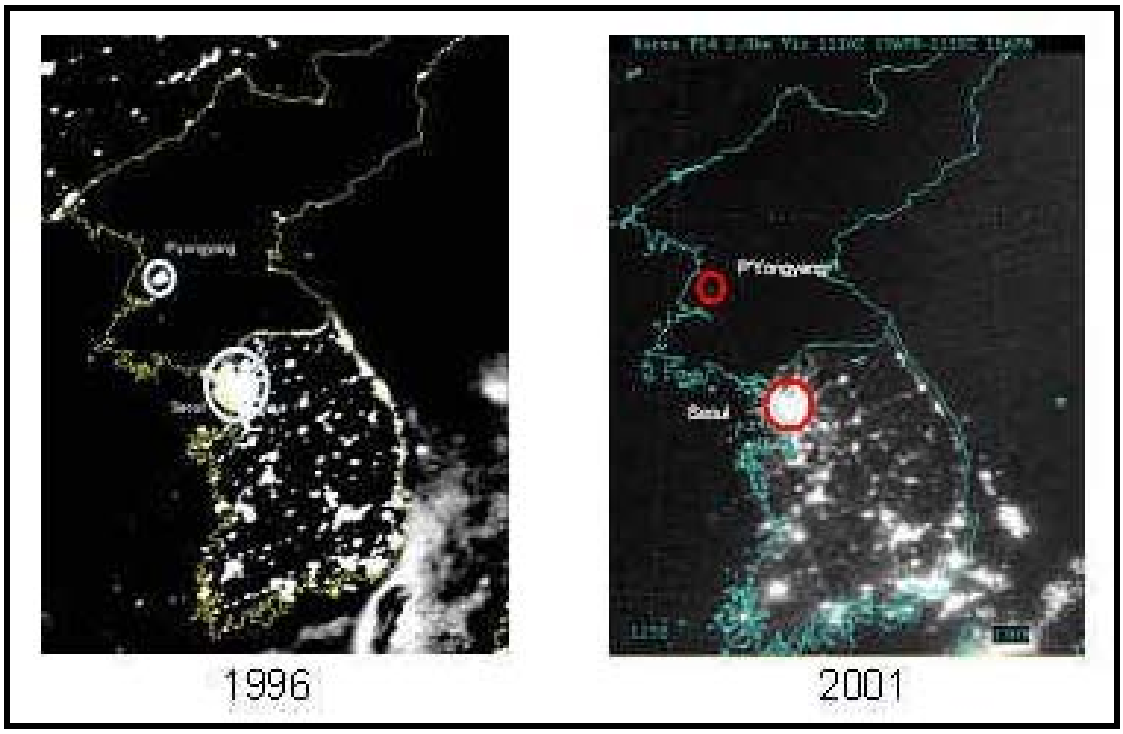

Figure 2.6: Power availability comparison of ROK and DPRK
[After: GS 04]

C. COMPUTER HARDWARE INDUSTRY

North Korea pilot-tested the production of 4-bit computers in the late 1960's. From the 1980's to early 1990's, the Academy of Sciences and the Kim Il Sung University assembled PC-level 8-bit computers. North Korea's hardware production all but stopped when the Pyongyang Electronic Calculator Factory (built in the mid-1990's) was shut down. The hardware sector is technologically dated, with most hardware such as computer systems and communications equipment being imported from China and Southeast Asia [NIS 02].

Although North Korea now spends approximately 3-4% of its Gross National Product (GNP) on science and technology, it still lacks sufficient resources to fully fund a complete computer hardware industry, including large-scale semiconductor production. In May 1992, the DPRK requested funding through the United Nations Industrial Development Organization (UNIDO) to augment the cost of IT research and development. The request for electronic computers in the amount of US$2.4M was used to produce approximately 20,000 units of 32-bit PCs per year.

UNIDO Project Number	Project Description	Requested Funds
DRK/020/V/92-05	Semiconductor parts	US$1.5M
DRK/021/V/92-05	Electronic computers	US$2.4M
DRK/021/V/92-05	Digital controller devices	US$6.0M

Table 2.4: Information Technology Items Requested by the DPRK from UNIDO (May 1992)
[From: ATIP 97]

It is almost impossible to ascertain the exact types and quantity of computers the DPRK currently possesses. However, the case can be made that large-scale imports of computers would be extremely difficult to conduct due to the current Coordinating Committee for Multilateral Export Controls (COCOM) and Wassenaar regulations on dual-use technology imports. The Intel Pentium family of microprocessor and most 80xxx microprocessor-based computers are restricted by these regulations. In 1997, it was reported that the Korean Computer Center (KCC), PIC, and the Kim Chaek Technical University all had Digital Equipment Corporation (DEC) computer workstations and PCs imported through Japan and Singapore [ATIP 97].

The COCOM and Wassenaar restrictions helped to precipitate North Korea's development and production of indigenous hardware and software. The DPRK has successfully developed a Personal Data Assistant (PDA), the Hana-21. Development of the Hana-21 began in 1998 at the Industrial and Technical Corporation (ITC) in cooperation with the North Korean Academy of Science and the Korea Computer Center. The first prototype was a system called "Koryo" which was simply an English-Korean and Korean-English translator taking its input from a pen [TPK 03]. The Hana-21 uses an original Korean operating system (OS) and offers the choice of either Chinese or Korean at startup, which insinuates that the product is also intended for the large Chinese market. The PDA features such applications as a word processor, several dictionaries, and translators, with all characters corresponding to Unicode for greater interoperability. According to the North Korean website The People's Korea, the DPRK released the Hana-21 for sale in late April 2003 and it is priced overseas at 200 Euros [TPK 03]. The local price of the PDA was not available.

Figure 2.7: North Korea's first locally produced Personal Data Assistant

[From: TPK 03]

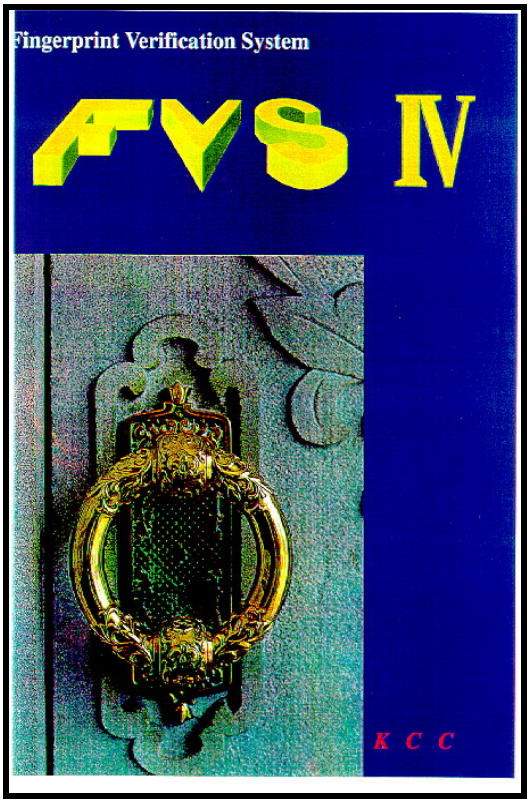

Figure 2.8: FVS IV Biometric System

[From: ATIP 97]

D. SOFTWARE INDUSTRY

Small and medium-sized research institutions such as the KCC, the Pyongyang Programming Center (PPC), and Kim Il Sung University develop a significant portion of North Korea's computer software. Major research and development areas are biometric technology, voice recognition, automated translation programs, game programs such as the Go Game, and multimedia educational programs for children and students. With the exception of the biometric systems, which could be used for CND, none of the publicly disclosed software programs developed by North Korea's software industry is germane to the area of CNO. North Korea is believed to have achieved a certain level of technological capability, although it seems to be unsophisticated in terms of screen composition and appearance [NIS 02].

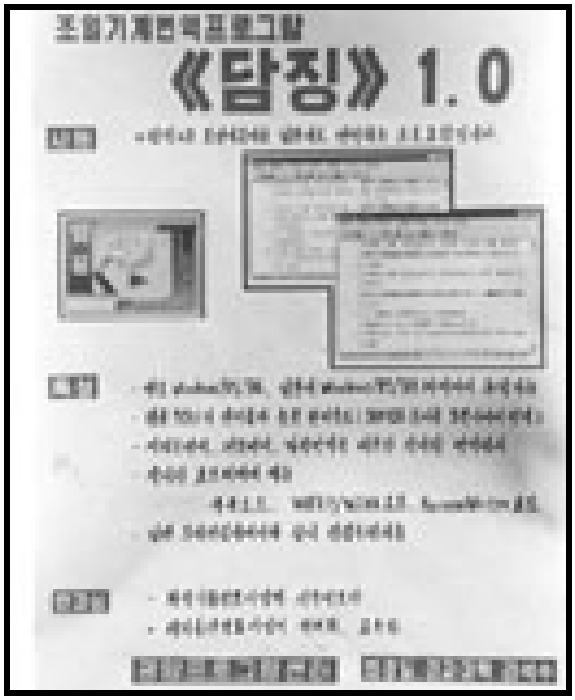

Figure 2.9: "Tamjing", Korean-Japanese Translation Program
[From: TPK 00]

Figure 2.10: Dinga Animation Software Developed in the DPRK

[From: ICAS 02]

The DPRK sponsors the Nation Program Contest that encourages programmers from academia, industry, and the public sector to enter their applications for review and judging. Applications such as a patent information retrieval system that is able to retrieve inventions and patent information from a national computer network and a data storage compression program were among the many contest entries in the past years. Special incentive programs were offered to the award-winning programmers. For example, a high school student receiving the highest award is given the opportunity to enter the college of choice.

Figure 2.11: Visitors observe new software demos at student programming contest

[From: TPK 00]

In 2002, North Korea once again unveiled a plethora of locally developed software at an exhibition in a Beijing hotel. Software ranged from translation applications to video games and were developed using Western software standards for use on Microsoft Windows and Apple Macintosh systems [Artyukov 02].

Figure 2.12: North Korean software exhibits at the World PC Expo in September 2001 [From: TPK 01]

North Korea is also attempting to market its software to the rest of the world through shell companies. PIC-International (http://www.pic-international.com) is a company in Singapore that offers a wide range of DPRK developed software for both the PC and MAC operating systems on its website [Hoff 01]. PIC is and continues to be the primary information technology research institute in North Korea.

E. LAWS AND REGULATIONS

The Internet interface is still in its infancy stage of development in North Korea, and as most of the Western world struggles to reach some consensus on the uniformity of laws and regulations pertaining to Internet use, the DPRK may have a distinct advantage. The DPRK being a communist state has established a plethora of censorship laws

regarding telecommunications. It is assumed that all telecommunications are monitored by the state, and the institutes currently conducting Internet research warrant special attention by censors.

No established laws regarding the use of the Internet were found during the course of this research. Government offices, state research facilities, and state officials utilize almost all of North Korea's computers. All international telephone connections are facilitated through a state run exchange operator, which is also closely monitored. Until individual citizens begin to own personal computers and telephones in greater numbers, there is probably little or no major cause for concern on the part of the state, hence the lack of laws and regulations.

F. SUMMARY

This chapter provided information on the North Korean information technology infrastructure and related services. Additionally, the North Korean IT industry was discussed in great detail. An analysis of the data points gleaned from this portion of the research reveals that North Korea recognizes the importance of IT in a modern world. However, it is readily apparent that North Korea does not possess the necessary infrastructures needed to pose a formidable CNO threat. Although the DPRK has an emerging hardware and software industry, the overall effectiveness of the software and the systems being developed on computer network operations remains questionable.

