CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES | BURKE CHAIR IN STRATEGY

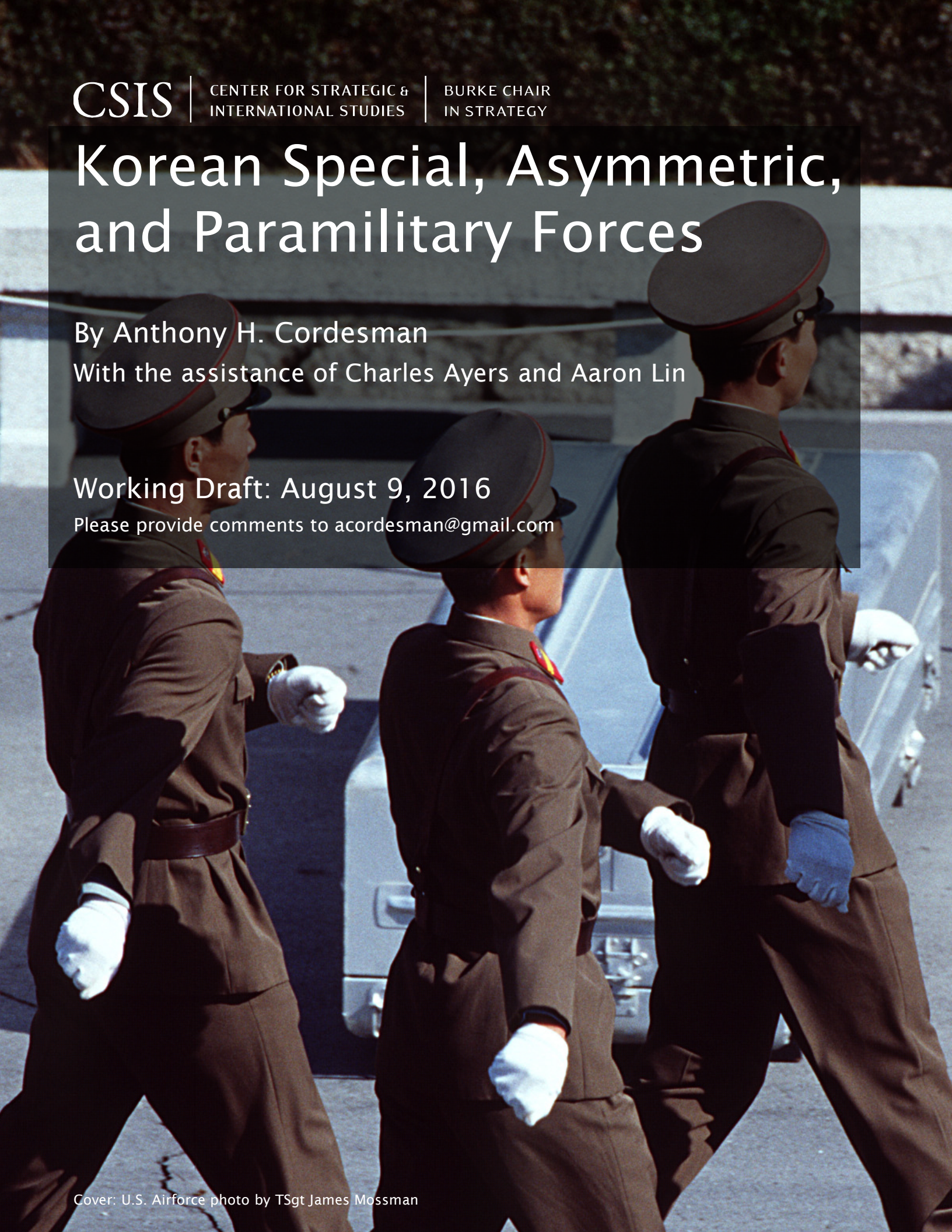
Korean Special, Asymmetric, and Paramilitary Forces

By Anthony H. Cordesman

With the assistance of Charles Ayers and Aaron Lin

Working Draft: August 9, 2016

Please provide comments to acordesman@gmail.com



Cover: U.S. Airforce photo by TSgt James Mossman

Contents

KOREAN SPECIAL, ASYMMETRIC AND PARAMILITARY FORCES

The DPRK and ROK have long competed in creating effective special and paramilitary forces. Pyongyang has also developed major capabilities for unconventional warfare in the border/DMZ area to attack deep into the ROK. The DPRK has mixed attacks by covert and Special Forces with limited naval and artillery strikes, while using missile and nuclear tests to obtain asymmetric leverage.

According to the South Korean Ministry of National Defense:[1]

> The North has been strengthening its special warfare capabilities by deploying light infantry divisions to the frontline corps and adding an infantry regiment to the frontline. The number of special force troops is estimated to reach approximately 200,000. It is assumed that these troops have been trained to conduct composite operations, such as major target strikes, assassination of important figures, and disruption of rear areas, after infiltrating the rear areas of the South through either underground tunnels or AN-2 planes.

The DPRK was increasingly belligerent throughout 2012 and early 2013, significantly escalating tensions on the Peninsula. In 2012, in addition to two missile tests, the DPRK also jammed aircraft and naval GPS functionality using 50-100km range Soviet vehicle-mounted radar systems. The DPRK continued denial of service cyber-attacks on ROK institutions, including government agencies and the military.

The DPRK also has the world's third-largest chemical weapons arsenal, the world's largest Special Forces, a fleet of mini-submarines, and a significant artillery capability arrayed against Seoul and other key ROK locations.[2]

The sheer variety of each side's capabilities to conduct irregular or asymmetric warfare, and the DPRK's aggressiveness in threats and limited attacks, can be destabilizing and lead to miscalculation and escalation. Such forces also present a problem for any potential arms control agreement, since they give the DPRK a potential advantage in threatening and attacking the ROK that would be enhanced by any general reductions in conventional forces.

Paramilitary, Police, Internal Security, and Special Forces[3]

While Paramilitary, police, and internal security forces play an important role in the Korean balance, making accurate counts of these forces is even more difficult than estimating the size of more "conventional" forces. It is even harder to estimate the size and role of internal security forces, although these can play a major part in securing rear areas and forcing soldiers to fight.

The assessments that follow again reflect ROK and Western sources and viewpoints. It was not possible to find comparable assessments that reflect a DPRK view. Once again, it is important to note that the DPRK may see its choices as forced upon it by outside threats and pressures. At the same time, these differences between the DPRK and the ROK act as a warning that the internal security structures of each state show differences that reflect their ability and willingness to use force and to escalate.

DPRK

The DPRK has a wide range of forces and activities that support asymmetric warfare as well as covert operations in peacetime.

Special Forces

The DPRK's Special Forces are the most important fighting element of its irregular and asymmetric forces. The North Korean military is proud of these forces and often refers to them as "human torpedoes" (Navy), the "invincibles" (Air Force), and "human bombs protecting the center of the revolution" (Army).[4]

The 2014 ROK Defense White Paper estimates the DPRK Special Forces to be some 200,000 strong.[5] The US DOD report on DPRK forces issued in May 2013 notes that,[6]

> North Korean SOF are among the most highly trained, well-equipped, best-fed, and highly motivated forces in the KPA. As North Korea's conventional capabilities decline relative to the ROK and United States, North Korea appears to increasingly regard SOF capabilities as vital for asymmetric coercion.
>
> Strategic SOF units dispersed across North Korea appear designed for rapid offensive operations, internal defense against foreign attacks, or limited attacks against vulnerable targets in the ROK as part of a coercive diplomacy effort. They operate in specialized units, including reconnaissance, airborne and seaborne insertion, commandos, and other specialties. All emphasize speed of movement and surprise attack to accomplish their missions. SOF may be airlifted by An-2 COLT or helicopters (and possibly Civil Air Administration transports), moved by maritime insertion platforms, or travel on foot over land or via suspected underground, cross-DMZ tunnels to attack high-value targets like command and control nodes or air bases in the ROK.

