CHAPTER 13

SIGINT, EW, and EIW in the Korean People's Army: an Overview of Development and Organization

Joseph S. Bermudez Jr.

> *"The basic key to victory in modern warfare is to do well in electronic warfare …"*
>
> *Kim Jong Il*[96]

For many years now the leaders of the Democratic People's Republic of Korea, Ministry of People's Armed Forces, and the Korean People's Army have understood the importance of C^4ISR and, more specifically, signals intelligence and electronic warfare.

Electronic warfare is understood by the MPAF to consist of operations using the electromagnetic spectrum to attack (e.g., jamming, spoofing, etc.) the enemy. During the 1990s

[96] "Kim Jong Il Stresses Electronic Warfare Capabilities," *Radio P'yongyang*, 24 September 1999, as cited in FBIS.

the MPAF identified "electronic intelligence warfare" (China Chinungjon, EIW) as a new type of warfare, the essence of which is the disruption or destruction of the opponent's computer networks -- thus paralyzing the enemy's military command and control system. Although this appears to be analogous to information warfare the MPAF's understanding may also include elements of reconnaissance, cryptanalysis, intelligence collection, and disinformation operations, as well as the use of the Internet to cause disruption within the enemy's social and economic homeland. It would appear that EW and SIGINT operations are conducted at all levels of the MPAF and intelligence community. While EIW operations are conducted at the national level (e.g., General Staff Department, Reconnaissance Bureau, State Security Department, etc.). The MPAF believes that EW and EIW are complimentary and that they must be integrated with conventional forces and operations to be effective on the modern battlefield,[97]

> *Do not prepare for electronic warfare just because that is what others are doing. In modern warfare, modern and conventional weapons must be massed and combined.*
>
> *Kim Jong Il*[98]

Details concerning how the MPAF developed this understanding, and how it has organized and planned to conduct SIGINT, EW and EIW operations, are extremely limited. What follows, albeit somewhat disjointed and

---

[97] "Ex-KPA Major Writes on DPRK Military Situation," *Pukhan*, January 2000, pp. 86-93, as cited in FBIS.

[98] Author interview data; "Ex-KPA Major Writes on DPRK Military Situation,"; and "Future Electronic Warfare Discussed," *Nodong Sinmun*, December 5, 1999, p. 6, as cited in FBIS.

certainly incomplete, provides an unclassified overview of the subject.

Accuracy in any work dealing with the KPA is a matter of relatives. Inevitably a certain amount of the information in this paper will be incorrect. Other material may be misinformation, disseminated by interested parties to serve their own purposes. The catchwords *probably*, *estimated*, *are believed to*, and *apparently* must appear frequently in any work of this type. This chapter is intended to stimulate discussion and provide other researchers a point of departure for additional research.

Development

If one were to attempt to assign a point of origin to the DPRK's current interest in SIGINT, EW and EIW he would probably identify the immediate post World War II years. In these years, the Soviet Union, as it set about establishing a communist government in the northern half of the Korean Peninsula it, provided SIGINT training and equipment to the nascent Ministry of Internal Affairs and Reconnaissance Bureau of the emerging nation.

Information concerning the role that this SIGINT capability played during the subsequent Fatherland Liberation War (e.g., Korean War) is both murky and outside the scope of this chapter.[99] Suffice to say that during the buildup to, and

[99] For information concerning HUMINT and COMINT activities during the war readers are referred to Matthew Aid's excellent studies "US Humint and Comint in the Korean War: From the Approach of War to the Chinese Intervention," *Intelligence and National Security*, Vol. 14, No. 4, Winter 1999, pp. 17-63; and "American Comint in the Korean War (Part II): From the Chinese Intervention to the Armistice," *Intelligence and National Security*, Vol. 15, No. 1, Spring 2000, pp. 14-49.

initial months of, the conflict it played a significant role at the tactical, operational, and strategic levels. During the subsequent years of the war, the capabilities and successes of DPRK and People's Republic of China SIGINT in general appear to have fluctuated considerably. They apparently achieved some success at the tactical level, little success at the operational level, and almost no success at the strategic level.

The immediate post-armistice years were ones of tremendous political, social and economic turmoil within the DPRK as Kim Il Song sought to consolidate his position and deal with a war-ravaged nation. While apparently low on Kim's list of priorities, SIGINT training, equipment, and capabilities were reconstituted within the Ministry of Internal Affairs and Reconnaissance Bureau.[100]

It wasn't until the mid-1960s that the domestic situation had evolved sufficiently so that Kim would focus on the position of the KPA to wage war (including SIGINT and EW) on the modern battlefield. In an October 1966 speech to the Second Korean Workers' Party Congress, Kim stressed the need to develop the defense industry and to proceed with economic and national defense development simultaneously,

> *...We must strongly fortify the Korean People's Army with modern weapons and combat material. We must employ all means to modernize the weapons and make them more powerful based on the successes of ultra-modern science and technology*

[100] It is likely that Kim used these COMINT capabilities as much against his political opposition as he did against the DPRK's external enemies.

> *... In modernizing the Korean People's Army and developing military science and technology ... We must develop and introduce military science and technology in accordance with the reality of our country and correctly incorporate old style weapons along with modern weapons.*[101]

It is interesting to note Kim's emphasis upon what could now be identified as combined arms and asymmetric warfare.

While the initial results of Kim's speech were focused upon the establishment of the Second Economic Committee to oversee the acquisition and production of modern weapons, a number of steps were initiated which would lay the foundations for future EW/EIW developments. Included among these were the establishment of science and technology curriculums within the civilian and military educational systems, the training of small numbers of intelligence and KPA personnel in computer sciences, EW, and SIGINT within the Soviet Union and PRC, and the acquisition a very small number of first-generation mainframe computers from the Soviet Union. These first-generation computers are believed to have been operated by the Ministry of Public Security (formerly the Ministry of Internal Affairs) and Academy of Defense Sciences in critical programs (e.g., SIGINT, nuclear, etc.).[102]

---

[101] *Kukbang Kwa Kisul*, "South Army Official Looks at DPRK's Weapons," January 1989, pp. 102–113, as cited in FBIS.

[102] During 1962 the Ministry of Internal Affairs became the Ministry of Public Security. The State Security Department would subsequently separated out from the Ministry of Public Security in 1973.

The importance of Kim's 1966 speech was dramatically reinforced in 1968. When, in January, as part of an escalating guerrilla war against the ROK, the KPN attacked and captured the U.S. Navy SIGINT vessel *USS Pueblo*. The subsequent exploitation and evaluation of this intelligence coup undoubtedly revealed to the DPRK the advanced level of U.S. capabilities, their own vulnerabilities, and their woefully inadequate SIGINT capabilities. This set in motion a renewed effort to develop SIGINT and EW capabilities within the KPA.