THIS PAGE INTENTIONALLY LEFT BLANK

III. ACADEMIC ACTIVITY AND PUBLIC COMMUNITY

A. INTRODUCTION

This chapter will examine the involvement of North Korean academia in CNO activities. Educational opportunities made available to civilian students and military members with regard to information technology will also be carefully examined.

B. INFORMATION TECHNOLOGY INFRASTRUCTURE

With the assistance of academia, in 2001 North Korea began publishing and distributing a substantial quantity of publications related to information technology and the sciences. This was an attempt by officials to broaden the knowledge of the average worker and young person with respect to information technology. Information technology was quickly becoming a vital national interest to the DPRK; this realization led to the creation of the Bright Star Network (Kwang Myong), maintained by the Central Scientific and Technological Information Agency (CSTIA). This computer network is dedicated to science and technology. Recent publications applicable to cutting-edge technological developments with commercial value are posted on the network.

The Comprehensive Kumsung Youth Publishing House published a tome entitled "Solving Problems of Computer Intelligence Development" in order to familiarize readers with basic computer terminology and operation. This and many other IT related books were published with the aid of academia aimed at stimulating the minds of young students and increasing the general information technology awareness throughout the regions of the DPRK. However, the vast majority of these publications were simply introductory books and provided no real in depth knowledge of information technology.

C. KWANG MYONG (BRIGHT STAR NETWORK)

When computers began to become popular in North Korea in the early 1990's, research institutions and academia were the first to have them installed. By mid-decade sophisticated LANs were being developed and installed at these institutions. The Bright Star Network was developed in 1996 with the objective of linking the various regional research facilities and academia LANs throughout North Korea. This was the genesis of

what is now the North Korean Intranet, which now reaches more than just academia and research institutions. The government and military are now heavily connected to the Intranet.

The Kwang Myong Network's data is transmitted via fiber optic cable with a backbone capacity of 2.5 GB between the CSTIA and each province. The Central Information Company of Science and Technology, the Invention Offices of Scientific Academies and the People's Study Grand Palace are among the many North Korean government entities that maintain databases on the network. The sign-up fee is free in Pyongyang in order to promote the spread of computer networks [TPK 03].

Prior to becoming the national Intranet, the Kwang Myong's content was limited to science and technology with over 30 million scientific documents posted on the network [Conner 01].

Figure 3.1: Users of the Kwang Myong Network in Pyongyang
[From: DPRKNTA 04]

D. INFORMATION TECHNOLOGY PUBLICATIONS

North Korea first embarked on publishing and distributing considerable volumes of science and technology literature in 2001, with the objective of aiding its workers and young people acquire a broad knowledge in the field of information technology. The May 2001 issue of the state-published youth magazine *Vanguard Youth* reported that the future of the science, technology, and information industries hinges on the performance of the young students. The magazine was quoted to say, "*Young people must study, study, and study to meet the requirements of the times and to improve the standard of science and technology development.*" [NIS 02]

The Comprehensive Science Encyclopedia Publishing House (CSEPH) published *The Basics of Windows Programming and Beginners Visual Basics of Programming Language* aimed at motivating young students to express an interest in computers and increase the general awareness of information systems throughout the country. The Comprehensive Manufacturing Publishing House (CMPH) has also published books such as *Computer Common Sense*, *Glossary of Computer Terminology*, and C*omputer Manual*. In addition to the basic computer publications, information science and technology tomes such as *Numerical-Type Integrated Circuits and their Applications*, *Optical Fiber Communications*, and *Electronic Material Handbook* were published by the CMPH. The Comprehensive Kumsung Youth Publishing House (CKYPH) published computer beginner's guides. These guides included *Solving Problems of Computer Intelligence Development*, a guide intended to familiarize its readers with computers.

The Information Technology Forum for Unification, which consists of 110 South Korean IT professionals, was established in August 2001 to facilitate the exchange of ideas and technical publications with North Korean IT civilians. In late 2001 civilian researchers at the Pyongyang Informatics Center (PIC) requested 250 IT books from South Korea [Soo-min 01]. The majority of the books requested were published between 1999 and 2001 and focused primarily on graphics and virtual animation. Publications on common operating systems and communication methods were also requested, in addition to the books on the multimedia sector and Motion Pictures Experts Group (MPEG) technology. The North Koreans also requested a large quantity of books on language fonts and codes as the DPRK is committed to "Koreanizing" as much information as

possible [Soo-min 01]. Conspicuously absent from the list of requested publications were books relevant to cyber security, suggesting that North Korea was more interested in commercial IT development rather than developing an offensive cyber force.

There are also a few technical periodicals available in North Korea. The scientific magazine *Science World* is a government-sponsored publication that features all the latest information technology and scientific innovations of North Korean scientists and researchers. It was *Science World* that boasted the most recent developments and testing of the country's Intranet.

E. INFORMATION TECHNOLOGY EDUCATION

In 1975 an eleventh grade education became mandatory, and in the early 1990's a primary and secondary education became compulsory. In the 1990's the majority of the instruction provided to students consisted of mathematics, Korean language, physical education, drawing, and music. Today there seems to be an emphasis placed on computer related subjects being taught in the DPRK starting at the grade school level.

It has been stated several times by Kim Jong Il that information technology is the future of North Korea and those who are not actively educating themselves will be left behind. Kim Jong Il himself is known to be an avid user of the Internet and realizes the importance of information technology in today's global arena.

Figure 3.2: North Korean Grade Level Students in an IT Lab
[From: TPK 01]

In an effort to emphasize the importance of IT, North Korea began opening computer science colleges with the Kimilsung University and at the Kimchaek Industrial University

in 1999. In April 2001 the Mankyongdae Student Palace, Pyongyang Student Boy's Palace, and Kumsung First and Second Junior High Schools established specialized curricula designed specifically for young Koreans who demonstrated an aptitude for computer science [Seong-in 01]. Kids at the Mankyongdae Student Palace are being taught basic programming skills with such tools as Visual Basic. In a recent visit to North Korea, former CNN correspondent and Beijing Bureau Chief Rebecca Mackinnon observed students using programming software written in English. It was unclear whether they actually understood the software being demonstrated or whether the entire event was staged for the benefit of the foreigners in keeping with the DPRK propaganda machine.

Figure 3.3: Computer Classroom in the Mangyongdae School Children's Palace [From: NKZONE 04]

Kim Jong Il has now made computer education mandatory in North Korea. Jong Il has stated that there are three basic types of fools in the 21st century: people who smoke, people who do not appreciate music, and people who cannot use the computer [Choe 03]. Today in the DPRK, possessing a computer-related job is a sign of privilege. According to Tak Eun Hyok, a North Korean army defector to the South, "*everyone wants to learn the computer, believing they can get good jobs.*" Computer science now tops the lists of curricula that young military officers and college students wish to study [Choe 03].

Figure 3.4: Instructional Aid for Microsoft Windows in a North Korean Classroom at the Pyongyang 6.9 Middle School
[From: Crowcroft 04]

Plans were being made by a South Korean nonprofit organization to open an information technology college in Pyongyang in cooperation with the DPRK's Education Ministry in 2002. The International Foundation for Northeast Asia Education and Culture says that it had reached a tentative agreement with the DPRK to open the

institution but details still remain sketchy and the status of the institution is unknown [Cohen 01].

In 2001 officials at Syracuse University in New York State developed a scholarly exchange program in conjunction with the DPRK's Kim Chaek University of Technology (KUT) to have seven North Korean civilians study information technology at Syracuse University [Snyder 03]. The bilateral program focuses on the general area of information technology that supports the civilian sector IT infrastructure in the DPRK. Researchers from KUT studied various programs which included secure fax programs, digital libraries, machine translation programs, decision support, watermarking programs, graphic communication via personal digital assistants, and the implementation of IT in various public sectors on their most recent visit to Syracuse [ASPAC 03]. Computer security was not among the list of topics studied by the visiting North Korean students. This collaboration is the first of its type between the two countries and Syracuse University intends on continuing the student exchange program. Officials in charge of the program were contacted for further comment, however they refused to release any additional information associated with the exchange program.

Figure 3.5: Kim Chaek University of Technology and Syracuse University Officials [From: ASPAC 03]

The IT education of the KPA is shrouded in more secrecy than public IT education. Very little is known about the IT education of the KPA, however, the Asia-Pacific Center for Security Studies (APCSS) reported that the KPA is rapidly evolving into a "modestly digitized" army [APCSS 02].

F. NORTH KOREAN ACADEMIA AND IT RESEARCH

There are three major academic research institutions in the DPRK actively involved in the discipline of information technology. The three institutions are the Pyongyang University of Computer Technology (PUCT), Kim Chaek University of Technology (KUT), and Kim Il Sung University.

1. Pyongyang University of Computer Technology (PUCT)

Pyongyang University of Computer Technology was founded in 1985 and since its inception has produced over 4,000 Computer and IT engineers. The three-year university has a faculty that specializes in computer and information technology and its graduates are now playing a vital role in the development and production of information technology in various sectors of the DPRK's national economy [KCNA 02].

2. Kim Chaek University of Technology (KUT)

Kim Chaek University of Technology (KUT) was originally part of the Kim Il Sung University before it was established as the Pyongyang College of Technology in 1948. The university boasts 10 research institutes and 54 laboratories with a student body of approximately 10,000 and a faculty of approximately 2,000 [MIIS 03]. KUT is well known for its development of various software and artificial intelligence. Faculty members are often solicited to provide information technology lectures to high-ranking Party officials [TPK 01].

Figure 3.6: The DPRK's hopeful engineers and scientists being produced at the Kim Chaek University of Technology
[From: TPK 01]

The North Korean website *The People's Korea* reported in 2001 that KUT has been training engineers who will contribute to the future development of the DPRK's information technology. The Computer Engineering department at KUT is planning on the introduction of state-of-the-art technology needed to modernize computer facilities related to economic construction. The present task at KUT is to upgrade its voice recognition technology to a world-class level [TPK 01].

3. Kim IL Sung University

Kim Il Sung University was established in October 1946 at the foot of Moran Hill. It is the DPRK's first university and today it serves as a model for other universities throughout North Korea. It has approximately 10 institutes consisting of electronic computers, cell engineering, and atomic energy with more than 1200 distinguished faculty members [KCNA 96].

Figure 3.7: War-damaged Kim Il Sung University in 1953
[From: KCNA 96]

Kim Il Sung University has an extensive and challenging computer science curriculum offering a plethora of computer programming courses. The faculty has developed and produced several software products, including the program protection software Intelligent Locker, Worluf Anti-Virus, a Chinese character editing program, War Game, and Simanas, a simulation and analysis program for engineering problems [ATIP 97].

G. SUMMARY

This chapter examined the extent of North Korean academia's participation in the development of information technology and CNO activity. Although at times it was difficult to discern the distinction between academia and state agency, it was determined that several academic institutions play an integral role in the accomplishment of the DPRK's overall IT strategic objectives. Many of these institutions are developing and producing state-of-the-art software for both the domestic and international market. It was

unclear whether or not these institutions were actively participating in CNO activities sponsored by the DPRK. It was also unclear whether or not these institutions were engaged in the development of software relevant to CNO. There is strong evidence that North Korea academia is heavily involved in information technology development but nothing conclusive to suggest that these institutions are involved in CNO activities.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EXTERNAL INFORMATION TECHNOLOGY AID

A. INTRODUCTION

This chapter explores the information technology aid provided to North Korea. It also briefly discusses the export restrictions that apply to North Korea.