An ROK estimate of the size of DPRK Special Forces is shown in **Figure III.1**. The IISS estimated that the DPRK's Special Purpose Forces Command had a total of 88,000 personnel in 2016. The land component reportedly comprised eight (Reconnaissance General Bureau) Special Forces battalions, 17 reconnaissance battalions, nine light infantry brigades, and six sniper brigades. The air component had three airborne brigades, one airborne battalion, and two sniper brigades. The naval component had two amphibious sniper brigades.[7]

Jane's discusses the DPRK Special Forces in more detail; the different types of Special Forces and their respective missions and roles are depicted in **Figure III.2**. Most sources – including ROK and US intelligence and military sources – believe that the DPRK Special Forces number approximately 200,000 personnel and are divided into two categories: light infantry units (140,000 troops) and the 11th Storm Corps (60,000 troops).

According to *Jane's*, the primary missions of these Special Forces units are: "reconnaissance, establishing a 'second front' within the ROK strategic rear, destruction and disruption of the ROK/US C4ISR structure, neutralization of ROK and US air bases, and neutralization of ROK and US missiles and weapons of mass destruction (WMD). These missions include operations against US bases in Japan. Navy sniper brigades have the added mission of capturing the ROK islands along the Northern Limit Line (NLL) in the West Sea."[8]

DPRK Special Forces are divided into seven divisions (with an organic light infantry battalion or regiment), five to seven reconnaissance battalions, and 25 Special Forces brigades, with the latter composed as follows:[9]

- 12 Light infantry/mechanized light infantry
- 3 Reconnaissance brigades

- 3 Airborne brigades
- 3 General sniper brigades
- 2 Navy sniper brigades
- 2 Air Force sniper brigades

The 11th Storm Corps is the main DPRK military organization that trains and undertakes special and unconventional warfare. In peace, the 11th Storm Corps likely has administrative control over all special operations units, while during war it is the primary headquarters for coordination. USFK Commander General Walter Sharp described the 11th Storm Corps in February 2011 as "elite special operations units capable of carrying out highly complicated missions," and ROK sources believe that Lieutenant General Kim Yong-bok is the commander. It has been reported that the cover designation of the 11th Storm Corps is the 630th Large Combined Unit.[10]

While the majority of the planes that comprise the Air Force are older models, the DPRK can deploy Special Force operatives effectively behind ROK front lines in an attack. There are more than 20 air operation and reserve bases run by the DPRK Air Force, some of which have underground runways.[11]

The 11th Storm Corps Bureau, as well as the Reconnaissance General Bureau, has access to "specialized high-speed semi-submersible infiltration landing craft (SILC), Yugo, and Yono-class SSM and Sang-O and K-300 (an improved Sang-O) class SSC."[12] While technically the DPRK military can transport approximately 4,000 troops by air and 15,000 troops by sea at one time, due to the economic difficulties of the past 30 years and the correlated reduction in operational readiness, it is likely that this capacity has dropped by 20-40%.[13]

North Korean special operations units have been expanding urban, night-time, and mountaineering training from 2003 to the present. These shifts in training have been accompanied by a reorganization of the ground forces that expanded light infantry forces and converted seven mechanized infantry divisions into light infantry divisions.[14]

Additional Paramilitary and Reserve Forces

The DPRK has an expansive system of additional paramilitary and reserve forces, which are also summarized in **Figure III.3**. A ROK Ministry of Unification report notes,[15]

> According to one of North Korea's four military guidelines, "to arm the entire population," the regime has mobilized around 30 percent of the population between the ages of 14 to 60 to acquire over 7.7 million reserve forces. Every member of the reserve forces is given various combat gears, including personal arms, equipment, and crew-served weapons. These forces respond to emergency calls and enter boot camps to receive 15 to 30 days of military training at least once a year.
>
> Upon the departure of the Chinese army in 1958, North Korea organized its reserve forces and civil defense corps called the Worker-Peasant Red Guards (WPRG) in January 1959, in addition to reorganizing discharged soldiers among the WPRG members into the Reserve Military Training Unit (RMTU) in 1963.
>
> The Red Youth Guards (RYG), a military organization for senior middle school students, was created in September 1970. The RMTU, the core of North Korea's reserved forces, consists of men between the ages of 17 and 50, as well as unmarried women volunteers between ages of 17 and 30. Its local units are organized into either divisions or brigades depending on the size of the administrative unit or workplace…. The RMTU members are given 100 percent of personal arms and equipment as well as 70 to 80 percent of crew-served weapons, and are required to complete as much as 500 hours of training each year.
>
> The intensity of their training is equivalent to those taken by active-duty soldiers. As the RMTU is organized, equipped with firearms and undergo intensity of training similar to those of soldiers on active duty, they can

be immediately mobilized to defend rear areas or called up as reserve forces in case war breaks out. At present the RMTU accounts for over 600,000 troops.

Meanwhile, the WPRG was renamed as the Worker-Peasant Red Army (WPRA) at the Party Conference that convened on September 28, 2010, and is expected to play a role similar to that of the regular army. The WPRA currently consists of those men not belonging to the RMTU who can be mobilized between ages of 17 and 60, as well as of women who are organized at each administrative unit and workplace between ages of 17 and 30.

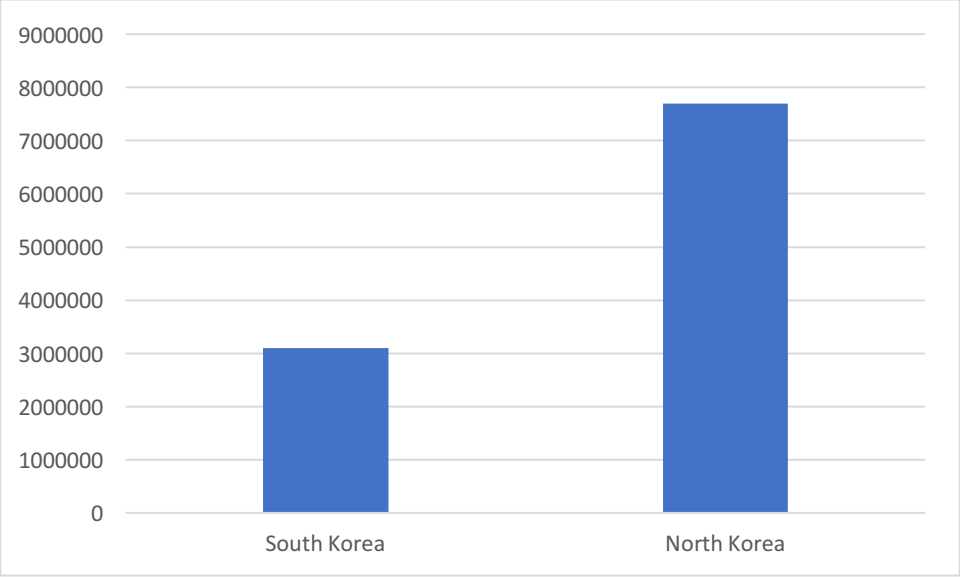
Along with the civil defense corps, the WPRA's basic responsibilities include guarding the workplace and other important facilities, as well as regional and antiaircraft defense. They are supplied with all personal arms and equipment and some crew-served weapons. A total of 160 hours of training is required. Their current numbers stand at 5.7 million.