Although MPAF extensively studied the Vietnam and 1973 Arab-Israeli Wars, including SIGINT and EW operations, it wasn't until the mid-1980s that it initiated a broad effort to improve these capabilities. A fundamental component of this effort was the reorganization of the 1984 establishment of the Mirim Academy in Pyongyang subordinate to the Education Bureau. The mission of the academy was to educate military officers in the principles and practices of electronic warfare, creation and management of military computers systems, and computer sciences. The initial two-year class of approximately 100 students were selected from postgraduate students of the physics, automation, and mathematics departments of Kim Il-song University, Kim Chaek University of Technology, other elite universities, and top officer candidates from the Kang Kon General Military Academy, Kim Jong-suk Naval University and Kim Chaek Air Force Academy. To help staff the faculty the DPRK hired SIGINT and EW specialists from the former Soviet Union including instructors from the Frunze Military Academy. Among the courses taught were jamming, radar detection, missile control and guidance, computers, and infrared detection and tracking. These developments were accompanied by curriculum changes in many educational institutes which began to offer computer science and technology courses. A computer science

department was created within Kim Il-song University, research institutes were established within Kim Chaek University of Technology and the Academy of Sciences, and computer colleges were constructed within Pyongyang and Hamhung. The MPAF also dispatched a small number of students to the former Soviet Union for specialized electronic warfare instruction.[103]

With the graduation of the first class in 1986 the MPAF reorganized the academy into the Mirim College, moved the campus, and expanded the curriculum to include two-, four-, and five-year courses of study. Entrance to the college was now opened to top graduates from provincial high schools and qualified enlisted personnel. The curriculum was organized into five majors -- command automation, computer sciences, programming, reconnaissance, and electronic warfare. Courses also included computer calculation, information transmission, and the development of codes. Today, it is estimated that the school graduates approximately 100 students per year, most of whom are commissioned as second lieutenants. They are usually assigned positions as computer or EW specialists at brigade level or above. A few of the most accomplished graduates are assigned as instructors or researchers at research institutes, or to the Reconnaissance Bureau or State Security Department. Sometime afterwards the name of the college was changed to the Electronic

[103] Author interview data; "IT Sector Growing in North Korea," *Joong-Ang Ilbo*, May 3, 2000; and "Computer Science and Electronics Engineering in North Korea," *Investigative Research Report on North Korea's Science and Technology*, December 1993, pp. 409-462, as cited in JPRS. The Mirim Academy may have also been known as the 525th Electronic Research Institute, or a separate institute with this designation may also have been established at this time. "Ex-DPRK Major Unveils KPA Military Plan," *Pukhan*, February 1, 2000, pp. 92-99, as cited in FBIS; and http://www.nis/go.kr, accessed June 21, 2002.

Warfare Institute (a.k.a., Automated Warfare Institute).[104] By 1990, sufficient students had graduated to enable the KPA to establish the Electronic Warfare Bureau within the General Staff Department. Concurrent with this, electronic warfare departments were established within corps, division, and brigade headquarters. Priority for creation of these departments was given first to those units deployed along the DMZ.[105]

Accompanying these early developments was an explosion, during the late 1980s and early 1990s, in the establishment of new computer institutions and development and production facilities. In April 1987 the Integrated Circuit Test Facility of the Academy of Science's Electronics Institute was completed. It was constructed with UNDP funding and was tasked with training and research and development into integrated circuits. In October 1990, the DPRK established the KCC in Pyongyang to cultivate the development of computer professionals and software. By early 2000 the KCC consisted of some 4,500 employees and 900 computer programmers in their 20s and 30s. Regional computer centers had been established in Hamhung and Sinuiju. Additional computer centers for each province were apparently established by the end of the year. The KCC is equipped with a wide selection of domestic- and foreign-produced computers. The Ponghwa Diskette Factory in Pyongyang was completed in October 1990 with equipment imported from Japan. Following in the steps of the KCC were the Computer Personnel Training Center at the Kim Chaek University of Technology in April 1991, and the Pyongyang Program

---

[104] Ibid.

[105] Ibid.; and "DPRK Hacking Threat Creates Concern," *Choson Ilbo*, February 10, 2000; Chong Son-ku, "North Operating Mirim College for Electronic War," *Chungang Ilbo*, 22 September 1994, p. 4, as cited in FBIS.

Center in July 1991. In April 1992, the Pyongyang Integrated Circuit Factory initiated low-scale production of electronic components and sub-assemblies (e.g., television receivers, integrated circuits, semiconductors, etc.). Construction of the Pyongyang Computer Factory began during the early 1990s. It has become the DPRK's primary circuit board and computer production facility.[106]

Operation DESERT STORM appears to have been a seminal event in the MPAF's understanding of EW/EIW operations. It probably also exerted a strong influence on the MPAF's development of related doctrines since it was extensively studied by the MPAF's Research Institute for Military Sciences and the Strategy Research Institute, the Electronic Warfare Bureau and the Electronic Warfare Institute. Shortly afterwards, Kim Jong Il ordered a continued expansion of research into electronic warfare by all branches of the KPA and directed the expansion of the computer industry and computer related departments and courses at universities and colleges. The current KPA concept of EIW developed in the early 1990s as a direct outgrowth of these developments. It is also believed that during the 1990s the MPAF's Research Institute for Military Sciences and the Strategy Research Institute initiated the use of computer simulations to study international and other possible conflicts.

During 1996, several additional research institutes for the development of computer software were established in Pyongyang. These institutions have focused on technical

---

[106] Author interview data; "IT Sector Growing in North Korea," *Joong-Ang Ilbo*, May 3, 2000; "Computer Science and Electronics Engineering in North Korea," *Investigative Research Report on North Korea's Science and Technology*, December 1993, pp. 409-462, as cited in JPRS; and "DPRK Drive for Science, Technology Analyzed," *Sin Tong-a*, No. 12, December 1990, pp. 212-228, as cited in FBIS.

cooperation with other Third World countries and on importing hardware and software from Japan and the West. On November 24, 1999, the DPRK established the Electronics Industry Ministry. The ministry is subordinate to the Cabinet and responsible for the electronics industry and computer sciences, both of which are essential to successful SIGINT, EW and EIW operations.

The continued coalition operations in Iraq (e.g., Operation DESERT FOX, SOUTHERN WATCH, etc.) and Afghanistan (i.e., Operation ENDURING FREEDOM) have received extensive coverage and study by the DPRK and are apparently serving as a catalyst for continued SIGINT, EW and EIW development.[107] In September 1999, the DPRK proudly declared, "The electronic warfare capabilities of the People's Army have reached a high level enough to resolutely contain the enemies' invasion."[108]

The public statements and actions taken by the ROK Government and ROK Ministry of Defense during the past two years to improve computer security and skills indicate that the threat of KPA EW/EIW operations is taken seriously.[109] For example, in February 2000, ROK Defense Minister Cho Seong-tae ordered the Army, Navy, and Air Force to enhance the security of military computer networks (i.e., the Defense Information and

[107] Author interview data; "N.K. Establishes New Ministry for Electronic Industry Growth," *Korea Herald*, November 26, 1999; "Kim Jong Il Stresses Electronic Warfare Capabilities," *Radio Pyongyang*, 24 September 1999, as cited in FBIS; and "Defector Says DPRK Receives Spy Photos From Russia," *Korea Times*, 25 June 1996, p 1.

[108] "Kim Jong Il Stresses Electronic Warfare Capabilities," *Radio Pyongyang*, 24 September 1999, as cited in FBIS.

[109] In addition to the threat from the DPRK the ROK Government and Ministry of Defense are concerned over the vulnerability of their computer networks to attacks by other governments and civilian hackers.

Communication Network). The same month ROK President Kim Dae-jung ordered the Ministry of Defense to increase computer literacy among its members and established a cyber-terrorism report center within the Korea Information Protection Center.[110]

The DPRK shows every indication that it understands the importance of SIGINT, EW and EIW operations on the modern battlefield and is continuing to dedicate resources to enhance these capabilities.

Telecommunications and Computers

Communications within the MPAF and KPA is primarily through landlines, with radio, microwave transmission, and messengers as secondary routes. These communications "piggyback" the national telecommunications network, which is composed of a mixture of Japanese-, European-, and Russian-manufactured carrier systems, switches and telecommunications equipment. While relatively good within the capital city Pyongyang, the telecommunications network outside the city is antiquated, typically requiring the assistance of an operator to place calls. During the late 1990s, the DPRK initiated an ambitious project to place fiber optic cables between Pyongyang and major cities. This project was reportedly undertaken for two reasons. First, was the MPAF's awareness of the vulnerability of its existing telecommunications infrastructure to ROK/U.S.