B. DPRK'S MAJOR IT CONTRIBUTORS

Despite the technological advances being made in the area of information technology, much of North Korean current information technology is acquired from other nations willing to provide the neo-isolated state with the technology.

1. India

India has been one of the DPRK's largest contributors of information technology, providing training to North Korean information technology professional at the Indian Institute of Technology in Dehli [Hayes 02]. The Indian technology firm Electronic Trade and Technology Development Corporation (ETTDC) was awarded a $5.9 million contract by UNIDO in 1981 to supply information technology equipment to North Korea. The firm was primarily selected for the contract because it had experience circumventing COCOM restrictions and was planning on using western suppliers [Hayes 02]. The bulk of ETTDC's UNIDO contract was to build North Korea's first IC plant and provide the required training needed to operate the plant. However, due to a language barrier the training was grossly insufficient and the plant was only able to produce limited numbers of ICs. Our research did not uncover any IT contributions from India beyond those of ETTDC.

2. China

China continues to be one of North Korea's staunchest allies and provides a significant amount of information technology aid to the DPRK. North Korea's limited email service provided by www.silibank.com is being facilitated through an Internet connection in China. Kim Jong Il was reported to have visited China twice to closely

study China's information technology reforms. He was also reported to have visited Legend Computers, Ltd. in Shanghai [KN 01].

North Korea proudly exhibited its newly developed software products at the North Korea Computer Software Expo in Beijing in April 2002. The DPRK is also a regular participant in the Chinese annual computer trade show Comdex.

3. Russia

Our research did not find any information with regard to the type and quantity of information technology aid officially provided by Russia. However, after more than a decade of strained diplomatic relations, North Korea has resumed a dialogue with Russia. In 2001 a North Korean Defense Ministry delegation visited Russia to discuss military cooperation and military industrialization [PD 01].

4. Japan

The aid provided by Japan is more indirect in nature. Although trade talks between Japan and the DPRK have resumed, Japan continues to honor the COCOM and Wassenaar regulations. However, Japan hosts a large number of the DPRK's official websites used to spread the Party's message. Several of the DPRK's official websites originate from websites with a .jp top-level domain name. As noted earlier, the KCNA, which is North Korea's most prominent website, is hosted in Tokyo by the Korea News Service (KNS). Japanese officials must be aware of the IT services being provided to the DPRK, however this research has not been able to uncover any evidence that Japan is taking steps to prevent such actions.

5. South Korea

South Korea has one the world's highest computer diffusion rates. Although tensions still exist between the DPRK and the ROK stemming from North Korean Internet gambling sites being fed into the South, South Korean IT businesses are eager to invest in the underdeveloped North Korean IT industry. Several South Korean businesses have made major investments in the North Korean IT infrastructure.

In 2001 construction began on the first inter-Korean IT facility in North Korea, Koryo Business Town. The South Korean IT firm, Ntrack, in cooperation with the North, planned on building a 17,820 square meter IT complex in Pyongyang, with enough space for over 2,500 North Korean IT workers. The complex will be home to a 1,650 square meter IT research facility specializing in animation and web products [Nautilus 01]. An inter-Korean joint venture company was also launched in 2001 in Dandong, China. The Hana Program Center was established on May 10, 2001. This was reported as the first time that workers from both North and South Korean IT industries met to market software [Seong-in 01].

The South Korean multimedia and IT firm BIT Computer Corporation announced in June 2001 that the company would be providing a satellite Internet link between the shut-in country and the rest of the world. As part of the inter-Korean deal, BIT Computer Corporation will be the sole supplier of satellite Internet equipment in North Korea for five years. In addition, BIT was also in the process of providing IT training to North Korean personnel via the Internet at www.bitcampus.com. According to BIT president Cho Hyun-jung, the company will also provide the Choson Computer Center with IT books and manuals and emphasize that the entire venture is being conducted with the expressed approval of Kim Jong Il [CDES 01].

In June 2004 at the request of North Korea, a group of North Korean officials toured SK Telecom, South Korea's largest mobile carrier, and Samsung Electronics, South Korea's largest manufacturer of memory chips. This visit would imply that the North is looking to the South for ideas in expanding its own fledgling IT sector given the South's success with IT growth in the last decade. Computer technology has been a top priority in the North for several years now, and Kim Jong Nam, the eldest son of Kim Jong Il, is leading the campaign to arm its military with state of the art information technology [WT 04].

Officially, South Korea still bans the export of Pentium© class computers to North Korea. Many in Seoul fear the possibility of equipping the enemy with equipment and skills that could be easily directed at them.

C. COCOM AND WASSENAAR RESTRICTIONS

In an attempt to restrict trade with the former Soviet Union and the Warsaw Pact countries, the United States and its allies created the Coordinating Committee for Multi-lateral Export Controls (COCOM) in 1949. By November 1993 COCOM had outlived its usefulness and had become inadequate. At a meeting in The Hague, the 17 COCOM members agreed to terminate COCOM and establish a new multilateral arrangement. The Wassenaar Arrangement (WA) formerly replaced COCOM in July 1996 [UNVIE 04]. The 33 founding members of the Wassenaar Arrangement are: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Republic of Korea, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, Romania, the Russian Federation, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States. The WA restrictions were considered to be a more proficient tool to deal with the export of both conventional munitions and dual-use goods and technology to non-member nations.

According to a U.S. State Department release in 1996, the purpose of the Arrangement reflected in the Initial Elements agreed to at the meeting is to contribute to regional and international security. This is accomplished by promoting transparency and greater responsibility with regard to transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations; seeking, through national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals and are not diverted to support such capabilities; complementing and reinforcing, without duplication, the existing control regimes for weapons of mass destruction and their delivery systems, as well as other internationally recognized measures designed to promote transparency and greater responsibility, by focusing on the threats to international and regional peace and security which may arise from transfers of armaments and sensitive dual-use goods and technologies where risks are judged greatest; and, enhancing cooperation to prevent the acquisition of armaments and sensitive dual-use items for military end-uses, if the situation in a region or the behavior of a state is, or becomes, a cause for serious concern to the Participating States [USDOS 96].

This arrangement will not be directed against any particular state or group of states and will not impede bona fide civil transactions. Nor will it interfere with the rights of states to acquire legitimate means with which to defend themselves pursuant to Article 51 of the Charter of the United Nations [USDOS 96].

North Korea and its staunch ally to the North, China, are noticeably not signatories to the WA, which bars IT-related export to North Korea. The WA classifies North Korea as a terrorism-sponsoring nation, prohibiting the export of dual-use technologies to the nation. Under the current guidelines of WA the export of digital computers to North Korea having a composite theoretical performance (CTP) exceeding 190,000 millions of theoretical operations per seconds (MTOPS) is strictly prohibited without the issuance of a license. Additionally, the licenses are not issued to military or state entities in the DPRK and are routinely denied [WA 03]. The U.S. Department of Commerce (DOC) enforces even stricter guidelines regarding the export of computer technology to North Korea. The DOC mandates that a license be issued for the export of digital computers having a CTP exceeding 6 MTOPS or microprocessors with a clock frequency rate exceeding 25 MHz. Furthermore, the DOC restricts the export of the very technology needed to manufacture microprocessors and computers. Any computer containing U.S. technology is also restricted [DOC 04]. Despite both COCOM and WA restrictions and countless U.S. sanctions on dual-use technologies, North Korea has managed to acquire more basic computing power than the United States possessed during the Manhattan Project. The restrictions and sanctions have merely slowed the quantity and timing of production of computer and related equipment provided to economic actors throughout the country. The leading members of the Party and various high-level government officials have always had access to current or next generation computers [Seong-in 01]. The level of advancement made in such areas as nuclear power, satellite, and missile technologies indicated that the DPRK possesses sufficient computing power to accomplish complex operations. This should not come as a surprise as the Asia-Pacific Center for Security Studies reported in 2001 that Chinese-made Pentium computers are already in North Korea [Seong-in 01].

D. THE NORTH KOREA-CHINA RELATIONSHIP

The relationship between North Korea and China has evolved over time. China has long been an outspoken ally of North Korea and supported them during the Korean War. During the period of 1973-1984, China's support for North Korea increased steadily amidst a significant decline in Soviet support [LOC 04].

In the aftermath of the Tiananmen Square incident in 1989, Pyongyang supported Beijing's response to the incident. By the early 1990s, the relationship between North Korea and China had grown much warmer. However, although Pyongyang and Beijing become closer allies, Beijing has not transferred any major weapons systems to North Korea.

Kim Jong Il has made several visits to China in the recent years in an effort to bolster the relationship between the two countries. North Korea recognizes the magnitude of the Chinese IT market and as a result most software programs developed in the DPRK target the vast Chinese market. North Korea is a regular participant in the Chinese IT expos and Beijing played host to a North Korean software exhibition in 2002. In 2004 North Korea established a software development facility in the Chinese province of Shenyang.

Although it was reported by the Asia-Pacific Center for Security Studies that Chinese-made Pentium computers were present in North Korea, the quantity is unknown. It is also unclear as to the type and quantity of IT equipment exported from China to North Korea. Given the fact that China is not a participating member of WA, it would not be unfair to speculate that China has provided North Korea with the necessary IT equipment and training needed to improve its IT infrastructure and CNO prowess. China's IT sector is considered comparable to the United States' and following the assumption that China and North Korea are engaged in the free trade of information technology, the WA is not dramatically hindering North Korea's IT development and growth.

E. THE CHINESE IT INDUSTRY AT A GLANCE

According to the State Development and Reform Commission (SDRC), China has developed the world's third largest manufacturing industry of electronic and IT products

surpassing that of Japan. In 2003, China's IT manufacturing industry reported sales revenues totaling US$227 billion, a 34 percent increase from the previous year. China's export of desktop computers is estimated to reach 20 million units by 2007, rising from 2003's exports of 11.21 million units [China 04].

China built its first computer based on a Soviet model in 1958. In the late 1970s, China began producing computers for commercial and industrial uses soon after microcomputers were in production. The newly manufactured computers relied heavily on imported components and were developed in small quantities [Kraemer/Dedrick 02]. Today, China's IT sector is relatively advanced and produces a wide range of products for both export and domestic use. PDA's, PC's, monitors, CPU's, and a myriad of peripheral devices are among the many IT products being produced by China. With such a large and cheap labor market, several PC manufacturers have established several joint ventures with Chinese IT companies. Hewlett-Packard, Toshiba, and Compaq have formed joint ventures with local companies to market their own products and gain access to local distribution channels [Kraemer/Dedrick 02]. Companies like IBM, Dell, Acer, and Siemens have launched IT ventures of their own in China, manufacturing desktop and notebook PCs, monitors, storage products, motherboards, servers, networking equipment, and various peripheral devices. Table 4.1 lists the major foreign PC makers, their Chinese joint venture partners, and their products.