In addition, the Red Youth Guards (RYG) consists of male and female senior middle school students aged between 14 and 16. Organized into companies and battalions at each school, RYG members are subject to a total of 160 hours of on-campus drills every Saturday and seven days of training during vacations, including a shooting exercise using live rounds at the RGY drill camp. As the royal guards of the regime, the RYG are mainly responsible for removing anti-revolutionary elements and playing a leading role in improving North Korea's combat capability.

In an emergency, they would perform the duties of rear guards or suicide squads to supplement those of junior army officers. They are supplied with all personal arms and equipment and some crew-served weapons. They undergo a total of 450 hours of training (substantially increased from 270 hours in the past) a year. Their current number stands at one million.

North Korea also has about 400,000 reserve troops affiliated with other paramilitary forces, including the Ministry of People's Security, the Logistics Mobilization Guidance Bureau, an agency responsible for providing and managing war supplies, and the Speed Battle Youth Storm Trooper Squad, a team that is often brought into public work projects. They are on a constant alert for immediate mobilization.

Figure III.1: Reserve and Paramilitary Forces



Source: Republic of Korea, Ministry of National Defense, *Defense White Paper 2014*

Figure III.2: DPRK Special Operation Forces, Missions and Roles

Type of Special Forces	Missions and Roles
Objectives	Attack andd estroy targets, distrub the enemy's rear area, launch terrorist attacks, neutralize major strategic and tactical facilities (communication stations, missile bases, airfields, etc.)
Sniper Brigades	Breach the enemy's major defense lines, disguise as ROK troops and infiltrate, strike strategic targets with 82-mm mortars and multiple rocket launchers, organize pro-DPRK sympathizers
Seaborne Sniper Brigades	Start a guerilla war using hi-speed boats and LCACs, launch a surprise attack on naval vessels, radar bases, and supply bases
Air Force Sniper Brigades	Strike euqipment and facilities in air bases
Airborne Infantry Brigades	Destroy logistics bases, secure strategic strongholds, block reinforcement
Army Corps Reconnassance Battalions	Open secret passages, reconnoiter, kidnap key figures, destroy enemy facilities
Light Infantry Brigades	Secure key launts, support main units, launch attacks on enemy command posts (comprised of a total of 6 battalions, each with 6 companies; each company consists of 120 troops and equipped with 60-mm mortars and portable missile launchers)

Source: Ministry for Unification and Institute for Unification Education, *Understanding North Korea*, ROK Government, 2012, 122.

Figure III.3: The DPRK's Reserve and Paramilitary Forces

Type	Strength	Notes
Reserve Military Training Unit	60,000	Subject to combat mobilization; men (ages 17-50) and women (ages 17-30)
Worker and Peasant Red Guard	5.7 million	Similar to the ROK's Homeland Reserve Forces
Red Youth Guard	1 million	Military organization of middle school students
Paramilitary units	400,000	Secret Service Command, Speed War Youth Shock Troops, Ministry of People's Security Logistics Mobilization Guidance Bureau
Total	7.7 million	

Source: Ministry for Unification and Institute for Unification Education, *Understanding North Korea*, ROK Government, 2012, 131.

Infiltration Routes

There are a number of different estimates of the efforts the DPRK has made to create tunnels under the DMZ. Work by *Jane's* and GlobalSecurity.org note that the DPRK has created a series of infiltration tunnels since the 1970s, four of which have been discovered by US and ROK forces (see **Figure III.4** below). Each uncovered shaft was large enough to permit the passage of an entire infantry division in one hour, though the tunnels were not wide enough for tanks or vehicles. All the tunnels ran in a north-south direction and did not have branches, and, with each discovery, engineering within the tunnels has become progressively more advanced.[16]

According to North Korean defectors, Kim Il-sung issued a sweeping order in the early 1970s that required every Korean People's Army (KPA) division along the DMZ to dig and maintain at least two tunnels into South Korea.[17] The existence of such tunnels was reported by *Jane's* using information from a KPA engineer who had defected in 1974.[18]

These reports were further confirmed in late November 1974 when an ROK Army patrol stumbled upon a DPRK tunnel, complete with reinforced concrete slabs, electric power and lighting, weapons storage, sleeping areas, and a narrow-gauge railway with carts.[19] The tunnel's size was about three feet by four feet and, though of unknown length, it was estimated to be large enough to hide an entire infantry regiment – or to funnel thousands of soldiers into the South in short order.[20]

Another tunnel was discovered in March 1975. It measured 3,300 meters long, and, as *Jane's* reports, 1,100 meters of this length extended into ROK territory. It was dug at a depth of between 50 and 150 meters and measured 2m tall by 2m wide. As many as 8,000 troops may have been able to move through it in an hour.[21]

US and ROK forces uncovered two more tunnels in 1978 and 1990, the latter of which was 145 meters deep and large enough for three armed soldiers to run through side-by-side. The US and ROK have since made constant efforts to detect any such tunnels and tunneling efforts, but it is not possible to be certain how many exist, their location, or their capacity. *Jane's* reports that there are an estimated 20-25 such tunnels.[22]

Other sources agree with *Jane's*, placing estimates at around twenty.[23] ROK and US abilities to detect such tunnels through advanced technology like ground sensing radars, seismic monitors, and other devices – as well as classic measures like counter-tunneling – is unknown. The threat posed by any remaining tunnels and their potential to insert combat forces behind ROK-US forward defenses is substantial. If North Korea does attempt a military attack upon the South, it could be that the tunnels of the Korean DMZ will play a role in that conflict.

As of 2012, some estimates indicated there were more than 8,200 underground facilities across the DPRK, including tunnels, underground shelters, and mines. *Jane's* reports an "extensive nationwide system in excess of 11,000 fortified underground facilities."[24]

In addition, the DPRK military has disguised and camouflaged camps and facilities several times greater in scale than the camps that are not extensively camouflaged.[25] The KPA conducts camouflage, concealment, and deception (CCD) operations at all levels; in fact, 2004 was the "Year of Camouflage" for the KPA:[26]

> A KPA manual smuggled out of the DPRK in 2010 has instructions concerning camouflage, concealment and deception of the complete range of military equipment and facilities including "command posts, foxholes, runways, fighter jet and naval bases, and cave strongholds." The same manual stated that "Yugoslavian forces in an exposed camp deployed fake anti-aircraft guns, ground-to-air missiles, aircraft and tanks made of logs, plywood and cloth, and hid their actual weapons. As a result, NATO forces in fact destroyed only 13 of the 300 tanks though it claimed to have destroyed 40 per cent of the armoured targets." Lessons learned such as those have strongly influenced KPA CCD operations.