[110] Author interview data; "ROK Government To Establish Cyber Terrorism Report Center," *Yonhap*, February 25, 2000; "ROK President Stresses Military Computer Literacy," *Yonhap*, February 18. 2000; "ROK Defense Ministry Tightens Online Networks Security," *Korea Herald*, February 14, 2000; "DPRK Hacking Threat Creates Concern," *Choson Ilbo*, February 10, 2000; and "Weekly Views Preparation for Cyber Warfare," *Hangyore*, May 13, 1999, pp. 46-47, as cited in FBIS.

SIGINT, EW, and EIW operations, and second, to enhance intranet, Internet and communications services throughout the nation. Wireless services include, cellular phones, pagers, and satellite TV and phones. Cellular phone service is believed to have begun within the capital of Pyongyang sometime in 1998. Its use, as well as access to satellite TV, is restricted to high-ranking KWP and MPAF officials. During 1996, a KPA defector reported a somewhat peculiar incident in which, on the orders of Kim Jong Il, Russian-manufactured pagers were issued to company and battalion commanders of at least some of the units deployed along the DMZ. The stated reason for this action was to improve the efficiency of the KPA's "command and communication system during emergencies."[111]

Beginning in 1996, a small group of computer technicians began building the Kwangmyong (Bright) Network, a national level intranet. This network currently has nodes in Pyongyang, each provincial capital, and several major cities.[112] Although isolated from the world, it allows for e-mail messaging and the sharing of web pages on the domestic level. The reason for this isolation is twofold. First, is the fear that its enemies (i.e., ROK and U.S.) would use it against the nation, and second, to prevent the people from being "contaminated" by outside influences. This has resulted in all Internet Web sites promoting the DPRK being actually located in Japan, PRC, or other nations. There is extremely limited access to the World Wide Web available in Pyongyang (and possibly a few other selected cities). Although it probably possessed others before it, the DPRK's first known permanent link to the Internet began in October 1996 through the Pyongyang office of the

---

[111] "DPRK Supplies Russian Pagers to DMZ-Deployed Army Troops," *Yonhap*, October 29, 1996, as cited in FBIS.
[112] "China Report Highlights N. Korea's Homegrown Web," *Reuters Internet Report*, March 23, 2001.

United Nations Development Plan.[113] Access to the Internet is restricted to only select KWP, government (e.g., Ministry of Foreign Affairs, State Security Department, Ministry of Public Security, etc.), and MPAF (e.g., Reconnaissance Bureau, Electronic Warfare Bureau, etc.) officials and employees. Kim Jong Il has reportedly shown a personal interest in the Internet and routinely spends time surfing the Internet.[114] All Internet access -- domestic and international -- is monitored by the State Security Department. DPRK computer security technology is reported to be relatively sophisticated.[115]

Although the DPRK has been producing computers since the late 1980s, it has only recently been able to manufacture computers comparable to lower-end Pentium class systems. Even this production is believed to be heavily dependent upon imported components. Available evidence suggests that the quality of indigenously manufacture computer equipment is low.[116]

---

[113] "DPRK Linked to Internet Through UNDP Office," *Hanguk Ilbo*, December 1, 1995, p. 8.
[114] "Character Study of DPRK's Kim Jong Il," *Wolgan Chungang*, June 1, 2000, pp. 74-87, as cited in FBIS.
[115] Interview data, Cho, Un-hui. "Do They Use Cellular Phones in North Korea?," *Chungang Ilbo*, 12 July 12, 2001; and "Cyber Commerce with North Korea Proposed," *Korea Herald*, June 8, 1999.
[116] Chung, Chang-hyun. "IT Sector Growing in North Korea," *JoongAng Ilbo*, May 3, 2000.

Command and Control[117]

All power within the DPRK originates with Kim Jong Il, who is simultaneously Chairman of the National Defense Commission, General Secretary of the KWP, and Supreme Commander of the KPA. The primary path for command and control of the KPA extends through the National Defense Commission to the Ministry of People's Armed Forces and its General Staff Department. From here command and control flows to the Korean People's Navy Command, Korean People's Air and Air Defense Command, various bureaus and operational units. Two secondary paths exist to ensure political control of the KPA. The first extends through the KWP Central Committee to the Central Military Committee and onto the General Political Bureau subordinate to the National Defense Commission. From the General Political Bureau it extends down via a separate chain-of-command to the lowest-levels of the KPA. The second extends from the National Defense Commission to the State Security Department. This department controls the MPAF's Security Command, which also maintains representatives to the lowest-levels of the KPA. As a unified armed force the chief of the general staff not only directly commands the ground forces but also the naval and air forces.

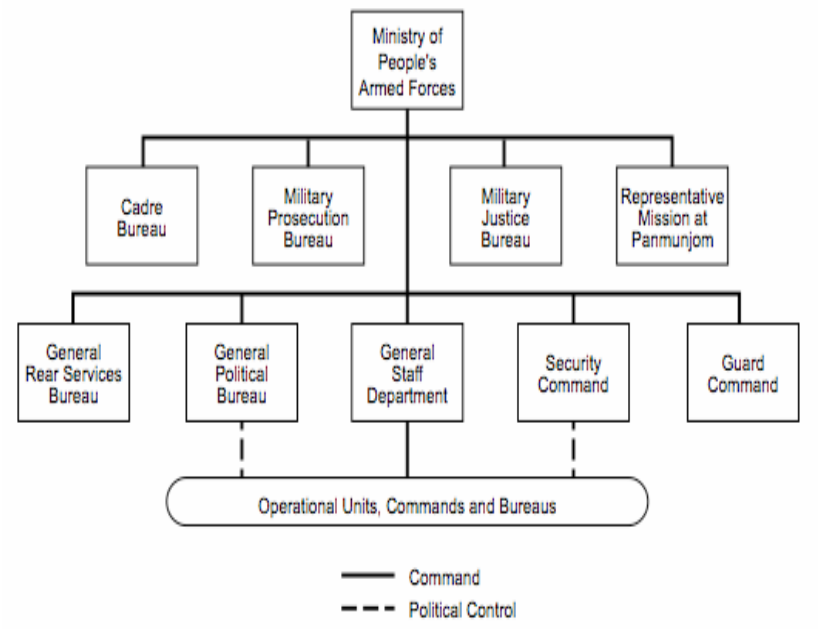
[117] Author interview data; United States Forces Korea, *Analysis of the North Korean Threat*, Backgrounder No. 12, Public Affairs Office, Seoul, 1999; *North Korea: The Foundations for Military Strength—Update 1995*, p. 13; and Bermudez Jr., Joseph S.; Brower, Kenneth; and Segal, Gerald, "North Korea A Potential Time Bomb," *Jane's Intelligence Review: Special Report No.2*, April 1995.

Ministry of People's Armed Forces[118]

As the Minister of the People's Armed Forces Vice-Marshal Kim Il-ch'ol is the National Defense Commission's officer directly responsible for the KPA. Eight vice-ministers assist him. Operational and administrative control of the KPA is exercised through the Chief of the General Staff, Vice Marshal Kim Yong-ch'un. Directly subordinate to the MPAF are the Cadre Bureau, General Political Bureau, General Rear Services Bureau, General Staff Department, Guard Command, Representative Mission at Panmunjom, Military Justice Bureau, Military Prosecution Bureau, and Security Command (see Figure 13.1). Of these only a few organizations and sub-organizations have a direct involvement in SIGINT, EW, and EIW operations.