Foreign company	Joint venture (JV) or wholly owned (WO)	Chinese partner	Products, operations
IBM	JV	Great Wall	Desktop and notebook PCs, storage products, motherboards
	WO		Servers
Compaq	JV	Stone Group	Desktop PCs
	JV	Star Group	Notebook PCs
Hewlett-Packard	JV	Legend	Desktop PCs, inkjet printers
Dell	WO		Desktop and notebook PCs
Acer	WO (3 separate units)		Monitors, peripherals, motherboards, software, networking equipment
Toshiba	JV	Tontru	Servers
NEC	JV	N/A	Desktop PCs
LG Electronics	JV	Tontru	Monitors
Siemens	WO	N/A	Desktop PCs

Table 4.1: Major Foreign PC Companies Activities in China
[From: Kraemer/Dedrick 02]

Nine years ago the Asian Technology Information Program (ATIP) reported that computer applications were still in an early stage in China. China had managed to develop some supporting software and applications software, such as spread sheets, accounting software, word processors, desktop publishing, CAD/CAM, multimedia, Chinese operating systems, and antivirus applications [ATIP 95]. Today China is concentrating its software research and development in machine translation, Chinese character recognition, voice composition, automatic code generation, distributed processing systems, parallel processing, and pattern recognition [Joseph 02]. In 2001, Chinese government officials projected that the country's software exports would be approximately US$1.5-2 billion by 2005 [AU 03]. We were unable to find any evidence that China is engaged in the research and development of software programs pertinent to computer network operations. The fact that there is no evidence of such CNO tools does not negate the fact that China has been accused of conducting CNO activities against other states, nor does it mean that China may not be developing CNO tools that we did

not uncover. Moreover, there is ample evidence that Chinese military theorists are well aware of the potential value of CNO [Thomas 00].

Figure 4.1: Basic Chinese IT Rankings

[From: AU 03]

F. CHINESE CNO ACTIVITIES

Although the U.S. and China officially deny the idea of Chinese state sponsored cyber warfare against Taiwan or the U.S., the Central Intelligence Agency (CIA) believes that the Chinese military is currently researching ways to disrupt targeted civilian and military computer and infrastructure systems using virus attacks. A CIA assessment likened China's virus attack abilities to those of technically advanced hackers, however, these abilities are currently limited to temporarily disabling sectors of Internet users [Lyman 02].

China has never publicly stated its involvement in CNO activities against its adversaries. However, the exploits of Chinese hackers are well known on the Internet.

Soon after the 1999 accidental bombing of the Chinese embassy in Belgrade, Chinese hackers unleashed a barrage of computer network attacks and exploitation against various U.S. government systems. Intruders claiming to be from Mainland China defaced the websites of the U.S. Departments of Energy and Interior, among others. The webpages displayed the message "We are Chinese hackers who take no care about politics". Officials reported that the hack of the Interior Department was definitely traced back to China [Messmer 99]. In 2001, Business Week reported that Chinese hackers had infiltrated several U.S. government websites to express their outrage regarding the collision of a U.S. EP-3 surveillance aircraft with a Chinese fighter. The U.S. Labor and Health and Human Services Departments were both victims of website defacement [France 01]. The Chinese hacker group Honker Union of China claimed responsibility for several of the webpage defacements [Ward 01].

Figure 4.2: A Message Reportedly Used by Chinese Hackers
[From: Ward 01]

In July 2004, South Korea's spy agency the NIS confirmed the identities of Chinese hackers who were suspected of attacking the computer systems of 10 South Korean government agencies. According to the NIS, one of the Chinese hackers was enrolled in a Korean language class at a foreign language school in China that has been run by the Chinese People's Liberation Army since 1986 [Song-wu 04]. The Japanese newspaper Mainichi Shimbun reported in August 2004 that a group of Chinese hackers had launched an attack on about 200 Japanese and Taiwanese websites. The group

reported posted messages on its website calling for people to attack Japanese servers [MDN 04].

Chinese hackers are becoming more imaginative with their activities and are now offering made to order virus services. The Chinese anti-virus software firm Rising PR reported that Chinese hackers are upgrading existing viruses enabling them to subvert anti-virus applications [CCRC 04]. North Korea could very well be taking advantage of these services being offered by Chinese hackers.

G. SUMMARY

This chapter examined the information technology aid provided to North Korea. The COCOM and Wassenaar restrictions and their effectiveness were also examined highlighting the restrictions placed on North Korea's import of dual-use technology. Additionally, an overview of China's IT industry was discussed as China is not a signatory of the COCOM and Wassenaar restrictions. Hence, North Korea would potentially have access to Chinese IT products.

THIS PAGE INTENTIONALLY LEFT BLANK

V. GOVERNMENT ACTIVITY

A. INTRODUCTION

This chapter examines whether North Korea includes CNA/E in its military doctrine and whether it is training cyberwarriors. It also examines the state run companies involved in information technology and state propaganda on the Internet.

B. GOVERNMENT ENTITIES INVOLVED IN DPRK IT DEVELOPMENT

Within the last decade, North Korea has expressed a keen interest in the IT sector. North Korea's interest in the IT sector is directly related to its goal in constructing Kangsong Taeguk, a powerful nation [Seong-in 01]. More focus has been placed on IT development since Kim Jong Il assumed power and according to the North Korean Central Television Broadcasting Station in May 2001, "Kim Jong Il promises a bright future for the IT industry".

In March 2004, North Korea established the "Korea 6•15 Service Office in Shenyang" in the Liaoning Province of China. The software producer is the first of its kind in Shenyang, and the home offices of the "Korea 6•15 Editing Corporation" in the DPRK closely control its operation. The company plans on developing programs for the printed media and will offer specially tailored software based on its customer's requests. Korea 6•15 announced that it would provide software that satisfies the demand from Chinese consumers at competitive prices [LKD 04].

Today in the DPRK there are seven key research institutions focusing on information technology. These institutions are primarily responsible for the significant progress made by North Korea in the information technology sector. The four primary research institutions actively pursuing information technology are Pyongyang Informatics Center (PIC), Korea Computer Center (KCC), DPRK Academy of Sciences, and Silver Star Laboratories (UNBYOL).

1. Pyongyang Informatics Center (PIC)

The PIC was established on July 15, 1986 with the purpose of developing computer-based modern management techniques. The PIC was also to aid in the

formation of a Computer Group, whose purpose was to promote the use of computers by government and industry [Hayes 02]. Today the PIC employs over 200 qualified software engineers whose average ages is 28 years with 1.5 computers per person [Park 01]. The PIC primarily focuses on software development and is responsible for the development of the General Korean Electronic Publication Systems, 3D CAD, embedded Linux software, web applications, interactive programs, accounting software, and more recently virtual reality software. It is reported that the PIC is responsible for developing the filters to be used between the Kwang Myong Intranet and the Internet.

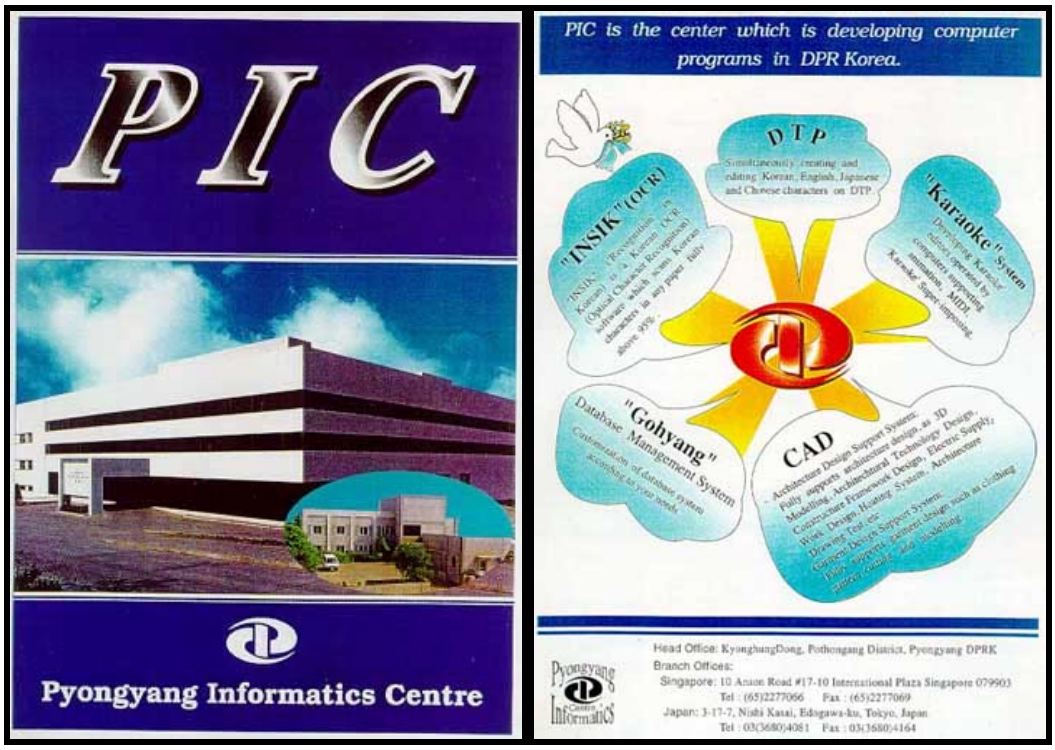

Figure 5.1: Pyongyang Informatics Center
[From: Hayes 02]

The PIC was described as well endowed with computer hardware and strong in software generation [Hayes 02]. In 2001, the PIC's primary software programs were highlighted at the Pyongyang Computer Program Expo.

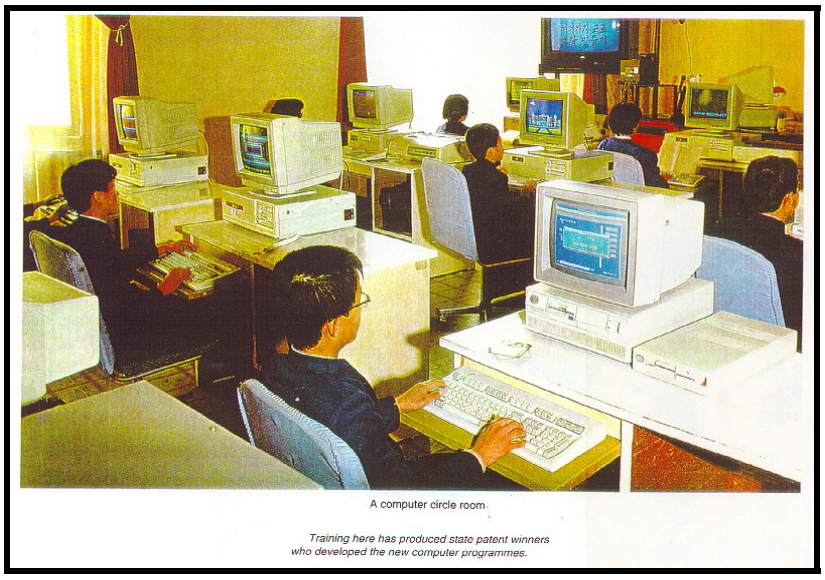

Figure 5.2: Programmers at the Pyongyang Informatics Center

[From: ATIP 97]

2. Korea Computer Center (KCC)

The KCC was established in 1990 by Kim Il Sung to promote computerization in the DPRK. At its inception, the KCC employed approximately 800 employees who appeared to have an average age of 26 [Larmer 04]. Today Kim Jong Il's son Kim Jong Nam, who also heads North Korea's intelligence service, the State Security Agency (SSA), heads the KCC. Kim Jong Nam is also the chairman of North Korea's Computer Committee. In May 2001 the South Korean newspaper *The Chosun Ilbo* reported that Kim Jong Nam had moved the SSA's overseas intelligence gathering unit, which operates primarily by hacking and monitoring foreign communications, into the KCC building. In 2001, South Korean media reported that the KCC was nothing less than the command center for Pyongyang's cyber warfare industry, masquerading as an innocuous, computer geek-filled software research facility [Larkin 01].