The influence of these lessons can be seen in the DPRK's 2010 provocations. Directly before the November 2010 attack on Yeonpyeong Island (discussed in Chapter 4), the DPRK's military[27]

> …reportedly deployed decoy inflatable or painted plywood 122 mm and 240 mm rocket launchers among the real launchers to increase the difficulty of counter-battery artillery attacks and retaliation air strikes. ROK officials have stated that the KPA "is developing sophisticated camouflage and deceptions to avoid

> surveillance and precision bombing by state-of-the-art South Korean and US reconnaissance equipment and weapons systems... It seems they've got all sorts of decoy equipment and facilities, from fake cave positions of long-range guns and fake naval ships to fake aircraft, fake runways and bogus guns."

After the attack, the KPA appears to have tried to deceive ROK and US intelligence by continuously deploying SAM units and then removing them. Furthermore, reportedly the DPRK military was putting new and improved armored vehicle and fighter plane decoys in the DMZ corps.[28]

Figure III.4: DPRK Infiltration Tunnels Discovered by the ROK, to Date

	Tunnel No 1	Tunnel No 2	Tunnel No 3	Tunnel No 4
Location	8 km northeast of Korangpo	13 km north of Chorwan	4 km south of Panmunjon	26 kilometers northeast of Yanggu
Invasion route	Korangpo-Uijongbu-Seoul	Chorwan-Pochon-Seoul	Munsan-Seoul	Sohwa-Wontong-Seoul
Troop capacity	4,000/h*	8,000/h	8,000/h	8,000/h
Total length	3.5 km	3.5 km	1.64 km	2.05 km
Length south of Military Demarcation Line	1,000 m	1,100 m	435 m	1,030
Depth below surface	45 m	50-160 m	73 m	145 m
Discovery date	November 1974	March 1975	October 1978	March 1990

* This tunnel has concrete lining.
Source: IHS Jane's: Defence & Security Intelligence Analysis, "Jane's World Armies: North Korea," October 18, 2012, http://www.janes.com.

Artillery Near the DMZ

The vast majority of North Korea's military equipment is outdated in comparison with that used by South Korean and US forces, but the KPA often substitutes numbers and "mass" for modernization and quality. There are reports that the KPA has created thousands of artillery emplacements near the DMZ that are capable of inflicting significant damage and civilian casualties on Seoul.

US General Walter Sharp, a former commander of US troops in South Korea, has said the North has "an old but very large military that is positioned in a very dangerous place, very close" to South Korea.[29] In addition to its ballistic missiles, reports indicate that the KPA has approximately 8,600 artillery pieces (and 5,500 MRLs), the majority of which are located along the DMZ in natural caves, man-made tunnels, and bunkers (known as Hardened Artillery Sites, or HARTS). The 2014 ROK white paper notes that the DPRK's "170 mm self-propelled guns and 240 mm MRLs in forward positions are capable of surprise, massive concentrated fire on the Greater Seoul Metropolitan Area (GSMA)."[30]

The quality of DPRK artillery forces and their military competence is somewhat questionable. Despite North Korea's use of radar in its November 2010 artillery bombardment of Yeonpyeong, the accuracy of the attack was poor. South Korean Ministry of National Defense (MND) sources state that the KPA fired approximately 170 rounds; of these, 90 (53%) impacted the waters surrounding the island, while 80 (47%) impacted on the island.[31]

Although inconclusive, this poor accuracy suggests that KPA artillery troops – at least those in the IV Corps – are in need of greater training despite DPRK pre-attack planning and exercises. Additionally, ROK MND sources claim that approximately 25% of the 80 rounds that impacted the island were duds and failed to detonate on impact (12% if the total of 170 is taken into consideration).[32] This high failure rate suggests that some DPRK-manufactured artillery munitions, especially MRL rounds, suffer from either poor quality control during manufacture or that storage conditions and standards are poor.

Despite the limits to the quality of DPRK artillery, a DPRK artillery attack on the ROK could still be devastating, especially in the environs surrounding Seoul. Lee Yang Ho, ROK Defense Minister during the 1994 nuclear crisis, said one computer simulation conducted during his term projected 1 million dead: "all industry would be destroyed, gas stations, power plants. This is such a densely populated area that even if North Korean artillery were not very accurate, any place you would hit there would be huge numbers of casualties."[33]

ROK

The IISS only provides limited data on the ROK's Special Forces. Its 2016 *Military Balance* estimates one (Special Warfare) command with seven Special Forces brigades. The IISS includes the ROK's 4,500 man Coast Guard in its count of active paramilitary forces. The ROK Coast Guard has some 54Patrol and Coastal Combatants, roughly 30 logistics and support craft, 5 smaller maritime patrol aircraft, 7 multirole helicopters, and 8 transport helicopters.[34]

The ROK Special Forces are well-trained, modeled on US Special Forces and using US equipment. Each military branch (Army, Navy, Air Force, Marine Corps) has its own special operations units, though the largest is the Army Special Warfare Command (SWC) with 10,000 troops that "are tasked with infiltrating deep behind enemy lines for reconnaissance and surveillance, destruction of key military facilities, sabotage, and kidnapping enemy VIPs. Additionally, they combat terrorism, protect VIPs, and carry out top-secret operations. Furthermore, the SWC also has brigades whose specific duty is to engage and eliminate the DPRK's light infantry troops if they infiltrate the ROK."[35]

The SWC also prepares for a wide array of potential scenarios, such as DPRK use of WMD, missiles, terrorist actions, or other provocations to gain concessions. In the case of an internal DPRK crisis, the SWC also must be ready to handle crises such as an outbreak of civil war, manmade or natural disasters, large-scale refugee flow, loss of control or transfer of WMD, and the DPRK's collapse. In the case of military action on the Peninsula, the SWC would combine with US Special Operations Korea, currently based in Yongsan, to jointly make the Combined Unconventional Warfare Task Force. This combined force would then plan and conduct special operations on the Peninsula.[36]

The ROK Navy's Special Forces unit is modeled on the US's Underwater Demolition Team unit, and is similarly intensively trained, competent, and able to undertake operations flawlessly – such as its rescue of the *Samho Jewelry*'s 21 crewmembers after the ship was hijacked by Somali pirates

in early 2010. The Air Force also maintains an elite Special Forces group, able to infiltrate behind enemy lines in advance of airlift operations or airborne troops, in order to accurately guide planes in their troop and equipment drops.[37]

Counterterrorism, Terrorism, and Low-Level Asymmetric Warfare

There is no clear dividing line between terrorism and asymmetric warfare. It is also a historical fact that the side with the stronger regular military forces is either less likely to use such tactics than the weaker side, or to conceal them in the form of state-sponsored terrorism.

DPRK

The US and ROK feel that the historical record shows that there was nothing new about the DPRK's use of limited or asymmetric attacks – some of which the US and ROK have labeled as terrorism – in 2010. The DPRK has repeatedly challenged the ROK using low-level covert operations and asymmetric attacks, using these incidents to put pressure on both the ROK and the US. The DPRK has also deployed large amounts of its force structure for the same purpose, keeping the ROK under constant pressure. It has created a special balance in the border area by creating tunnel systems and deploying large amounts of artillery in caves and sheltered positions within range of Seoul, as discussed above.