[118] Author interview data; "ROK Journal on DPRK Leadership," *Pukhan*, October 1998, pp. 60-77, as cited in FBIS.

Figure 13.1. Organizational Chart of the DPRK Ministry of People's Armed Forces



General Staff Department

The General Staff Department exercises administrative and operational control over the KPA ground forces, KPAF, KPN, Workers' and Peasants' Red Guard, and Paramilitary Training Units. It is roughly equivalent to the ROK Joint Chiefs of Staff. The General Staff Department is staffed by officers and enlisted personnel from all the branches and is responsible for organizing, training, and equipping, as well as planning and executing all operations within the KPA.

Subordinate to the General Staff Department are 24 known bureaus, and a number of military academies, universities and research institutes. A number of these bureaus have

operational units subordinate to them and are directly involvement in SIGINT, EW, and EIW operations.

The Border Security Bureau is responsible for controlling unauthorized movements and preventing illegal entries and exits along the borders with the PRC and Russia. It controls a total of four Border Security Brigades. The Coastal Security Bureau is responsible for controlling unauthorized movements and preventing illegal entries and exits along the coastlines facing the East and Yellow Seas. It controls a total of six coastal security brigades.

The Classified Information Bureau is responsible for overseeing all aspects of the production, transmission and storage of classified information within the KPA, including planning and inspection, encryption, and decryption. It is also believed to have an operations security (OPSEC) responsibility and works in cooperation with the Communications Bureau. It is unclear what roles this department may play in the creation of code systems for the KPA, or in the decryption of enemy communications.

The Communications Bureau is responsible for the administration and operation of all communications within the KPA. It conducts monitoring of both domestic and foreign telecommunications traffic and is believed to work closely with the Reconnaissance Bureau and State Security Department in conducting SIGINT operations. This bureau also plays an important role within the area of communications security for the KPA and works in cooperation with the Classified Information Bureau. Subordinate to the Communications Bureau is the 9th Signals Brigade (a.k.a., 9th Communications Brigade) and a communications school. Aside from overseeing all communications within the KPA, this unit apparently operates a nationwide SIGINT collection system, and plays

a critical role in maintaining communications with special operations forces operating within the ROK and overseas.

The Electronic Warfare Bureau is responsible for the administration and training of all SIGINT and EW/EIW assets within the KPA. In coordination with the Communications Bureau and Reconnaissance Bureau's Technical/Radio Department it probably oversees both offensive and defensive EW/EIW operations. The Electronic Warfare Bureau is believed to consist of a staff, the Electronic Warfare Institute, and a small number of SIGINT, EW, and EIW assets.[119]

The Military Training Bureau is responsible for education and training within the KPA, including the education and training at military schools and academies. In fulfilling its mission, the Military Training Bureau conducts research and evaluates combat operations through a small number of research institutes and "think tanks." The most significant are the Research Institute for Military Sciences and the Strategy Research Institute. These institutes are known to have conducted extensive historical research not only on World War II and the Fatherland Liberation War (i.e., Korean War), but more significantly on the Arab-Israeli conflict, Iran-Iraq War, Operations DESERT STORM, ALLIED FORCE, DESERT FOX, and ENDURING FREEDOM. These institutes also conduct research into the development of new weapons by other nations.[120]

---

[119] It is unclear whether there is a separate 525th Electronic Research Institute or if this is another designation for the Electronic Warfare Institute. Author interview data; "Ex-KPA Major Writes on DPRK Military Situation," *Pukhan*, January 2000, pp. 86-93, as cited in FBIS; and "Future Electronic Warfare Discussed," *Nodong Sinmun*, December 5, 1999, p. 6, as cited in FBIS.

[120] Author interview data; "Lessons for DPRK From NATO Bombing of Yugoslavia," *Nodong Sinmun*, 20 April 1999, p. 1, as cited in FBIS; "DPRK's Keen Interest in New Weapons Used in Yugoslavia,"

Ground Forces

At present, the KPA fields 12 infantry corps. The organization of the infantry corps is flexible, with the number or organic and attached units dependent upon the corps mission and area of responsibility. There are two distinct groupings of infantry corps—forward and rear. Three corps are considered forward corps and are organized in a similar fashion. Although not adjacent to the DMZ, a fourth corps is organized in a similar manner as the three forward corps. Forward corps are larger and better equipped than rear corps, having their full complement of personnel, more modern weapons, and a larger and more diverse number of organic and attached units. This disparity between forward and rear units follows down through subordinate units.

At corps-level two elements exist which will be primarily concerned with SIGINT and EW operations – the EW/SIGINT battalion and communications regiment. Although the EW/SIGINT battalion is the primary asset assigned to offensive SIGINT and EW operations, its organization and capabilities are unclear.

At the infantry/motorized infantry division level the SIGINT and EW assets consist of an EW/SIGINT battalion or company, and a communications battalion. EW/SIGINT battalions are believed to be found only within some divisions deployed along the DMZ. While it is believed that the remaining divisions have a EW/SIGINT company, some rear area divisions may have none. All divisions

---

Yonhap, 13 May 1999, as cited in FBIS; "DPRK Military Studies Merging of East, West German Armies," *Choson Ilbo*, 25 April 1997, p. 2, as cited in FBIS; and *Sisa Journal*, "Journal Views DPRK's Military Organization," 6 June 1996, pp. 30–31, as cited in FBIS.

staffs have, at least, several SIGINT/EW/EIW trained officers.

Unique to those divisions deployed along the DMZ is a DMZ police battalion. This battalion consists of 8-12 DMZ police companies and operates a wide range of ground surveillance equipment including radar, infrared and thermal imaging devices, seismic and acoustic sensors, etc (see Figure 13.2). They also possess a basic SIGINT collection capability. This is most evident in the Joint Security Area at Panmunjom.

Figure 13.2. KPA Guard Tower with SIGINT Antennas

The KPA currently deploys four mechanized corps and one tanks corps. The organization of the mechanized corps appears to be flexible, with the number of organic and attached units dependent upon the corps mission and area

of responsibility. Like the infantry corps there appears to be two distinct groupings—forward and rear. The forward corps are probably somewhat larger and better equipped than the rear corps. It is believed that, like the infantry corps, all these corps include a EW/SIGINT battalion. It would appear, however, that it is smaller and more mobile. The existence of the EW/SIGINT battalion within the tank corps is unknown, but would appear to be reasonable.

Division level EW/SIGINT units are responsible for operations within the forward zone, from the corps' forward line to a depth of 15-30 km in the ROK/U.S.'s rear. Corps level EW/SIGINT battalions will be responsible for operations to a depth of 75-150 km. Independent units from the Electronic Warfare Bureau will likely support division and corps operations. The Electronic Warfare Bureau, KPAF, KPN, Reconnaissance Bureau, and State Security Department will conduct operations beyond the corps area of responsibility. Special assets of the Electronic Warfare Bureau, Reconnaissance Bureau, and State Security Department will conduct EIW operations.

KPA ground force EW/SIGINT units are equipped with a wide variety of intercept, direction finding, surveillance and jamming equipment. The vast majority of it is believed to be of Russian, former Soviet, and East European origin. Although they are believed to also employ quantities of PRC origin equipment, commercial equipment purchased on the open market in Japan, the PRC, U.S. and throughout the world, and ROK and U.S. military equipment which has either been captured or acquired covertly.

With the notable exceptions of the selected General Staff Department assets noted above and the corps and division EW/SIGINT units, the level of computerization within the KPA's ground forces is low. What computerization there is,

is believed to be concentrated within the administrative elements of the command.