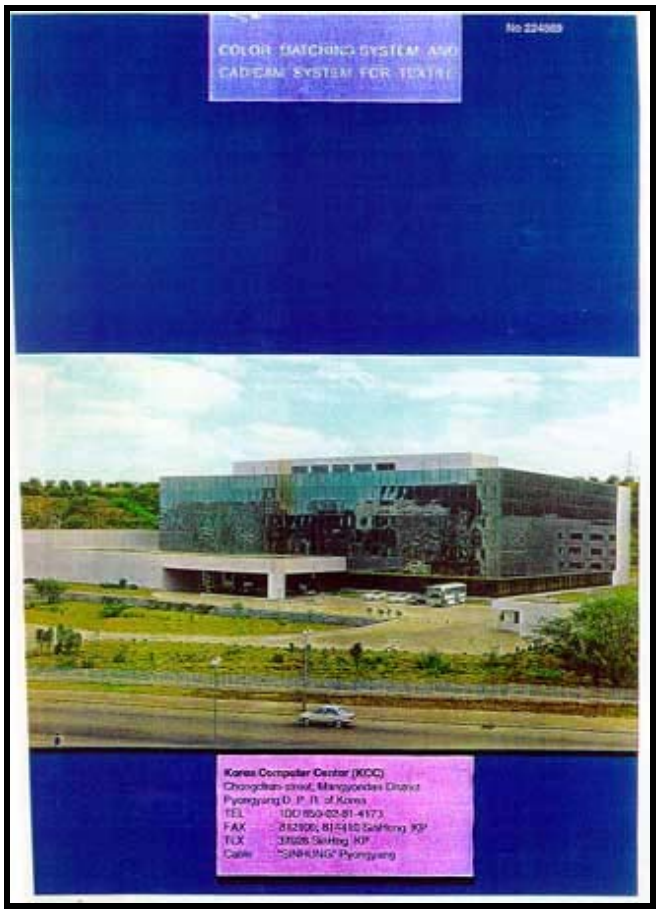

Figure 5.3: Korea Computer Center
[From: TPK 00]

The KCC now develops some of North Korea's cutting edge software, which includes voice recognition systems, fingertip identification systems, and artificial intelligence systems. In the year 2000, researchers at the KCC successfully created a Korean version 1.0 of the Linux operating system. The KCC has also developed a Korean typewriting program that interfaces with Windows and Mac operating system for use in offices throughout the country. The program was named "Our Company" and enables North Koreans to input Korean text in Windows and Mac OS applications [TPK 01].

For the past several years the KCC has dominated Japan's annual FOST competition, a tournament for computers playing Chinese chess [AP 03]. The KCC exports much of its software through its Beijing office and is currently contracted by several South Korean companies to provide a wide range of software. It was reported by

an official at South Korea's Samsung, who paid $730,000 for five KCC-developed programs, that the KCC programmers do not have a lot of access to the outside world, but their fundamentals i.e., basic knowledge in computing and software are very strong [Larimer 04].

Figure 5.4: Programmers inside the Korea Computer Center
[From: TPK 01]

3. DPRK Academy of Sciences

Established in 1952 as the Ministry of Science and Technology, the Academy of Sciences provides leading scientific research work and unified guidance on national scientific and technical administrative work [UNDP 00]. Located in the Eunjong District of Pyongyang, the Academy of Sciences' most basic mission is to produce scientific and technologies research and development. The Academy has produced such software programs as Pidulgi, a multilingual conversation study program; Mae a Korean language optical character recognition (OCR) program; Mangnami-kong, an artificial intelligence development program; and Mujigae, a Japanese-English translation program [TPK 00]. Due to a lack of research funding, the Academy of Sciences research has become

dismally limited with more of an emphasis being place on physics and mathematics instead of information technology [NIS 02].

4. Silver Star Laboratories (Unbyol)

The Silver Star Laboratories (SSL) was established in 1995 under the Korean Unbyol General Trading Corporation. According to Kang Yong Jun, the director of SSL, the average age of the researchers at SSL is 26 years, with most graduating from Kim Il Sung University and other distinguished universities across the country. Prospective employees are usually graduates of the Pyongyang Senior Middle School No.1, a genius-training center.

SSL has developed such programs as Silver Mirror, a remote control program, communications, and artificial intelligence software. SSL also produces several language recognition programs and multimedia software, in addition to taking special orders from foreign companies [KCNA 98]. The SSL won the championship at the fourth and fifth annual FOST Cup World Computer Go Championship competitions held in 1998 and 1999, respectively [Park 01].

C. MILITARY DOCTRINE

In order to provide an accurate representation of the CNO threat posed by North Korea, a careful analysis of the DPRK's current military doctrine should be conducted. The Korean People's Army (KPA) has long had ties to China and the former Soviet Union. China is well known for developing a capable cyber attack program. It is presumed that the KPA and the myriad of North Korean intelligence gathering agencies have an understanding of their adversaries' capabilities if not a rudimentary information warfare (IW) capability [BBC 02]. It was reported in 2002 by Richard Clarke, Special Advisor to the President for Cyberspace Security under the Clinton and Bush administrations, that North Korea was one of the nations "developing information warfare units, either in their military, or in their intelligence services, or both" [Clarke 02].

The quantity of the information on North Korea's military doctrine is sparse, however, the KPA's reported overall objective is to "disturb the coherence of South Korean defenses in depth including its key command, control and communications, and

intelligence infrastructure" [GS 02]. Although the DPRK has no published official doctrine specifically addressing its CNO capabilities or intentions, information gleaned from several open source data points implies that CNO is of great interest to the North Korean military. The KPA has expressed a desire to upgrade its existing force infrastructure to support the existing strategic objectives of credible deterrence. This was a result of the KPA analyzing recent U.S. military operations in which IT played a major role [Minnich 01]. After more than 10 years North Korea resumed high-level military talks with Moscow, a move that suggests that the DPRK is attempting to acquire Russian hardware and software upgrades. Kim Jong Il is also an outspoken proponent of information technology and is fully aware of the implications associated with the use of CNO.

D. TRAINING CYBERWARRIORS

Determining a state's participation in CNO activities can prove to be a daunting task often times producing dubious results. Proving the North Korean government's direct or indirect involvement in CNO could prove to be even more difficult given the level of secrecy exercised by the Kin Jong Il regime.

In 1984 during what can be considered as North Korea's technological revolution, the Mirim Academy was established in Pyongyang's Sadong district. The academy matriculated the top students from the Air Force Academy and other military services for an intense two-year program in information technology and electronics warfare. In 1986 Mirim Academy officially became a five-year college and was renamed the Mirim College and relocated to a new location in the mountainous Hyungjaesan district. Instead of admitting only military service members, the newly formed Mirim College now admitted highly intellectual enlisted servicemen and the top percentile high school students from each of the country's provinces. The North Korean populace now knows Mirim College as the Automated Warfare Institute (AWI) or the University of the Gifted. It offers such curriculums as command automation, computers, programming, automated reconnaissance, and electronic warfare. Sub-specialties such as computer calculation, information transmission, and development of codes are also offered [NIS 02].

South Korean officials have long speculated that the Automated Warfare Institute was being used to train and produce a new type of soldier, the cybersoldier. Since the mid 1990's South Korean military and intelligence officials have been sounding the alarm as to the activities at the Automated Warfare Institute. Since its inception in 1984, the Automated Warfare Institute allegedly has been steadily producing up to 100 cybersoldiers each year, trained in such disciplines as virus creation and network penetration [AP 03]. Given the fact that North Korea spends 31.3% of its gross domestic product (GDP) on defense, and is working arduously to modernize and digitize its military, cyber-warfare does not seem so far fetched.

In early 2003 South Korea's Internet service was brought to a near standstill due to the introduction of a virus-like computer infection into its network [AP 03]. South Korea lacked credible evidence that North Korea was responsible for the denial of service attack, but still suspected that the DPRK was responsible.

It has long been suspected that the Chinese military has been researching ways to disrupt targeted military and civilian computer and infrastructure systems using virus attacks [Lyman 02]. To assume that China's technical knowledge of CNA/E was passed on to North Korea is not an unfair assumption. However, we did not uncover any evidence of China supplying North Korea with any weapons systems. China is now actively involved in negotiations to halt North Korea's nuclear weapon development.

E. THE INTERNET AND NORTH KOREAN PROPAGANDA

The North Korean government is fully aware of the implication the Internet has on modern society. As it is often reported, Kim Jong Il is a prolific Internet surfer and fully understands the impact of getting his message out on the information superhighway.

There are several websites dedicated to disseminating the Party's message all of which are hosted outside of the DPRK. The most prominent would be that of the Korean Central News Agency (KCNA) (http://www.kcna.co.jp). Founded in 1946, the news agency developed its official website in 2002 for the distribution of North Korean news and events. Although the website is hosted by the Korean News Service (KNS) in Tokyo, the KCNA website states that the state-run agency is located in the capital city of Pyongyang with branches located all over North Korean and some foreign countries

[KCNA 03]. The website is overwhelmingly anti-U.S., which is evident by numerous articles posted representing the DPRK's version of world events involving the U.S. The KCNA website also features an extensive archive of articles organized by month dating back to December of 1996. It is readily apparent that the purpose of this website is to spread the DPRK's propaganda to the rest of the free world as the overwhelming majority of the country citizenry has no access to the KCNA website.

Figure 5.5: KCNA Website

[From: KCNA 04]

The People's Korea (http://210.145.168.243/pk) is another North Korean sponsored website that spreads the country's propaganda abroad. Located in Tokyo, The People's Korea provides an extensive collection of articles on a wide range of topics. There were several important data points gleaned from this website with regard to North Korean IT innovations and new products.

Figure 5.6: The People's Korea Website

[From: TPK 04]

The People's Korea website also contained a link to the DPRK's sponsored information website, the DPRKorea Infobank (www.dprkorea.com). The DPRKorea Infobank website was launched with the assistance of the Hong Kong based Pan Economic Development Association of Korean Nationals in October 1999. The launch was timed to coincide with the 51st anniversary of the founding of the Worker's Party of Korea. The website provides instant access to government related news on the economy, culture, sports, and tourism. The site also claims to provide an online shopping service for Korean books, stamps, and goods. Although the site has been under construction for several months there are signs of service improvement.

Figure 5.7: DPRKorea Infobank website

[From: DPRKI 04]

In November 2003 North Korea unveiled its newly developed official website, Naenara-DPRK (http://www.kcckp.net/external_e/). The website was created and is managed by the Korean Computer Center (KCC). Further investigation revealed that the website was registered to PSI-USA, Inc., however the location of the web-server was unknown.