The DPRK's willingness – and inventiveness – in using the threat and reality of such attacks was so consistent between 1950 and 2007 that it led the Congressional Research Service to prepare a 36-page chronology which covered 164 examples of armed invasion; border violations; infiltration of armed saboteurs and spies; hijacking; kidnapping; terrorism (including assassination and bombing); threats/intimidation against political leaders, media personnel, and institutions; incitement aimed at the overthrow of the ROK government; actions undertaken to impede progress in major negotiations; and tests of ballistic missiles and nuclear weapons.[38]

The CRS report summarizes these trends as follows:

> The most intense phase of the provocations was in the latter half of the 1960s, when North Korea (Democratic People's Republic of Korea, or DPRK) staged a series of limited armed actions against South Korean and US security interests. Infiltration of armed agents into South Korea was the most frequently mentioned type of provocation, followed by kidnapping and terrorism (actual and threatened). From 1954 to 1992, North Korea is reported to have infiltrated a total of 3,693 armed agents into South Korea, with 1967 and 1968 accounting for 20% of the total. Instances of terrorism were far fewer in number, but they seemed to have had a continuing negative impact on relations between the two Koreas. Not counting the DPRK's invasion of South Korea that triggered the Korean War (1950-1953), the DPRK's major terrorist involvement includes attempted assassinations of President Park Chung Hee in 1968 and 1974; a 1983 attempt on President Chun Doo Hwan's life in a bombing incident in Rangoon, Burma (Myanmar); and a mid-air sabotage bombing of a South Korean Boeing 707 passenger plane in 1987. Reported provocations have continued intermittently in recent years, in the form of armed incursions, kidnappings, and occasional threats to turn the South Korean capital of Seoul into "a sea of fire" and to silence or tame South Korean critics of North Korea. Then, in July 2006, North Korea launched seven missiles into the Sea of Japan, and in October 2006, it tested a nuclear bomb.

While it was not possible to find comparable assessments from a DPRK viewpoint, it is important to note that Pyongyang may see the use of unconventional or asymmetric warfare as the only way it can safely – and effectively – exert military pressure on the ROK and the US and force the pace

of negotiation. In realpolitik, the difference between terrorism and asymmetric warfare is often a matter of perspective and semantics.

Ties to Outside Actors

The DPRK has also provided financial support and training to Palestinian and Iranian militant groups in the past. It has directly initiated terrorist attacks, such as the 1987 bombing of a Korean Air flight. Despite issuing a joint statement with the US in 2000 renouncing terrorism, the country has continued to collaborate with former terrorist groups in its illegal activities – which will be discussed further in the next section. The US State Department reported in a 2011 assessment of counterterrorism and terrorism in the DPRK that,[39]

> **Overview:** The Democratic People's Republic of Korea (DPRK) is not known to have sponsored any terrorist acts since the bombing of a Korean Airlines flight in 1987. On October 11, 2008, the United States rescinded the designation of the DPRK as a state sponsor of terrorism in accordance with criteria set forth in U.S. law, including a certification that the government of the DPRK had not provided any support for international terrorism during the preceding six-month period and the provision by the DPRK of assurances that it will not support acts of international terrorism in the future.
>
> Four Japanese Red Army members who participated in a jet hijacking in 1970 continued to live in the DPRK. The Japanese government continued to seek a full accounting of the fate of 12 Japanese nationals believed to have been abducted by DPRK state entities in the 1970s and 1980s. The DPRK has not yet fulfilled its commitment to reopen its investigation into the abductions.
>
> **Legislation and Law Enforcement:** The United States re-certified North Korea as "not cooperating fully" with U.S. counterterrorism efforts under Section 40A of the Arms Export and Control Act, as amended. In making the annual determination designating the DPRK as "not cooperating fully," the Department of State reviewed the country's overall level of cooperation in our efforts to fight terrorism, taking into account U.S. counterterrorism objectives with the DPRK and a realistic assessment of its capabilities.
>
> **Countering Terrorist Finance:** The Financial Action Task Force (FATF) remained concerned about the DPRK's failure to address the significant deficiencies in its regulatory regimes. In January, the DPRK engaged the FATF to discuss its anti-money laundering and counterterrorist financing regulatory regimes. While the FATF welcomed this initial engagement and said it remained open to further engagement, there were no further contacts. In its public statement in February, the FATF publicly urged the DPRK to immediately and meaningfully address these deficiencies.
>
> The DPRK's financial system was opaque and compliance with international standards was difficult to gauge….
>
> **Regional and International Cooperation:** In June, the UN Counter-Terrorism Committee Executive Directorate (CTED) held consultations with the DPRK on strengthening its implementation of United Nations Security Council Resolutions 1267/1989, 1988, and 1373. CTED plans to continue to engage the DPRK to assist in its implementation of those resolutions.

Little changed in the country report the State Department issued in 2015,[40]

> **Overview:** The Democratic People's Republic of Korea (DPRK) is not known to have sponsored any terrorist acts since the bombing of a Korean Airlines flight in 1987. In October 2008, the United States rescinded the designation of the DPRK as a state sponsor of terrorism in accordance with criteria set forth in U.S. law, including a certification that the DPRK had not provided any support for international terrorism during the preceding six-month period and the provision by the DPRK of assurances that it would not support acts of international terrorism in the future.
> Four Japanese Red Army members who participated in a 1970 jet hijacking continued to live in the DPRK. The Japanese government continued to seek a full accounting of the fate of 12 Japanese nationals believed to have been abducted by DPRK state entities in the 1970s and 1980s. In May 2014, the DPRK agreed to re-open its investigation into the abductions, but as of the end of 2015 had not yet provided the results of this investigation to Japan.

> **Legislation, Law Enforcement, and Border Security:** In May, the United States re-certified North Korea as a country "not cooperating fully" with U.S. counterterrorism efforts pursuant to Section 40A of the Arms Export and Control Act, as amended. In making this annual determination, the Department of State reviewed the DPRK's overall level of cooperation with U.S. efforts to counter terrorism, taking into account U.S. counterterrorism objectives with the DPRK and a realistic assessment of DPRK capabilities.
>
> **Countering the Financing of Terrorism:** The DPRK is not a member of any FATF-style regional body. In July 2014, it was admitted as an observer, but not a full member, of the Asia-Pacific Group (APG) on Money Laundering, a FATF-style regional body. Nevertheless, the DPRK failed to demonstrate meaningful progress in strengthening its anti-money laundering/ combating the financing of terrorism (AML/CFT) infrastructure. While encouraging the DPRK's continued engagement with FATF and APG, the FATF highlighted continuing concerns about North Korea's "failure to address the significant deficiencies in its [AML/CFT] regime and the serious threat this poses to the integrity of the international financial system."

It was reported in April 2013 that the DPRK and Iran agreed on a deal to exchange DPRK mineral resources for Iranian crude oil, a further increase in economic ties between the two countries.[41]

WMD and Missile Exports

The DPRK has also exported missile technology and may develop the potential for exporting nuclear materials or weapons to other countries or non-state actors – including terrorist organizations. Reporting by the US Department of Defense cites two possible cases of exporting missile and WMD-related technology and equipment:[42]

> • In addition to Iran and Syria, past clients for North Korea's ballistic missiles and associated technology have included Egypt, Iraq, Libya, Pakistan, and Yemen. Burma has begun distancing itself from North Korea but remains a conventional weapons customer.
>
> • In October 2009, the ROK seized North Korean-origin chemical warfare protective suits destined for Syria.