Korean People's Air and Air Defense Command

The primary mission of the Korean People's Air and Air Defense Command -- more commonly known as the Korean People's Air Force's -- is the air defense of the DPRK mainland and territorial waters. Secondary missions include reconnaissance, transportation and logistic support, insertion of special operations forces, strategic bombing, and provision of tactical air support to KPA ground force and KPN units.[121]

The KPAF is a coequal service under the MPAF, with both the KPN and the KPA. Control of the KPAF is vested in its commander who is responsible to the chief of the general staff. It is headquartered in Pyongyang,[122] has a total strength of 110,000,[123] and approximately 1,700 aircraft. Among the elements subordinate to the KPAF are wide variety of operational and support aviation and air defense units.

---

[121] Author interview data; *Defense White Paper 1998*, pp. 61-62; *Defense White Paper 1997-1998*, pp. 50-51; U.S. Marine Corps. *North Korea Country Handbook*, Marine Corps Intelligence Activity, MCIA-2630-NK-016-97 (FOUO), Washington, D.C., May 1997, pp. 36-38; *North Korea: The Foundations for Military Strength—Update 1995*, pp. 16-21; *North Korea Handbook*, pp. 3-9 to 3-13; Yu, Yong-won, "Comparison of North and South Korea's Air Power," *Wolgan Choson*, March 1991, pp. 378-391, as cited in FBIS; and Kenchi Aoki, "Air Power of the ROK Navy, ROK Army, and the North Korean People's Armed Forces Air Force," *Aerospace Japan*, January 1991, No. 1, pp. 58–61, as cited in FBIS.

[122] Some sources indicate that KPAF headquarters is located at Chunghwa, immediately south of Pyongyang.

[123] This figure is believed to include the three air force sniper brigades.

Little is known concerning the KPAF's C^4ISR capabilities. It does operate an air defense network that maintains surveillance of the skies above and around the nation and a reconnaissance unit with limited SIGINT and EW capabilities. This unit is equipped with a small number of specially configured H-5R, An-2/24, MiG-17/21/23 aircraft. It does not possess any AEW aircraft. During the 1990s, however, it is known to have modified at least one An-24 to mount a MiG-29 radar, which may have been an attempt to develop a rudimentary AEW capability. Additionally, it has conducted limited development of electronic countermeasures (ECM) resistant modifications for its SAM forces.[124]

The level of computerization within the KPAF is believed to be relatively low. The vast majority of such equipment is located at the Air Force Command Headquarters level, Kim Chaek Air Force Academy, and in the administrative elements of the command. The vast majority of radars are old, of Soviet origin, have limited capabilities, and are vulnerable to even minimal ECM. There are, however, a small number of more modern radars of Russian and PRC origin with significantly better resistance to ECM. A major facet of DPRK political efforts with Russia during the past three years has been the attempt to acquire more modern radars and upgrades to the various elements of the KPAF's existing C^4ISR system.

Following the April 15, 1969 attack and shoot down, by KPAF MiG-21 fighters, of a U.S. Navy EC-121M aircraft conducting a BEGGAR SHADOW (SIGINT) mission over the Sea of Japan, the U.S. initiated the COMBAT DAWN program of high-altitude UAV over-flights of the DPRK. These

[124] Author interview data; and "Defector Says DPRK Receives Spy Photos From Russia," p. 1.

flights were undoubtedly a tremendous nuisance for the DPRK but probably served, along with UAV operations in the Vietnam and 1973 October Wars, as the impetus for the subsequent acquisition of UAVs by the KPAF. Since the late 1980s, the KPAF has operated an unknown number of UAVs, which it has obtained from the PRC, Russia and possibly Iran. It is presently believed that the UAVs are operated solely by an element of the KPAF. These UAVs are equipped with cameras for reconnaissance or target acquisition and may be employed in the ECM or decoy mission. During the early 1990s, probably as a result of the use of UAVs during Operation DESERT STORM, the DPRK initiated a domestic UAV program. One aspect of this has been the manufacture at least one version of UAV based upon the PRC jet-powered D-5 target drone.[125] During 1994, Syria provided the DPRK with both access to its UAVs, including the DR-3 Reys, and information concerning its operational use.[126] More significantly, it is subsequently reported to have provided a few examples of each of its systems, including the DR-3, to the DPRK.[127] During the late 1990s the DPRK acquired a small number of Pchela-1T UAVs from Russia. These have reportedly been used for reconnaissance along the DMZ. Technology and information from Russia, Syria and Iran has undoubtedly found its way into the DPRK's ongoing UAV programs. It is probable that UAVs of both foreign and domestic design are presently under production; however, it

[125] For details of the D-5 see, Munson, Kenneth. *World Unmanned Aircraft*, Jane's Publishing Company, Ltd., London, 1988, p. 32.

[126] For information on the DR-3 see, Butowski, Peter, "Russian Reconnaissance UAVs—Part 2," *Jane's Intelligence Review, Pointer*, Vol. 3, No. 1, January 1996, pp. 4-5; and Zaloga, Steven J., "Russian Unmanned Aerial Vehicles," *Jane's Intelligence Review*, July 1994, pp. 291- 296.

[127] The exact date of the transfer of the DR-3s from Syria to the DPRK is unclear. "DPRK Acquires Several UAVs From Middle East 'Military Partner'," *Choson Ilbo*, April 22, 2001.

is unlikely that the DPRK produces a UAV in the same class as the DR-3.[128] The use of UAVs by the U.S. during Operation ENDURING FREEDOM has only served to reinforce the importance of such systems for the KPAF.

In any future war the KPAF can be expected, at a minimum, to conduct barrage jamming of ROK/US air defense radars and communications nets, and to utilize chaff and infrared flares during combat missions. UAVs will operate in the photo and electronic reconnaissance, as well as the counter-SAM and jamming missions. It is presently unclear whether the KPAF possesses an anti-radiation missile (ARM) capability. A primary mission for the KPAF's few high performance aircraft will be the disruption or destruction of U.S. E-3A and Japanese E-767 AWACS aircraft.

Korean People's Navy Command

The primary mission of the Korean People's Navy Command -- more commonly known as the Korean People's Navy (KPN) -- is the defense of the DPRK territorial waters and coasts. Secondary missions include insertion of special operations forces, coastal surveillance, and protection and control of coastal shipping and fishing operations.

The KPN is a coequal service under the MPAF, with both the KPAF and the KPA ground forces. Control of the KPN

[128] Author interview data; "Russian Pchela Hi-tech Reconnaissance Drone Profiled," *RenTV*, August 13, 1999, as cited in FBIS; "Chechen Conflict Taught Russia Vital UAV Lessons," *Jane's Defence Weekly*, June 30, 1998; "DPRK Deploys Russian UAV's Along DMZ," *Choson Ilbo*, May 2, 1998, as cited in FBIS; "North Korean Forces Suffer Mobility Loss," p. 62; "'No Knowledge' on New Missile," *Yonhap*, 16 September 1993, as cited in FBIS.

is vested in its commander who is responsible to the chief of the general staff, MPAF. It is headquartered in Pyongyang and has a total personnel strength of 60,000. The total combat ship strength of the DPRK is approximately 990, with 840 vessels assigned to the KPN, Maritime Department, and Operations Department, 150 vessels assigned to the MPAF's Coastal Security Bureau, and ranks the KPN as one of the world's largest navies.[129]

Little is known concerning the KPN's C^4ISR capabilities. Its coastal defense network maintains surveillance radar installations at more than 40 locations on both coasts and on a number of islands, with heavy concentrations on the southwest coast from Haeju to Changsan-got, on the southeast coast from Kosong-up to Hodo-ri, and at major KPN bases. This network provides complete and overlapping coverage of the sea approaches to the DPRK. The majority of the radars employed by the KPA are older Soviet models of limited capabilities and are vulnerable to jamming. There are also a small number of more modern radars of Russian and PRC origin, as well as commercial maritime radars obtained from Japan. Coastal Security Bureau and paramilitary patrols and observation posts supplement the coastal surveillance radar network. The KPN maintains a small number of intelligence gathering vessels, or AGIs, and many of its larger vessels have rudimentary SIGINT collection capabilities.