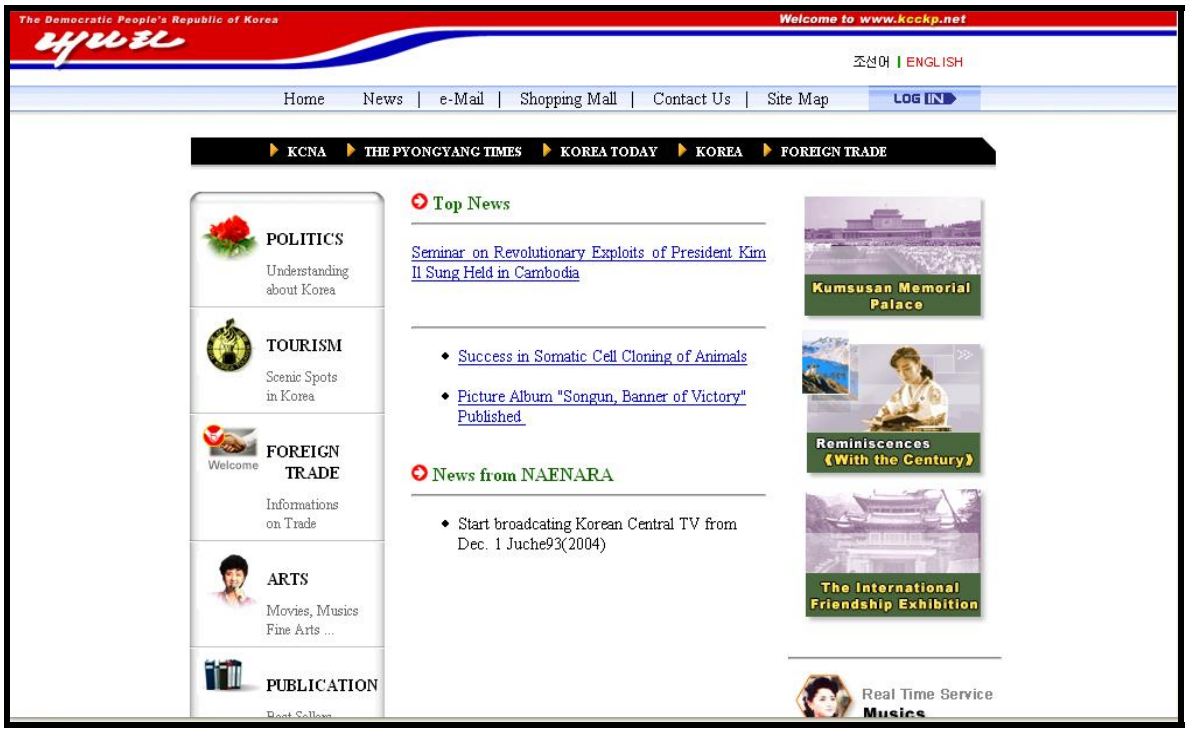

Figure 5.8: Naenara-DPRK website
[From: KCC 03]

F. SUMMARY

This chapter examined the involvement of the North Korean government in the IT sector along with its participation or sponsorship of CNA/E activities. In addition, North Korea's military doctrine with regard to CNO was examined. Although no credible evidence was found indicating the direct involvement of the DPRK's government or military in CNA/E activities, it would be fair to assume that the DPRK senior leadership considers CNO to be an integral component of modern warfare.

This chapter also discussed the various North Korean government research institutions conducting research and development of modern IT products and systems. The growth of IT in North Korea was examined and it was found that North Korea's IT sector is growing at a phenomenal rate.

VI. COMPUTER NETWORK ATTACK/EXPLOITATION ACTIVITY

A. INTRODUCTION

This chapter examines the CNA/E activities of North Korea. There have been several reports of suspected CNA/E activities being sponsored by North Korea. This chapter aims to verify the validity of these allegations and examine the reported cases of CNA/E.

B. COMPUTER NETWORK ATTACK (CNA)

CNA is a relatively new weapon in the modern warfighter's arsenal, and can be used to inflict significant damage at the speed of light. CNA is defined as operations to disrupt, deny, and degrade information resident in computers and computer networks, or the computers and networks themselves. CNA relies on the data stream to execute an attack, for example, the transmission of malicious code to a central processing unit (CPU) that causes the computer to short out the power supply thereby rendering the computer useless [FM 03]. CNA includes attacks stemming from viruses, worms, and distributed denial of service.

C. COMPUTER NETWORK EXPLOITATION (CNE)

The first step in carrying out a successful computer network attack is identifying the prospective system's vulnerabilities and then exploiting those vulnerabilities. Therefore, CNE is an integral operation in the execution of CNA against an adversary. CNE is defined as enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks [FM 03].

D. DIFFICULTIES OF IDENTIFYING NORTH KOREAN HACKERS

Given the ubiquitous and anonymous nature of the Internet, it is becoming unceasingly difficult for law enforcement to properly identify computer attackers and the origin of their attacks. Three techniques used by hackers to cover their tracks are:

1. IP Spoofing

A sophisticated attacker will undoubtedly attempt to conceal his source IP address in the performance of an attack. IP spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host [Webop 04]. Therefore, an attacker in North Korea could spoof or hide his true IP address making it nearly impossible to verify his true origin.

2. Communication Bouncing

A North Korean attacker might intentionally bounce his communications through several computers in numerous unsuspected countries before reaching his target. This creates a problem for computer forensic investigators in that they will have to re-trace and identify all the bounce points to determine the origin of the attack. In some cases, these communications bounce through countries that do not consider computer hacking a crime or that are not willing to assist in an investigation.

3. Manipulation of Event Logs

Most critical systems are usually protected by an intrusion detection system (IDS) and maintain an event log of the systems activities. However, these protection mechanisms are far from perfect and an attacker might be able to alter logs after gaining unauthorized access to systems, concealing all evidence of their attack.

E. NORTH KOREAN HACKING ACTIVITY

North Korea has long been suspected of conducting computer network operations against other nations, especially South Korea. However, because North Korea is such a closed country, very little is known of the country's CNO activities.

Not much is known in the unclassified realm of North Korea's exploits either attempted or succeeded. There has been widespread speculation that North Korea possesses a credible CNO capability, but evidence of such activity is almost non-existent.

South Korea, however, is taking the North Korean hacking threat seriously and announced in June 2003 that the Defense Security Command (DSC) will be establishing a special intelligence-protecting office to cope with the rising threat posed by North Korean hackers [APAN 03].

LT. General Song Young-guen, the commanding general of South Korea's DSC has long been an outspoken voice warning of the North's cyber warfare capabilities. In early 2003, Young-guen reported that the DPRK was found to be operating a highly skilled military unit with the specific mission of hacking into South Korea's networks seeking secret information. In May 2004 at the 2004 Defense Information Security Conference, Young-guen reported that the highly skilled contingent of North Korean hackers had been set up under orders from the Supreme Leader Kim Jong Il. This is the first time a South Korean official has publicly confirmed the existence of hacking units in the DPRK. According to Young-guen, the hacking capability of the elite North Korean hacking unit is assessed as equivalent to that of the CIA [Jin 04].

In March 2003 the Weekly Post (www.weeklypost.com) reported that North Korea had approximately 2,000 strategic units comprised of skilled computer hackers whose mission is to destroy computer information and communication networks. The Weekly Post stated that the 2,000 North Korean cyber terrorists were scattered in South Korea, Hong Kong, Russia, and Japan. According to the Weekly Post, the Japanese suspect that the DPRK was involved in a January 25, 2003 cyber attack on South Korean and Japanese networks [WP 03].

WorldNet Daily alleged that the infamous hacker Kuji who hacked into the Rome Air Development Center at Griffiss Air Force Base in New York in 1994 was actually a highly trained North Korean hacker [LoBaido 2000]. These allegations proved to be false, however, as the true perpetrators of the Rome Air Development Center break-in were two young British hackers with no affiliation to North Korea [Ungoed-Thomas 98].

During the course of this research no credible evidence was discovered to indicate that North Korea was actively participating in any CNA/E activities whether covertly or overtly. However, there was plenty of conjecture and speculation as to the actual CNO capabilities and intentions of the DPRK.

In an April 2004 telephone interview with Director Baek of South Korea's National Intelligence Service (NIS), Director Baek stated that his organization had no knowledge of confirmed CNA/E activities originating from within North Korea. He also stated that the NIS had no evidence of North Korea sponsoring CNA/E activities against South Korea or any other country. Officials at the Korea Information Security Agency (KISA), who disclosed that very little is known on the computer network activity of their neighbor to the north, also echoed Director Baek's comments.

F. OBSTACLES ASSOCIATED WITH THE DPRK'S CNA/E ACTIVITES

Computers are available in minute numbers to the general population of North Korea. Most of the computing power available in the DPRK is hoarded by state run research facilities. In addition, the technical knowledge needed to carry out CNA/E activities is not widely possessed outside of the state's laboratories scattered all over the country.

According to a Nautilus Institute study conducted in October 2002, the DPRK's network access was almost zero due to its lack of a functioning telecommunication infrastructure [Hayes 02]. Today, connectivity speeds remain slow and the quality remains poor; these factors are certainly not conducive to effectively conducting CNA/E operations. The DPRK is conspicuously absent from a systematic accounting of national networked readiness. North Korea possesses almost none of the factors required for achieving a favorable network policy. Even with the aid of South Korean enterprises, the DPRK's connectivity level remains low due to censorship and limited access to computers.

The absence of stable and continuous electricity throughout the country is a major obstacle for North Korea. North Korea's electrical grid is antiquated and stretched way beyond capacity. The country spends most of the time in the dark without electricity. It would be extremely difficult to conduct CNA/E operations without reliable power. Given the level of sophistication and complexity of the protection software on modern computers systems, it often takes hours before an exploitation or attack is successfully completed.

It does not take a lot of processing power to conduct CNA/E operations, although supercomputers or high-end Pentium processors can be useful for cracking passwords and keys. However, if North Korea wishes to test the effectiveness of its CNA/E tools on computer systems running modern operating systems such as Windows XP© or Windows 2000©, it is a requisite that North Korea possesses similar systems running similar software. It has long been suspected that North Korea possesses a limited number of Pentium machines.

In a recent visit to South Korea, North Korean officials demanded the unrestricted export of South Korean made Pentium processors to North Korea. This would suggest that the North's attempt at producing a Pentium equivalent processor has not yet been fully achieved. Several reports have stated that the core of North Korea's computing base is centered on the use of 80386 and 80486 processors.