A US expert reports that,[43]

> In April 2004 President of the Supreme People's Assembly Presidium Kim Yong-nam told visiting journalist Selig Harrison, "We make a clear distinction between missiles and nuclear material. We're entitled to sell missiles to earn foreign exchange. But in regard to nuclear materials, our policy past, present, and future is that we would never allow such transfers to al-Qaeda or anyone else." Foreign Minister Paik Nam-soon added, "We denounce al-Qaeda, we oppose all forms of terrorism, and we will never transfer our nuclear material to others." As the nuclear stalemate continued, however, the DPRK shifted. In 2005 Harrison reported that Vice Foreign Minister Kim Gye-gwan had warned, "[The United States] should consider the danger that we could transfer nuclear weapons to terrorists, that we have the ability to do so." Kim said the regime had no plans to transfer but would not rule it out "if the United States drives [us] into a corner." James Kelly, the U.S. State Department's assistant secretary for East Asian and Pacific Affairs, testified in July 2004 that a similar threat had been made during trilateral talks in April 2003.

The possibility of nuclear material exports should not be exaggerated. Moreover, DPRK-produced plutonium would not be ideal for terrorist groups lacking in high levels of nuclear weapons sophistication, as the type of bomb design that can utilize plutonium is difficult to build, compared to a uranium-based weapon. On the other hand, an operational highly enriched uranium program could increase proliferation risk. While a uranium bomb would require twice as much fuel, it is easier to weaponize and thus more attractive to non-state actors or states generally lacking in nuclear sophistication.[44]

ROK

For the ROK, the State Department reports in 2011 that,[45]

> **Overview:** The Republic of Korea strengthened its counterterrorism efforts in 2011. The Republic of Korea's National Intelligence Service (NIS), the Korean National Police Agency (KNP), and various intelligence entities worked in close coordination with U.S. and international counterparts to access and contribute to multiple counterterrorism databases. The Government of the Republic of Korea reviewed and strengthened its emergency response plan.
>
> In September 2011, the FBI Legal Attaché Office in Seoul worked jointly with the NIS and KNP to investigate an international terrorism subject who had relocated to the Republic of Korea. Subsequently, NIS and KNP provided information and monitored the subject until he departed the country.
>
> **Legislation and Law Enforcement:** In September 2005, the Republic of Korea signed the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT) and the National Assembly ratified it in December 2011.
>
> **Countering Terrorist Finance:** The Republic of Korea is a member of the Financial Action Task Force (FATF) and the Asia/Pacific Group on Money Laundering (APG), a FATF-style regional body. The National Assembly passed the "Prohibition of Financing for Offenses of Public Intimidation Act" in September, which the Financial Intelligence Unit (FIU) had submitted in October 2010. Prior to passing the Act, the National Assembly made important changes to the law. In addition to criminalizing the provision, collection, and delivering of funds and assets to terrorists and terrorist organizations, the revised act established a freezing regime that controls the disposition and transfer of movable and immovable assets, bonds, and other property or property rights.
>
> In December 2010, the FIU submitted a separate bill amending the Financial Transaction Reports Act to impose stricter penalties on financial institutions that violate reporting requirements. The bill was pending in the National Assembly at year's end….
>
> **Regional and International Cooperation:** South Korea is a member of the United Nations, Asia-Pacific Economic Cooperation (APEC), the Association of Southeast Asian Nations' (ASEAN) Regional Forum, ASEAN+3, East Asia Summit, the Asia-Europe Meeting (an interregional forum consisting of the EC, 27 EU members and 13 members of the ASEAN Plus), Asia Cooperation Dialogue, Forum for East Asia-Latin America Cooperation, the Organization for Economic Cooperation and Development, the G20, and the Conference on Interaction and Confidence-Building Measures in Asia. It is also a partner country of the Organization for Security and Cooperation in Europe and the North Atlantic Treaty Organization.
>
> In 2011, the South Korean government organized numerous international conferences to share information and best practices. It hosted the Seventh Plenary Meeting of the Global Initiative to Combat Nuclear Terrorism in June, and the Third APEC Seminar on the Protection of Cyberspace in September. South Korea also hosted the FATF/APG workshop on Money Laundering Typologies in December.
>
> The South Korean government held bilateral consultations on counterterrorism with the United Kingdom, Japan, China, Russia, Algeria, Uzbekistan, and Israel.

The State Department report issued in April 2014 had few substantive changes,[46]

> **Overview:** The Republic of Korea remains committed to its counterterrorism programs and has maintained strong cooperation with the United States and the international community. The Republic of Korea has not faced any major domestic terrorist threats, and the various agencies with counterterrorist responsibilities have remained vigilant in countering what they perceive as emerging threats, such as potential home-grown terrorism through internet recruitment.
>
> The Republic of Korea is becoming more involved in bilateral and international counterterrorism efforts in response to the growing exposure of its citizens living and traveling abroad. South Korean and U.S. law enforcement agencies worked closely on sharing information on known or suspected terrorists, implementing an agreement passed in 2008 on Preventing and Combating Serious Crime (PCSC), and holding joint investigations on known and suspected terrorist encounters that occurred in the Republic of Korea.

In November, the Republic of Korea and the United States held the Fourth Bilateral Consultation on Counterterrorism, where the two countries shared information on ways to enhance bilateral cooperation and expand South Korea's multilateral engagement.

Legislation, Law Enforcement, and Border Security: The National Assembly failed to pass a comprehensive counterterrorism law, first proposed in 2001, that would have significantly improved the Republic of Korea's ability to conduct counterterrorist activities. The Republic of Korea derives its authority to perform counterterrorist activities from Presidential Directive 47, which was last revised on May 21, 2013. The revision was mostly administrative and did not add any new authorities.

Countering the Financing of Terrorism: The Republic of Korea is a member of the Financial Action Task Force (FATF) and the Asia Pacific Group on Money Laundering, a FATF-style regional body. In accordance with UNSCRs 1267 (1999) and 1373 (2001), the Republic of Korea is tightening its existing domestic legislative framework and administrative procedures to combat terrorist financing. For further information on money laundering and financial crimes, see the 2014 International Narcotics Control Strategy Report (INCSR), Volume 2, Money Laundering and Financial Crimes: http://www.state.gov/j/inl/rls/nrcrpt/index.htm.

Regional and International Cooperation: The Republic of Korea is a member of the UN, APEC, ASEAN+3, East Asia Summit, Asia-Europe Meeting, Asia Cooperation Dialogue, Forum for East Asia-Latin America Cooperation, OECD, the G-20, and the Conference on Interaction and Confidence-Building Measures in Asia. South Korea is also a partner country of the OSCE and NATO. In October 2013, the Republic of Korea hosted the Conference on Cyberspace 2013, where representatives from 87 countries and 18 international organizations discussed how to combat cyber-attacks and the use of cyberspace for terrorist activities.

To promote capacity building abroad, the South Korean government has launched development assistance initiatives in Afghanistan, Iraq, and the West Bank and Gaza, which include contributions to counterterrorism and stabilization programs. Also, various South Korean ministries provide information and communication technology advancement assistance to developing countries that includes programs to counter cyber-terrorism and to build a secure information technology infrastructure.