The level of computerization within the KPN is believed to be lower than that of the KPAF. The vast majority of such equipment is located at the Naval Command Headquarters

[129] The exact strength of the KPN is unclear. The numbers used in this chapter are drawn primarily from "N. Korea Deploys 10 More Subs;" *Defense White Paper 1998*, p. 60; *Jane's Fighting Ships 1998-1999*, pp. 397-403.

level, Kim Jong-suk Naval University, and in the administrative elements of the command.

Operations

Among the principles that the MPAF believes will be critical for success during wartime SIGINT, EW, and EIW operations are,[130]

> Limiting electronic emissions by strict adherence to COMSEC regulations which emphasis the use of landlines, total or partial radio silence, etc.
>
> When electronic emissions are required, to limit the enemy's ability to exploit them by limiting their duration, use of directional antennas, using reduced power outputs, etc.
>
> Extensive use of electronic deception operations which will include the creation, operation, and maintenance of false communication networks, the random use of decoy transmitters, etc.
>
> Strict adherence to tactical COMSEC and OPSEC techniques such as the frequent relocation of C^4ISR assets when possible, fortification of such units when relocation is not feasible or desirable, the frequent and random changing of call signs and frequencies, etc.
>
> Extensive route training of communications operators to follow COMSEC regulations and to operate their networks/assets under conditions of extensive enemy jamming and countermeasures (electronic and physical attack).

[130] Author interview data; and U.S. Army, *North Korean People's Army Handbook*, FC 100-2-99, April 1992, pp. 13-1 to 13-3.

> Education of a cadre of officers and enlisted personnel dedicated to the SIGINT, EW, and EIW missions.
>
> Thorough prewar physical and electronic reconnaissance to locate and identify major enemy C^4ISR networks and assess their vulnerabilities.
>
> Rapid wartime neutralization or destruction of enemy C^4ISR capabilities.
>
> Secure its computer networks from EIW operations while conducting such operations against the enemy's military and civilian networks.

As might be expected, the DPRK has conducted ongoing SIGINT, EW, and EIW operations against the ROK, U.S., and Japan since the end of the Fatherland Liberation War. As is standard with almost any country conducting such non-wartime operations, they utilize signal interception to collect data on ROK/US order-of-battle, equipment, operations, and intentions; radio direction finding to locate emitters and unit locations; wiretapping of landlines in the rear areas; etc. Over the years KPA EW/SIGINT units have occasionally conducted jamming operations of front line ROK/U.S. units. The State Security Department and Reconnaissance Bureau are likely to be the primary agencies involved in code breaking and receiving support (in the form of intercepts) from the Electronic Warfare Bureau, KPAF and KPN.

Wartime SIGINT, EW, and EIW operations will undoubtedly attempt to target the entirety of the ROK/U.S. C^4ISR spectrum. The DPRK will undoubtedly attempt to use the Internet to strike at military, political, economic, and civilian assets (e.g., telecommunications networks,

financial institutions, power grids, water supply systems, emergency services systems, etc.) within the ROK, U.S., and Japan. On the Korean Peninsula wartime EW/EIW operations will initially witness electronic and physical attacks focused upon the ROK/U.S. command and control communications systems, early warning air defense and coastal defense radars. Operations will then be expanded to include the entire ROK/U.S. C^4ISR spectrum and against Japan. These operations will be conducted by the Electronic Warfare Bureau, Reconnaissance Bureau and the State Security Department (the Investigative Department of the CCSKA may also play some role).[131]

Unique among KPA wartime EW/EIW operations will be the employment of special operations forces. The KPA currently deploys one of the world's largest special operations forces with an estimated strength of 100,000 men and women. One of the primary wartime missions for these units is the disruption or destruction of ROK/US C^4ISR capabilities. They believe that the political, social, military, and geographic characteristics of the Korean Peninsula provide unique conditions whereby these units will be extremely effective in this mission.[132]

Intelligence and Internal Security Services

The primary missions of the DPRK's intelligence organizations are to: actively collect and disseminate timely

[131] Author interview data; "N.K. Establishes New Ministry for Electronic Industry Growth," *Korea Herald*, November 26, 1999; "Kim Jong Il Stresses Electronic Warfare Capabilities," *Radio Pyongyang*, 24 September 1999, as cited in FBIS; and "Defector Says DPRK Receives Spy Photos From Russia," *Korea Times*, 25 June 1996, p 1, as cited in FBIS.

[132] For a detailed look at KPA special operations forces see: Bermudez Jr., Joseph S. *North Korean Special Forces: Second Edition*, U.S. Naval Institute Press, Annapolis, November 1997.

and accurate information concerning any possible political, military, or economic threat to the security of the nation; to the political and military leadership; and the subversion of the ROK. Secondary missions include: overt and covert acquisition of foreign military and civilian technologies and equipment, support of the DPRK's foreign policy goals, training and support for foreign revolutionary and terrorist organizations, and the acquisition of foreign capital for state and intelligence operations.[133]

The primary missions of the DPRK's internal security organizations are to protect the government and KWP from domestic threats and to prevent or neutralize any foreign intelligence collection or subversion activities against the DPRK. Secondary missions include maintenance of domestic tranquility, normal police and civil defense activities, protection of natural resources, industrial security, protection of transport and communication networks, coast and border security, and acquisition of foreign capital.

The DPRK's intelligence organizations have proven that they are capable of fulfilling their missions, especially within Asia. Intelligence collection outside of Asia is problematic as a result of the DPRK's expanding economic crisis and political isolation in the international community. The DPRK's internal security organizations have proven to be extremely effective. There are no significant domestic threats to the Kim Jong Il government or the KWP and none are likely to emerge in the foreseeable future due the draconian methods employed by the internal security organizations.

---

[133] For a detailed look at DPRK support of terrorism and revolutionary organizations, see Bermudez Jr., Joseph S. *Terrorism: The North Korean Connection*, Taylor & Francis, New York, October 1990.

Organization

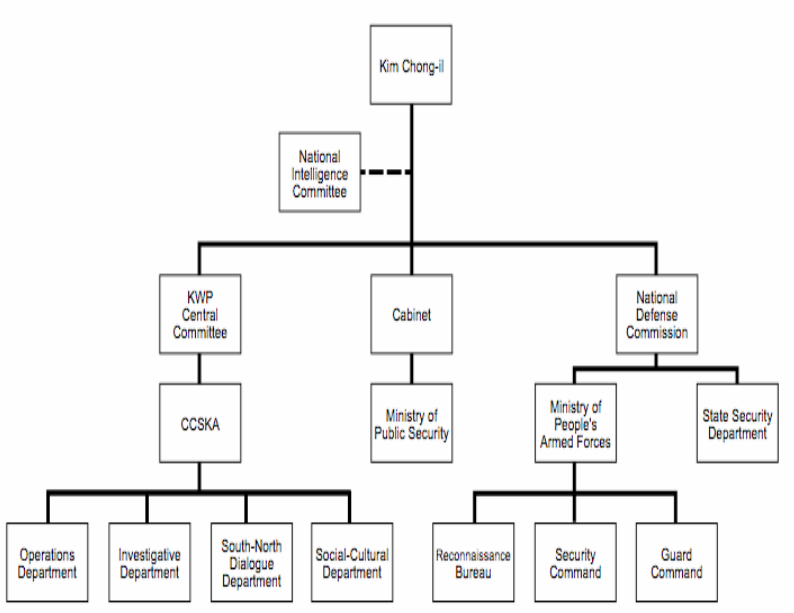
The organization of the intelligence and internal security community originates with Kim Jong Il, who is both general secretary of the Workers' Party of Korea and chairman of the National Defense Commission, and proceeds down through three distinct paths -- National Defense Commission, WPK, and Cabinet. The National Intelligence Committee supports all paths, which is a national-level policy and decision-making body for intelligence and security matters. Subordinate to the National Defense Commission are the MPAF and State Security Department. Subordinate to the MPAF are the Reconnaissance Bureau, Security Command, and Guard Command. The paths through the KWP and Cabinet are relatively short. Subordinate to the WPK is the office of the Central Committee secretary in charge of South Korean Affairs (CCSKA), which controls four intelligence-related departments. Subordinate to the Cabinet is the Ministry of Public Security.