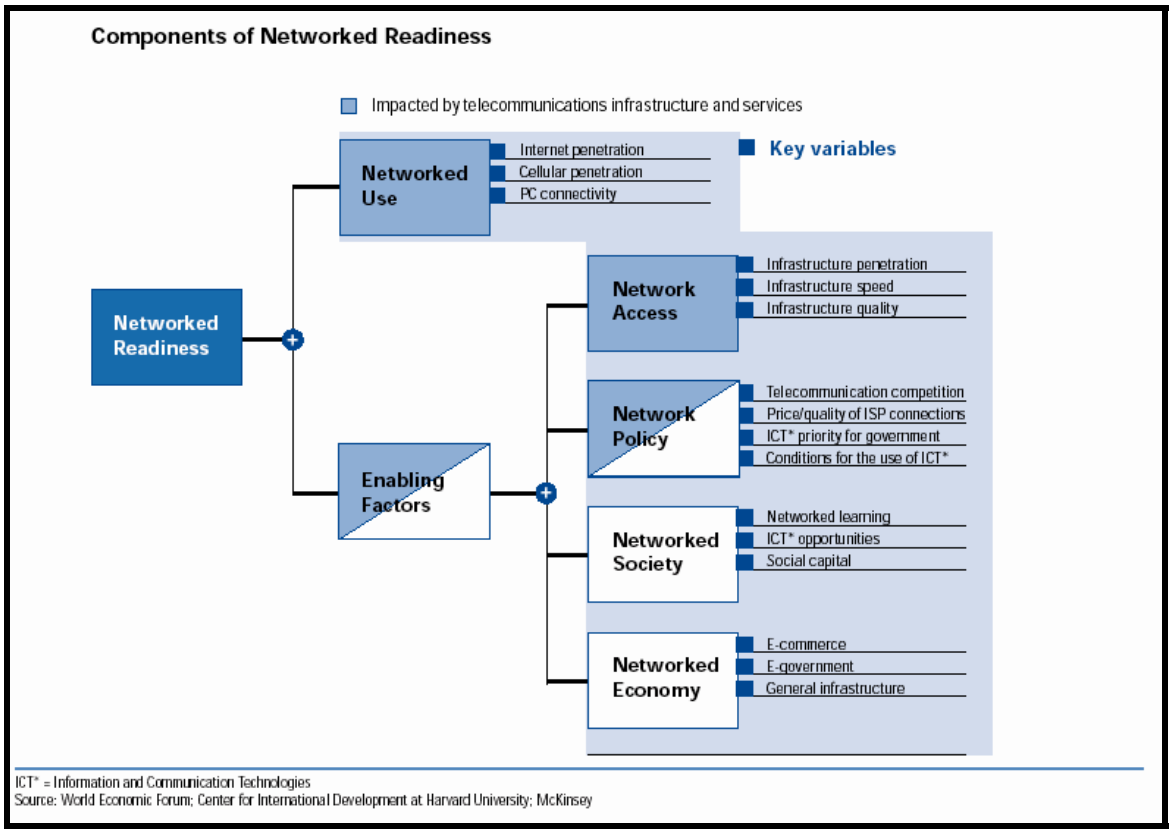

Figure 6.1: Components of Network Readiness

[After: Hayes 02]

G. SUMMARY

This chapter discussed the CNA/E activities of North Korea along with some of the difficulties associated with determining the source of the activity. It was determined that despite technological advances in the area of IT, North Korea did not pose a serious CNO threat given its lack of network readiness. This chapter also examined the reported cases of North Korean CNO activities.

VII. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSION

1. State Sponsored CNO Activities are Often Not Overt

Researching the activities of a closed society such as North Korea was a difficult task. Additionally, this research was limited to open source information, and the quality and quantity of pertinent information was sparse. When dealing with a country shrouded in secrecy such a North Korea, many of the conclusions drawn from available open source information is merely speculative. However, being eager to prove to the world that they will not be left behind, North Korea has made publicly available some of its current IT research and development projects on state sponsored websites. It is unclear exactly how much of this information is fact or fiction.

The CNO activities of North Korea are not well documented in open sources. Although there has been much speculation by South Korea, we were unable to confirm any CNO activity originating in North Korea or sponsored by the government of North Korea. Allegations of computer hacking by North Korea were discovered on the Internet, however, the sources failed to mention the specifics of the allegations and these allegations proved inconclusive.

We did not expect to find a "smoking gun" indicating North Korea was actively involved in state sponsored cyber warfare. However, there was an expectation that specific data items gleaned from the research conducted would indicate that North Korea was at the very least able to conduct CNO, if so desired. Specifically, the data points examined included those of North Korea's IT infrastructure, electrical infrastructure, and the level and pervasiveness of IT education. Evidence was uncovered indicating North Korea has a strong desire to conduct research and testing of its CNO capabilities at its various research laboratories and universities. Whether or not the DPRK is ready to deploy or have deployed such capabilities remains unknown. It is important to note however, that regardless of whether North Korea possesses the capability to conduct CNO against its adversaries, CNO does not appear to be the primary concern among the North Korean leadership. North Korea seems to be developing its IT capability to

promote economic growth rather than to attack an adversary's network. North Korea's recent request of IT publications from South Korea did not include any publications germane to CNO; rather they focused on commercial applications associated with fielding IT, such as design, graphics, and animation. Additionally, the subjects being studied by visiting North Korean students at Syracuse University do not include CNO.

We have shown that North Korea has integrated IT education into its educational system, and we have also shown that its military IT education includes virus creation and network penetration. Despite stringent export restrictions, North Korea possesses the basic technology needed to conduct CNO. Furthermore, North Korea possesses the connectivity needed to conduct limited CNO against an adversary. Although no direct evidence was uncovered to suggest that North Korea is actively involved in CNO activities, we believe that enough credible evidence was uncovered to indicate that North Korea possesses the wherewithal to conduct CNO against its adversaries.

2. Technology is a Factor in CNO

North Korea has developed several computer systems over the years and despite import restrictions on dual-use technology has managed to acquire such technologies from its allies. However, the lethality of the CNO activity is not directly proportional to the processing power of the systems used in the attacks. The fact is, very little processing power is needed to develop and deploy a lethal virus or worm. North Korea currently possesses sufficient processing capability to develop and deploy such mechanisms. However, its limited connectivity and unreliable electrical system could be obstacles to deployment.

North Korea need not develop its own hacking tools, as they are available for sale or even for free on the Internet. However, if North Korea's CNO capabilities are limited to deploying the typical hacker attacks found openly on the Internet, the CNA/E threat from North Korea may be of little national interest. On the other hand, if North Korean researchers are developing native viruses and worms for use in their CNO program, the threat will be greater.

3. Education is the Foundation

The North Korean leadership, particularly Kim Jong Il, recognizes the importance of IT education in North Korea. Starting at the grade level IT education has become compulsory throughout North Korea. In order to produce capable cyber warriors IT education has to be an integral part of the overall plan. The North Korean government has impressed upon its populace the importance of IT to the future of the country. Today, being an IT professional is North Korea is viewed as a job of prestige.

The idea of IT education has not escaped the North Korean military and the potential use of CNO as a weapon of mass disruption. As reported, the Mirim College allegedly has been steadily producing at least 100 cybersoldiers each year, trained in such areas as virus creation and network penetration. This highlights the fact that North Korea acknowledges the importance of CNO in modern warfare. However, we did not find any evidence of other North Korean schools teaching CNO.

B. RECOMMENDATIONS FOR FUTURE WORK

1. China-North Korea Relationship

Further examination of the relationship between China and North Korea should be conducted in order to assess exactly how much IT aid is being provided to North Korea. To assume that Chinese developed dual-use technology and IT products are prevalent in North Korea is not an unfair assumption. It is this trade relationship that should be further examined. A determination as to whether Chinese hackers are actively training North Koreans should also be made.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[AFP 04] Agence France Presse, "North Korea Recalls Mobile Phones, June 2004.

[AP 03] Associated Press, "North Korea May Be Training Hackers", http://miami.com/mld/miamiherald/news/world/5877291.htm, May 2003. Last accessed on August 13, 2004.

[AP 03] Associated Press, "North Korea Suspected Of Training Hackers", http://smh.com.au/articles/2003/06/10/1055010959349.html, June 2003. Last accessed on August 13, 2004.

[APAN 03] Asia-Pacific Area Network, Associated Press, "Korean Military To Create Units Against Hacking, Terrorism", June 2003.

[APCSS 02] Asia-Pacific Center for Security Studies, "Bytes and Bullets: Impact if IT Revolution on War and Peace in Korea", October 2002.

[ATIP 97] Asian Technology Information Program, "IT – In the North (DPRK)", http://atip.org/ATIP/public/atip.reports.97/atip-97-060-ext-03.html, 1997. Last accessed on August 13, 2004.

[Artyukov 02] Artyukov, Oleg, "North Korea May Become Hi-Tech Leader"; http://english.pravda.ru/world/2002/04/24/27943.html, April 2002. Last accessed on August 13, 2004.

[ASPAC 03] Asian Studied on the Pacific Coast, "Bilateral Research Collaboration Between Kim Chaek University of Technology (DPRK) and Syracuse University (US) in the Area of Integrated Information Technology", June 2003.

[AU 03] American University, "Country Analysis: China" http://www.american.edu/initeb/js5518a/Country-analysis-china.html, December 2003. Last accessed on August 17, 2004.

[BBC 02] British Broadcasting Corporation (BBC) Monitoring, Asia Pacific, "Chinese Military Delegation Visits North Korea, Discusses Friendship", November 2002.

[Beal 03] Beal, Tim, "Pyongyang Report Volume 3 No. 1", http://www.vuw.ac.nz/~caplabtb/dprk/pyr3_1.html, February 2001.
Last accessed on August 13, 2004.

[CCRC 04] Computer Crime research Center, "Chinese Hackers Advertise Made-to-Order Virus Service", http://crime-research.org/news/13.07.2004/487, July 2004.
Last accessed on August 17, 2004.

[CDES 01] Canada DPR Korea E-Clipping Service, "ROK Firm To Set Up Satellite For DPRK", June 01.

[China 04] China.org, The People's Daily, "China Becomes World's Third Biggest Hi-tech Producer", http://www.china.org.cn/english/2004/Feb/86226.htm, February 2004.
Last accessed on August 17, 2004.

[Choe 03] Choe, Sang-Hun, "North Korea Takes Fitful Steps into Computer Era", http://www.mercurynews.com/mld/mercurynews/business/7590144.htm, December 2003.
Last accessed on August 13, 2004.

[CIA 04] The Central Intelligence Agency, "The World Factbook", http://www.odci.gov/cia/publications/factbook/geos/kn.html, May 2004.
Last accessed on August 17, 2004.

[Clarke 02] Clarke, Richard, Testimony for the US Senate Judiciary Committee, Administrative Oversight and the Courts Subcommittee, "Administrative Oversight: Are We Ready For A Cyber Terror Attack?", February 2002.

[Cohen 01] Cohen, David, "In Cyberuniversities, a Place for South Korea's Women", http://chronicle.com/free/v47/i30/30a04101.htm, April 2001.
Last accessed on August 15, 2004.

[Conner 01] Conner, Michael, H., "North Korea's Homegrown Web for Elite Only", March 2001.

[Connole 98] Connole, Patrick, "US Cyber Law Chief Reports 'Substantial' Cyber attack", June 1998.

[Crowcroft 04] Crowcroft Genealogy, "DPRK – Third Visit April 13-20, 2004", April 2004.

[DPRKI 04] Democratic People Republic of Korea Infobank Website, http://www.dprkorea.com/, July 2004.
Last accessed on August 17, 2004.

[DPRKNTA 02] Democratic People Republic of Korea National Tourism Administration, "In Korea Portable Telephone Communication Possibly", May 2002.

[DPRKNTA 02] Democratic People Republic of Korea National Tourism Administration, "The Pyongyang Internet Coffee", October 2002.

[DPRKNTA 04] Democratic People Republic of Korea National Tourism Administration, "Business Trade Investment Exhibition News", January 2004.

[Dubrovin 03] Dubrovin, Denis, "I See Suffering in the Streets of Pyongyang", http://telegraph.co.uk/news/main.jhtml?xml=/news/2003/01/05/wkor05.xml. January 2003.
Last accessed on August 14, 2004.

[FAS 00] Federation of American Scientists, http://www.fas.org/nuke/guide/dprk/target/energy.htm, June 2000.
Last accessed on August 13, 2004.

[FM 03] Army Field Manual 3-13, "Information Operations, Doctrine, Tactics, Techniques, and Procedures", Department of the Army, November 2003.

[France 01] France, Mike, Business Week, “Red Alert over Digital Warfare on the Net”, April 2001.