DPRK Drug and Weapons Sales and Other Illegal Activities

The DPRK engages in a variety of illegal and questionable activities in order to raise money for the continued existence of the regime. After defaulting on its international debts in 1975, the regime ordered its embassies to finance their own operations. Since this time – starting in 1976 – the DPRK has become extensively involved in transnational criminal smuggling, including drugs, counterfeit US currency, endangered species products, counterfeit pharmaceuticals, counterfeit cigarettes, and has even opened an international chain of restaurants. It has also been reported that the DPRK is engaged in insurance fraud and human trafficking. In recent years, North Korea's illicit activities seem to have been partly criminalized and dispersed, with operations and profits being associated with certain key powerbrokers as oppose to the state itself.[47]

Although it would appear to be secondary to financial incentives, the DPRK does claim ideological justifications for these criminal acts – explaining them as tools of guerilla warfare undermining the enemy and as a justified action under the previously explained idea of *juche* (self-reliance).[48]

Drugs

After the DPRK lost the much support of its Cold War patrons, it significantly increased its involvement in drug trade and trafficking in the mid-1990s, roughly concurrent with Kim Jong-Il's accession to leadership. Drugs, counterfeit currency, and other illegal items were produced in the country and then transferred to criminal organizations – such as the Official Irish Republican Army, Japanese Red Army, Russian Mafia, Chinese Triads, Taiwanese organized crime

syndicates, and the Japanese Yakuza – for transport and distribution. Criminal groups also started to smuggle counterfeit currency and drugs on ships in mismarked or disguised containers, hiding money in jars of honey, inside the linings of boxes, and inside cigarettes. Customs officials have discovered these containers in the US, Taiwan, and Japan.[49]

DPRK diplomats relied on their diplomatic immunity and used diplomatic pouches to purchase drugs – mainly opiates – for resale in foreign countries. Diplomats have also been caught smuggling other objects, such as pharmaceuticals, products made from endangered species, and gems. Scandinavia ejected most of the DPRK diplomatic corps from the country after a series of drug seizures linked to DPRK embassies worldwide.[50]

After three years of diplomatic relations, Venezuela expelled all DPRK diplomats in 1977 for trafficking drugs. Russia arrested a DPRK envoy in 1996 with 50 pounds of heroin. Two years later, Russia arrested another two diplomats with 35 kilograms of cocaine, while Egypt arrested a diplomat trying to smuggle 500,000 tablets of rohypnol into the country. That same year, Germany arrested a deputy ambassador in the possession of heroin, and China arrested a consulate employee with 9 kilograms of opium.[51]

Overall, there were at least 50 cases in 20 countries linking the DPRK to drug trafficking, most of which involve the detention and/or arrest of DPRK diplomats.[52] In the wake of these arrests, the DPRK has increasingly turned to distribution networks run by organized crime gangs.[53]

Bureau 39, one of the Korean Workers' Party Central Committee's offices that obtains luxury items for DPRK elites, also procures components and technology for weapons programs and sets up illegal activities to fund its operations. The office, which is entirely outside the jurisdiction of the DPRK's cabinet and separate from its national economic planning process, was reportedly established in 1974 and put the currency it generated into a slush fund of about $5 billion that was exclusively under the control of Kim Jong-il.[54] It was reported in April 2013 that Kim Jong-un is believed to have more than $1 billion held in secret bank accounts in Austria, Switzerland, and Luxembourg.[55]

Bureau 39 operates through Korea Workers' Party-run and government-established front companies, such as Zokwang Trading Company (Macao) and Daesung Congguk (Austria). According to defectors, the DPRK regime cannot last without the income generated through Bureau 39's illegal activities.[56] **Figure III.5** shows a 2010 representation of DPRK government offices, with Bureau 39 at the top.

The DPRK has also indirectly promoted social stability in other countries through its links to non-state actors and criminal gangs. For example, the DPRK has assisted guerillas in Myanmar by acting as a middleman, providing weapons in exchange for drugs. This has resulted in perpetuation of the insurgency, with the rebels having an increased weapons capacity as well as money to buy more arms, hold large areas of territory, and continue violence and human rights abuses, such as the forced recruitment of child soldiers.[57]

Defectors have testified that drug production began in the late 1970s, followed later by the establishment of an experimental farm in 1988-9 in Hamkyung province (where pharmaceutical plants process it into heroin, as well). There was also a countrywide public order to produce opium for export in the early 1990s – at which point the police ordered farms to switch from grain production to growing poppies. Of course, this undermines subsistence agriculture and contributes to the North's famines.[58]

The major narcotics produced are heroin and methamphetamines. One refugee described the DPRK as a "narco-state in which all aspects of the drugs operation – from school children toiling in poppy fields to government-owned processing plants to state-owned cargo ships and trading companies – are controlled by Kim [Jong-Il]." State farms and villages have production targets. Bureau 39 oversees the international distribution of drugs with the help of the military, using commercial and military vessels, diplomatic personnel, and state-owned businesses to launder the profits.[59]

One CRS report describes the reported drug manufacturing activities of the DPRK as follows:[60]

> **Opiates**. According to press reports and North Korean defectors, farmers in certain areas have been ordered to grow opium poppies in the past. In 2006 congressional testimony, a representative of the State Department reported that North Korea cultivates 4,000 to 7,000 hectares of opium poppy, producing approximately 30 to 44 metric tons of opium gum annually. Though such estimates appear reasonable, they are nevertheless based on indirect and fragmented information. With the caveat that conclusive "hard" data is lacking, U.S. government investigative agency sources estimate North Korean raw opium production capacity at 50 tons annually. North Korean government chemical labs reportedly have the capacity to process 100 tons of raw opium poppy into opium and heroin per year.
>
> **Methamphetamine**. North Korea's maximum methamphetamine production capacity is estimated to be 10 to 15 metric tons of the highest quality product for export. This coincides with a time when markets for methamphetamine are dramatically expanding in Asia, especially in Thailand, Japan, the Philippines, and more recently in Cambodia and China.

There have been several instances in which drugs linked to the DPRK have been caught en route:[61]

> In 2001, the Japanese Coast Guard and a North Korean ship exchanged fire, resulting in the sinking of the North Korean naval vessel that was operated by North Korean special forces. Japanese authorities subsequently determined that the North Korean ship entered Japanese waters to deliver methamphetamines to Japanese Yakuza members. In the following year, Taiwanese authorities stopped and searched a Taiwanese fishing trawler which contained 174 pounds of heroin that it had received from a North Korean gunboat. In 2003, Australian police arrested three men in a coastal village west of Melbourne who had received $50 million of street-ready heroin from a dinghy launched by the state owned North Korean ship, *Pong Su*, which lay just off shore. North Korea has used its merchant fleet to act as a middleman for other groups involved in drug trafficking by bartering other goods, such as weapons, in exchange for drugs. A North Korean vessel laden with small arms was detained by authorities in Myanmar who believed that local insurgent groups were intent on trading heroin for the arms.

Since the mid-2000s, there has been a decrease in large-scale drug seizures directly tied to North Korea, a trend that has led some experts to conclude that there has been a d**ecline** in state-sponsored drug activities. Instead, there has been a trend "away from an industry marked by regime sponsorship to one primarily characterized by quasi-private production and crony capitalism" aimed at local production and consumption. Different individuals and state agencies seem to be using the drug trade for personal revenue, then turning over a portion of their proceeds to the central government or Kim family. These operations may also have increased the sophistication of their smuggling techniques, making international detection more difficult.