National Intelligence Committee

The National Intelligence Committee is a decision-making body led by Kim Jong Il and composed of four other members: the CCSKA, director of the Social-Cultural Department, director of the Investigative Department, and chief-of-the-general staff of the MPAF. This committee is the primary national-level policy and decision-making body for intelligence and security matters and, as such, it establishes overall policy direction for all intelligence and security activities, sets intelligence objectives, and

delegates responsibilities to the intelligence and security communities (see Figure 13.3).[134]

Figure 13.3. DPRK Intelligence Services



WPK, CCSKA

The office of CCSKA is responsible for implementing anti-ROK operations, based upon guidelines established by the National Intelligence Committee. It also exercises control over subordinate agencies and coordinates with the Reconnaissance Bureau, Ministry of Public Security and State Security Department. It apparently collects information from its subordinate intelligence agencies and other organizations, and disseminates finished intelligence

[134] Author interview data; Oh Il-hwan, "The Aims and Characteristics of North Korea's United Front Strategy," *Vantage Point*, March 1996, Vol. XIX, No. 3, pp., 27-29.

products to all DPRK government agencies. The CCSKA is headquartered in Pyongyang, as are the headquarters of its four subordinate departments: Social-Cultural Department, South-North Dialogue Department, Investigative Department, and the Operations Department.[135]

Social-Cultural Department (a.k.a, Liaison Department)

Its primary missions are the establishment and expansion of the WPK within the ROK (i.e., underground WPK cells), and the collection of political intelligence within the ROK and Japan. It is believed to also exercise operational control over the *Chosen Soren*. The Social-Cultural Department is organized into: administration and training sections; world regional sections; four regional sections dealing with the ROK; a political/cultural section for the ROK (e.g., ROKA, industry, etc.); and trading companies (e.g., Dae Song Trading Company). Within the context of its trading companies the department operates a number of ocean-going merchant vessels, some of which apparently possess limited SIGINT collection capabilities.

South-North Dialogue Department (a.k.a., Unification Front Department)

The South-North Dialogue Department is responsible for all open and covert issues relating to "South-North Dialogue" and the reunification of the Fatherland—including all anti-ROK psychological warfare and propaganda operations. Throughout the 1980s and 1990s the South-North Dialogue Department dramatically

[135] Author interview data; *Defense White Paper*, various editions 1990-1998; "The Aims and Characteristics of North Korea's United Front Strategy," pp., 27-29; and "Former North Korean Agent Discloses DPRK's Spy Activities," *Mainichi Shimbun*, 9 May 1996, p. 6, as cited in FBIS.

expanded its open and covert contacts with Koreans living overseas (especially within the U.S. and Canada). This department is apparently the driving force behind a number of Web sites supporting the DPRK.

Investigative Department (a.k.a, Research Department for External Intelligence)

The Investigative Department is responsible for the collection of external intelligence and conducting foreign operations. It is organized into a headquarters and six primary sections. These sections are: *Chosen Soren*; Japan; Americas; Europe; Africa & Asia; and ROK. This department has probably benefited considerably from access to the Internet.

Operations Department

The Operations Department is the primary organization responsible for the basic and advanced training of intelligence agents, escort training, and escort operations (i.e., covert infiltration of agents throughout the world). It is organized into a headquarters, basic training, advanced training, two sea-borne escort training centers, four sea-borne escort units (a.k.a., maritime liaison offices) and two DMZ escort units.

The Operations Department has been involved in kidnapping operations throughout the world. The primary objectives of these operations have been to secure persons who can serve as language and cultural instructors for operatives and to allow previously trained operatives to assume the victim's identity. These later operations have generally occurred within Asia, particularly Japan. To conduct these missions, the Operations Department employs a wide variety of specialized swimmer delivery

vehicles, semi-submersible infiltration landing craft, infiltration vessels ("mother" ships), and submarines. Almost all of the vessels captured or salvaged during the past ten years have been extensively equipped with commercial Japanese marine radars and electronics, as well as commercial GPS receivers. Infiltration vessels are believed to have occasionally conducted SIGINT collection missions.

Much of what is known concerning the operations of the CCSKA comes from a number of failed or aborted missions. During the past five years there have been at least ten such incidents -- five against the ROK and five against Japan, including the recent December 2001 pursuit and sinking of an Operations Department infiltration vessel off of Amami-Oshima, Japan. These missions clearly indicate that CCSKA operatives have regularly entered the ROK undetected, and that there are numerous ongoing operations in both the ROK and Japan.

The level of computerization within the CCSKA is believed to vary considerably with the levels being highest within the South-North Dialogue Department and lowest within the Operations Department. During the 1990s intelligence agencies in the ROK and Japan began to notice the use of commercial encryption software and Internet e-mail services by CCSKA agents identified operating in their countries. Beginning in the 1990s, the widespread availability of Internet access contributed significantly the ability of agencies of the CCSKA to obtain previously unavailable intelligence on an almost endless range of subjects. The websites of the U.S. Department of Defense are heavily visited by users from the DPRK. The Internet has also provided a means to quickly and easily disseminate propaganda and engage in disinformation campaigns.

MPAF, Reconnaissance Bureau[136]

The primary missions of the Reconnaissance Bureau are the collection of tactical and strategic intelligence within the military sphere, and strategic special operations throughout the ROK and overseas.

The Reconnaissance Bureau is headquartered in Pyongyang and organized into a: headquarters, Political Department, Intelligence Department, Special Department, Technical/Radio Department, Training/Plans Department, Maritime Department, and five reconnaissance battalions. Additionally, the Reconnaissance Bureau is believed to operate a small number of trading companies as "covers" and to generate financing for operations.

The Technical/Radio Department, in cooperation with the Electronic Warfare Bureau, is believed to be the organization exercising overall responsibility for SIGINT, COMSEC, EW, and EIW operations within the MPAF. The number and organization of the SIGINT assets within the MPAF is unclear. Ground-based assets are believed to consist of a small number of independent SIGINT collection sites located throughout the DPRK in areas of high interest (e.g., along the DMZ, the Russian and PRC borders, etc.); the EW/SIGINT battalions within KPA corps; and the EW/SIGINT battalions that exist within some KPA divisions. In addition to these assets the Technical/Radio Department exercises some degree of control over KPAF SIGINT collection aircraft and KPN AGIs. Assets subordinate to the Technical/Radio Department are responsible for EIW operations. This

[136] Author Interview data; and "DPRK Spy Organizations Targeting Japan Tokyo," pp. 68-73.

department also coordinates with the MPAF Communications Bureau and its subordinate units (i.e., 9th Signals Brigade). The relationship and level of coordination and cooperation between the Reconnaissance Bureau's Technical/Radio Department and the State Security Department's Communications Interception Bureau (a.k.a., Signals Interception Bureau) is unknown. The Communications Interception Bureau may be the senior service.