[GAO 04] General Accounting Office, “ GAO-04-628T - Improved Planning Needed to Ensure Delivery of Essential Government Services”, April 2004

[GS 02] GlobalSecurity.org, “DPRK Doctrine”, http://www.globalsecurity.org/wmd/world/dprk/doctrine.htm, December 2002.
Last accessed on August 17, 2004.

[GS 04] GlobalSecurity.org, “North Korea is Dark”, http://www.globalsecurity.org/military/world/dprk/dprk-dark.htm, April 2004.
Last accessed on August 17, 2004.

[Hayes 95] Hayes, Peter, Von Hippel, David, “The Prospects for Energy Efficiency Improvements in the Democratic People’s Republic of Korea: Evaluating and Exploring the Option”, http://www.nautilus.org/archives/papers/energy/dvh_hayesENEF.html, October 1995.
Last accessed on August 17, 2004.

[Hayes 02] Hayes, Peter, “DPRK Information Strategy – Does It Exist?”, http://www.nautilus.org/archives/pub/ftp/Phayes/DPRKInformationStrategyPubVersionOct11-021.htm, October 2002.
Last accessed on August 17, 2004.

[Hoff01] Hoffman, Frank, “E-Resources from North Korea”, http://koreaweb.ws/pipermail/koreanstudies_koreaweb.ws/2001-December/003000.html, December 2001.
Last accessed on August 17, 2004.

[Ho-Song 01] Ho-Song, Kwan, Dr., Korea Network Information Center, “The Survey and Future Activities on the Digital Divide in Korea and Asia-Pacific Region”, February 2001.

[ICAS 02] Institute for Corean-American Studies, Inc, "Digital Divide on the Korean Peninsula: Constructive Engagement Offers Solutions", June 2002.

[ITWorld 02] Anonymous, "North Korea to Exhibit Domestic Software in Beijing", http://www.itworld.com/Tech/2418/020215northkorea/, February 2002.
Last accessed on August 17, 2004.

[JIN 04] Jin, Ryu, Staff Reporter, Korea Times, "North Korea Operates Hacking Unit", May 2004.

[Joseph 02] Joseph, Manu, Wired News, "Software Wars: China vs. India", April 2002.

[KCC 03] Korean Computer Center, "Naenara Website", http://www.kcckp.net/external_e/, November 2003.
Last accessed on August 17, 2004.

[KCNA 03] Korean Central News Agency, http://www.kcna.co.jp, December 2003.
Last accessed on August 15, 2004.

[KCNA 02] Korean Central News Agency, "Pyongyang University of Computer Technology", http://www.kcna.co.jp/item/2002/200201/news01/25.htm, January 2002.
Last accessed on August 17, 2004.

[KCNA 98] Korean Central News Agency, "Silver Star Laboratories of Korea", http://www.kcna.co.jp/item/1998/9809/news09/23.htm , September 1998.
Last accessed on August 17, 2004.

[KCNA 96] Korean Central News Agency, "Kim Il Sung University The First University of the People", http://www.kimsoft.com/korea/kis-univ.htm, October 1996.
Last accessed on August 17, 2004.

[KN 01] Korea.net, "North Korea Eager to Develop IT Industry", May 2001.

[Kraemer/Dedrick 02] Kraemer, Kenneth, L and Dedrick, Jason, "Enter the Dragon: China's Computer Industry, http://www.computer.org/computer/homepage/0202/per/print.htm, February 2002 Last accessed on August 17, 2004.

[Kwan 01] Kwan, Lee Kyo, "NK Nearly Ready to Access Internet", September 2001.

[Larimer 04] Larimer, Tim, "North Korea Barely Has An Economy. But If You Need Computer Talent, It's Ready To Do Business", http://www.time.com/time/asia/news/magazine/0,9754,99027,00.html, February 2001. Last accessed on August 17, 2004.

[Larkin 01] Larkin, John, "North Korea Preparing For Cyberwar", http://archive.infopeace.de/msg00464.html, October 2001. Last accessed on August 15, 2004.

[LKD 04] Liaoning Korea Daily, "North Korea Established a Software Developing Company in Shenyang", March 2004.

[LoBaido 00] LoBaido, Anthony, WorldNetDaily, "Hello Kitty Battles in Cyberwars, International Hackers Sell Skills to Governments, private Sector", September 2000.

[LOC 93] Library of Congress, " World Studies: North Korea", http://lcweb2.loc.gov/cgi-bin/query/r?frd/cstdy:@field(DOCID+kp0090), June 1993. Last accessed on August 17, 2004.

[LOC 04] Library of Congress, " World Studies: North Korea", http://reference.allrefer.com/country-guide-study/north-korea/north-korea155.html, July 2004. Last accessed on August 17, 2004.

[Lyman 02] Lyman, Jay, "Report: U.S. Expecting Chinese Hack Blitz", http://www.newsfactor.com/perl/story/17465.html, April 2002. Last accessed on August 17, 2004.

[McWilliams 03] McWilliams, Brian, "North Korea's School for Hackers", http://www.wired.com/news/conflict/0,2100,59043,00.html, June 2003. Last accessed on August 17, 2004.

[MDN 04] Mainichi Daily News, "Chinese Hackers Attack Japanese Websites", http://mdn.mainichi.co.jp/news/20040807p2a00m0dm003000c.html, August 2004. Last accessed on August 17, 2004.

[Messmer 99] Messemer, Ellen, Cable News Network (CNN), "Kosovo Cyber-war Intensifies: Chinese Hackers Targeting U.S. Sites, Government Says", May 1999.

[Minnich 01] Minnich, James, M., "North Korea Tactics", September 2001.

[NASA 00] National Aeronautics and Space Administration, "Earth at Night", November 2000.

[Nautilus 01] The Nautilus Institute, "Inter-Korean Economic Cooperation", August 2001.

[NIS 02] National Intelligence Service, Republic of Korea, "North Korea", http://www.nis.go.kr/eng/north/, 2002. Last accessed on August 16, 2004.

[NKZONE 04] North Korea Zone, "Studying Programming", http://nkzone.typepad.com/nktech/2004/03/studying_progra.html, March 2004. Last accessed on August 16, 2004.

[Park 01] Park, Chan-Mo, "Current Status of Software Development in DPRK and Collaboration between the South and North", August 2001.

[PD 01] People's Daily, "DPRK Defense Chief Arrives in Moscow for Military Cooperation", April 2001.

[Seong-in 01] Seong-in, Bae, “North Korea’s Policy Shift Toward the IT Industry and Inter-Korean Cooperation”, East Asian Review, January 2001.

[Song-wu] Song-wu, Park, The Korea Times, “NK Hands Suspected in Cyberattacks”, July 2004.

[Soo-min 01] Soo-min, Seo, “NK Asks ROK Expert Group to provide IT Books”, May 2001.

[Thomas 00] Thomas, Timothy, L., Foreign Military Studies Office, “Like Adding Wings to the Tiger: Chinese Information War Theory and Practice”, http://fmso.leavenworth.army.mil/fmsopubs/issues/chinaiw.htm, November 2000. Last accessed on August 29, 2004.

[TPK 00] The People’s Korea, “Selected Items of Computer Programs Developed by the National Academy of Sciences”, http://210.145.168.243/pk/152th_issue/2000112909.htm, November 2000. Last accessed on August 14, 2004.

[TPK 01] The People’s Korea, “Computer Education Intensified in DPRK”, http://210.145.168.243/pk/154th_issue/2001012508.htm, November 2000. Last accessed on August 14, 2004.

[TPK 01] The People’s Korea, “Computer Network Rapidly Expanding in DPRK”, http://210.145.168.243/pk/156th_issue/2001022104.htm, February 2001. Last accessed on August 14, 2004.

[TPK 01] The People’s Korea, “Strategic Plan for IT Revolution in DPRK”, http://210.145.168.243/pk/167th_issue/2001082504.htm, August 2001. Last accessed on August 14, 2004.

[TPK 01] The People’s Korea, “DPRK to Enter World PC Market”, http://210.145.168.243/pk/168th_issue/2001100502.htm, October 2001. Last accessed on August 14, 2004.

[TPK 01] The People's Korea, "Training of IT Specialists in Full Swing", http://210.145.168.243/pk/171st_issue/2001120202.htm, December 2001. Last accessed on August 14, 2004

[TPK 03] The People's Korea, "DPRK Spreading Computer Networks", http://210.145.168.243/pk/189th_issue/2003030118.htm, March 2003. Last accessed on August 14, 2004.

[TPK 03] The People's Korea, "Modernization of Communication Networks Promoted in DPRK", http://210.145.168.243/pk/199th_issue/2003121304.htm, March 2003. Last accessed on August 14, 2004.

[TPK 03] The People's Korea, "DPRK Developed PDA Hana 21", http://210.145.168.243/pk/191th_issue/2003041201.htm, April 2003. Last accessed on August 14, 2004.

[TPK 03] The People's Korea, "DPRK-made Pocket Computer Popularized in DPRK", http://210.145.168.243/pk/198th_issue/2003112906.htm, April 2003. Last accessed on August 14, 2004.

[TPK 04] The People's Korea Website, http://210.145.168.243/pk, July 2004. Last accessed on August 17, 2004.

[UNDP 00] United Nations Development Program, Biodiversity Planning Support Program, "1st Workshop on National Biodiversity Strategies and Action Plans in Northeast and East Central Asia, Experiences and Lessons", April 2000.

[UNIDO 92] United Nations Industrial Development Organization, May 1992.

[UN 04] United Nations Statistical Database, December 2003.

[USDOC 04] United States Department of Commerce, "Export Administration Regulations, Category 3 – Electronics" http://w3.access.gpo.gov/bis/ear/ear_data.html, May 2004.
Last accessed on August 23, 2004.

[USDOS 96] United States Department of State, "Wassenaar Export Control Regime", July 1992.

[Ungoed-Thomas 98] Ungoed-Thomas, Jonathan, The Toronto Star, "How 'Datastream Cowboy' Took the U.S. to the Brink of War", April, 1998.

[UNVIE 04] United States Mission to International Organization in Vienna, "Brief History of the Wassenaar Arrangement" May 2004.

[WA 03] Wassenaar Arrangment , "Dual-Use List, Category 4 –Computers", http://www.wassenaar.org/list/wa-list_03_tableofcontents.html, December 2003.
Last accessed on August 23, 2004.

[Ward 01] Ward, Mark, British Broadcasting Corporation, "US and Chinese Hackers Trade Blows", May 2001.

[Williams 03] Williams, Martyn, "North Korean Internet Takes A Step Forward", July 2003.

[WP 03] Weekly Post, "North Korean Cyber Terrorist", http://www.weeklypost.com/030324/030324a.htm, March 2003.
Last accessed on August 17, 2004.

[WT 04] World Tribune.com, "North Korean Officials Tour Heart of South Korea's IT Industry", June 2004.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dorothy Denning
   Naval Postgraduate School
   Monterey, California

4. Joanne Kim
   Naval Postgraduate School
   Monterey, California

5. Cathy Azallion
   FGGM OSIS
   Fort George Meade, MD

6. Brian Steckler
   Naval Postgraduate School
   Monterey, California

7. Dartmouth College
   Institute for Security Technology Studies
   Hanover, New Hampshire

8. Peter Hayes
   Nautilus Institute for Security and Sustainability
   University of San Francisco
   San Francisco, California