The Maritime Department is believed to be headquartered in Wonsan and is responsible for infiltrating agents and special operations force personnel by sea using a variety of specialized midget submarines, infiltration vessels, semi-submersible infiltration landing craft, and swimmer delivery vehicles. It is believed to be organized into three operational bases. Each base consists of a small number of units or combat squadrons (battle groups). It is known that the Maritime Bureau operates YUGO-class SSm, SANG-O class SSc, and a variety of infiltration vessels, semi-submersible infiltration landing craft and support ships. Vessels of the Maritime Department are believed to have occasionally conducted SIGINT collection missions.[137]

The five reconnaissance battalions have personnel strength of approximately 500 each and are organized into a headquarters and five companies. Four are employed primarily for DMZ infiltration and are deployed one apiece within the four forward corps. The fifth battalion is responsible for overseas operations. These units will play a key wartime role in the location and destruction of ROK/US C^4ISR assets.

[137] "Agency Releases Videotaped Testimony by DPRK Infiltrator," *Yonhap*, 29 October 1996, as cited in FBIS.

As with the CCSKA, much of what is known concerning the operations of the Maritime Department comes from failed or aborted missions against the ROK. There have undoubtedly been numerous successful -- and thus undetected -- operations in both the ROK and Japan. The most recent detected example of a Maritime Department operation was the failed infiltration attempt by a SANG-O class submarine at Kangnung, ROK, in the fall of 1996.

As with the State Security Department the level of computerization within the Reconnaissance Bureau is believed to be high, with numerous modern desktop and mid-range computers. The vast majority of these computers are of Asian manufacture. The availability of Internet access during the past ten years has undoubtedly provided an order-of-magnitude improvement in the Reconnaissance Bureau's ability to collect quality information and produce timely intelligence on a wide range of subjects. As noted above in reference to the CCSKA, DPRK users frequently visit U.S. Department of Defense Web sites.

MPAF, Guard Command

Subordinate to the MPAF is the Guard Command, which is responsible for the personal security of Kim Jong Il and high-ranking officials. It is roughly comparable to the U.S. Secret Service or the ROK Office of Presidential Security. In the performance of its mission it works closely with the State Security Department and, to a lesser degree, the Pyongyang Defense Command. It is organized into an unknown number of departments, three independent "combat" brigades, a construction battalion, a reconnaissance unit, and support units. It possesses a small SIGINT capability, which is apparently focused primarily upon internal targets. The level of computerization within the Guard Command is believed to be high.

MPAF, Security Command

Although institutionally subordinate to the MPAF the Security Command is controlled by the State Security Department. This organization is responsible for the internal security within the KPA. As with the Guard Command it is believed to possess a small SIGINT capability, which is apparently focused primarily upon internal targets.

State Security Department[138]

The State Security Department functions as both an intelligence agency engaged in active operations overseas and a domestic political security force (i.e., secret police). It is most comparable in function to the former Soviet KGB, or to a lesser degree, the ROK National Intelligence Service (formerly National Security Planning Agency). It is responsible for security (physical and political) within the DPRK's embassies, missions, and legations located throughout the world. The State Security Department and the Guard Command are the agencies most directly responsible for the security of Kim Jong Il, and only he is reportedly exempt from their scrutiny. Following the constitutional amendments in September 1998, the State Security Department was subordinated to the National Defense Commission.

---

[138] Author interview data; "NK Reshuffles Political Structure;" *A Handbook on North Korea*, p. 20; "Attempted 1995 Military Coup d'Etat in DPRK Alleged," pp. 34-35; "Article on Past Military Coup Attempts in North," *Iryo Sinmun*, 21 May 1995, p. 9, as cited in FBIS; and "DPRK 'Intensifying' Internal Control," *Seoul Sinmun*, 6 May 1996 p. 2, as cited in FBIS.

The State Security Department is headquartered in Pyongyang and organized into 17 subordinate bureaus, "Special Mission Group," State Security Department Hospital, State Security Department University, Training Center, and Ministry of Public Security Liaison Office. The 17 subordinate bureaus are: Data Management, Entry/Exit Management, Equipment, External Intelligence, Finance and Supply (Kim Jong Il), Interrogation, Investigation (Dissidents), Investigation, Military Industrial Security, North/South Dialogue, Operations and Secretary (Kim Jong Il), Prison Camps, Protection and Security (Kim Jong Il), Rear Services, Research, Communications Interception, and Surveillance.

The Communications Interception Bureau (a.k.a., Signals Interception Bureau) is believed to be the DPRK's primary SIGINT agency. It is responsible for the creation of encryption systems and equipment, as well as the decryption of foreign code systems. It maintains a system of collection sites throughout the country that monitor for both illegal internal and foreign civilian and military transmissions. This system appears to be separate from that of the Reconnaissance Bureau's Technical/Radio Department. In addition to its SIGINT capabilities this bureau is believed to possess EW and EIW assets. The relationships among the Communications Interception Bureau, Technical/Radio Department and Electronic Warfare Bureau are unclear; however, the Communications Interception Bureau appears to be the senior service.

The general level of computerization within the State Security Department is believed to be high, with numerous modern high-end computers of Asian, European and U.S. manufacture.

Ministry of Public Security[139]

The Ministry of Public Security functions primarily as the national police and civil defense force for the DPRK. It is headquartered in Pyongyang and is organized into twelve subordinate bureaus, Communications Office, Public Security Political University, Public Security Training Center, Public Security Hospital, State Security Department Liaison Office and the Tonghung Trading Company.

The Public Security Bureau is the counter-espionage/counter-revolutionary element within the Ministry of Public Security. It is organized into eight departments: 1st Counter Espionage, 2nd Counter Espionage, Political, Public Security, Industrial Security, Investigation, Rear Services, and Surveillance. The bureau possesses a small SIGINT capability.

The level of computerization within the Public Security and Prison Bureaus is believed to be high.

Assessment

The DPRK possesses a long SIGINT history that predates its formal establishment as a nation and laid the foundations for today's SIGINT, EW, and EIW capabilities. These capabilities have played, and continue to play, a critical role in maintaining national security. The highest levels of the DPRK's political, military, and intelligence leadership understand the importance of strong and active SIGINT, EW, and EIW capabilities. During the

[139] Author interview data; "Kim Jong Il Thanks KPA, Security Officers," KCNA, 11 January 1996, as cited in FBIS; *A Handbook on North Korea*, p. 20; "Article on Past Military Coup Attempts in North;" "DPRK 'Intensifying' Internal Control;" and "Armed Forces Structure, Make-up Discussed," pp. 196-205.

past 15 years the DPRK has dedicated significant national resources to develop and expand these capabilities.

Today, while the DPRK's capabilities may be assessed as being above average for a Third World nation, they are significantly below those of its perceived adversaries – the ROK and U.S. Regardless, they are at the point where they do present a significant and growing threat.

Because of its relatively modest levels of computerization and telecommunications any enhancements that the DPRK undertakes within these fields have the potential to leapfrog several generations and present a significant force multiplier on the modern battlefield. The greatest obstacles the DPRK faces in continued development of advanced EIW capabilities are its grossly underdeveloped electronics and computer industrial infrastructure, national economic crisis, a closed and highly politicized society, and interagency rivalry.

Paradoxically, as the DPRK moves into the computer age, modernizing its telecommunication capabilities, and enhancing its EIW capabilities, it is also increasing its dependencies upon these technologies and thus its own vulnerabilities and is exposing its society to political "contamination" from the outside world. It understands this paradox and attempts to address these potential and volatile vulnerabilities.