Another explanation for the declining international drug presence is increasing demand with the DPRK itself; according to several studies and defector accounts, consumption of illicit drugs (particularly methamphetamine) has increased throughout North Korea over the past decade.[62]

Pharmaceuticals and Cigarettes

There are reports that the DPRK makes fake Viagra and Cialis in factories in Chongjin and also produces counterfeit cigarettes. By 2005, the DPRK had become one of the primary sources of internationally branded cigarettes, producing several brands in approximately 12 factories owned by both DPRK entities and by Taiwanese- or Chinese-operated companies.[63] From 2002-2005, DPRK-sourced Marlboros were recovered across the US in over 1,300 incidents.[64]

According to a former State Department official, a standard 40-foot container of counterfeit cigarettes can cost as little as $70,000 to produce but can have a street value of $3-4 million. Federal charges filed in 2006 document that over a period of several years, criminal gangs brought one 40-foot container into the US per month; the cigarettes are also sold in other Asian countries such as Singapore, Taiwan, the Philippines, Belize, Vietnam, and Japan. As early as 1995, Taiwan seized 20 containers of counterfeit cigarette wrappers on a ship going to the DPRK that could have been used to produce up to $1 billion (street value) in counterfeit cigarettes. Defectors have reported factories in several areas in the DPRK, with workers belonging to a special work force team that receives extract rations.[65]

Most of the DPRK-owned enterprises producing cigarettes illegally are located near Pyongyang. Rajin, a free trade zone port city on the east coast of the DPRK seems to be another main hub of counterfeit cigarette activity – where many of the factories are reportedly financed and owned by Chinese criminal organizations. One report indicated that the North Korean regime gives permission for port usage to certain deep-sea smuggling vessels and also offers a secure delivery channel for the gangs. According to the CRS,[66]

> A 2006 article on North Korean cigarette production found that DPRK cigarette manufacturers have been turning more toward producing domestic low-priced brand cigarettes instead of counterfeit products. The article states that relative to the price of rice, the price of a package of cigarettes has been falling and their quality has been rising. In 2007, the DPRK imported $12.95 million ($14.1 million in 2006 and $13.5 million in 2005) in tobacco products from China. Domestic brands now are taking market share from imports, and North Korean cigarette producers — even the factories operated by the No. 39 Department of the Workers' Party, which accumulates and manages Kim Jong-il's slush funds — reportedly have been producing more for the domestic market than counterfeits of brands such as Mild Seven, Crown (both Japanese brands), and Dunhill.
>
> Media reports indicate that Greek authorities seized some four million cartons of contraband cigarettes through the fall of 2006, of which three million were aboard North Korean vessels. For example, on September 25, 2006, Greek officials detained a North Korean freighter that was carrying 1.5 million cartons of contraband cigarettes and arrested the seven seamen on board. According to information from Greek customs authorities, the ship's load of counterfeit, duty-unpaid cigarettes would have brought 3.5 million euros in taxes.

Furthermore, state-run factories manufactured pharmaceuticals and processed and packaged opiates and methamphetamines. DPRK drugs, counterfeit currency, cigarettes, and pharmaceuticals can be forensically identified as coming from the DPRK and are actually very high-quality products in both packaging and manufacturing/chemical purity. However, reports indicate that the DPRK's criminal network partners now operate their own production and distribution networks within and outside of the DPRK, for example producing lower-quality counterfeit currency.[67] It appears that North Korea has continued these counterfeiting operations, and may have expanded them to other consumer goods. For example, in 2012 "Japanese shoe manufacturer ASICS complained that North Korea had imported and created knockoff versions of its shoes, and tourists in summer 2012 observed display cases selling Marlboro cigarettes with the brand name misspelled."[68]

Supernotes, Insurance, and Trafficking

DPRK state-run factories also print counterfeit US $100 bills (the "Supernote"). Part of the US-led 2005 Banco Delta Asia freeze of DPRK funds (discussed later in this report) was to stop Bureau 39 from laundering Supernotes – which have been described by the US secret Service as the most sophisticated counterfeits in the world.

These bills, allegedly manufactured in the city of Pyeongseong, use high-tech Japanese equipment, paper from Hong Kong, and French ink. The Supernote has been found in Las Vegas, first in 2005 and again in 2007, when a Chinese businessman was arrested laundering the bills in casinos. One Supernote distribution ring involved the Official Irish Republican Army distributing the notes to Ireland, Great Britain, Poland, Denmark, the Czech Republic, Belarus, and Russia, making an estimated $28 million; the bills have also reportedly been linked with DPRK WMD proliferation.[69]

The CRS notes,[70]

> Media reports indicate that counterfeit $100 bills are used in North Korean markets as currency and are valued at about the equivalent of $70. It is not clear, however, whether the counterfeit bills circulating are from existing stocks or are currently being produced. The anti-counterfeiting security features incorporated into new U.S. bills make counterfeiting much more difficult.

While there were several Supernote discoveries through 2009, many believed that these notes were produced earlier and that North Korea had largely abandoned its counterfeiting in the face of US security measures.[71] However, in June 2016, a North Korean agent was arrested in China with counterfeit $100 bills, with the apparent intent of purchasing household appliances and electronics. This apparent return of counterfeiting operations, and the relatively low quality of the forgeries, might suggest that the DPRK's finances are strained following the implementation of the 2016 sanctions, and its leaders are looking for alternative funding sources.[72]

In late 2006, media reports surfaced that the DPRK could be involved in insurance fraud at a state level. Some experts believe that property damage claims are significantly overstated, claims are made for deaths that are not due to an accident, and accident circumstances are being changed. DPRK state-initiated insurance fraud has not been conclusively confirmed, though this type of activity would fit the DPRK's criminal patterns. One source estimated that the DPRK's 2006 fraudulent claims could have been more than $150 million. On the reported insurance fraud and endangered species trafficking, the CRS reports,[73]

> A recent example cited in media reports of possible DPRK state involvement in insurance fraud involves a ferry accident that reportedly occurred in April 2006 near the coastal city of Wonsan. After the accident, North Korea declared that 129 people had died, all of whom were provided life insurance coverage when they bought a ticket. It was claimed that most of the victims had died of hypothermia, although weather data apparently indicated that temperatures were warmer than reported by Pyongyang's Korea National Insurance Corporation. In another case, in July 2005, a medical rescue helicopter apparently crashed into a government owned disaster supply warehouse, setting it on fire. It reportedly took the DPRK authorities only 10 days to file a claim that included a detailed inventory of hundreds of thousands of items — a task which insurance industry officials say normally takes most governments many months….
>
> Several reports link North Korean officials with trafficking in endangered species, which is in contravention to the U.N. Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES).55 The DPRK is not a member of CITES; however, DPRK diplomats allegedly have been caught trafficking in CITES-protected species between treaty member states, including France, Russia, and Kenya. According to the State Department, known DPRK violations of CITES began in the 1980s and have mainly involved trafficking in elephant ivory and rhino horn. Although some may argue that cases of endangered species smuggling by DPRK diplomats may have been for personal use, the sheer size of confiscated shipments —

> as much as several hundred kilograms each — suggests that endangered species trafficking could have been planned by a North Korean government entity.

The CRS also discusses the DPRK's potential human trafficking activities:[74]

> According to the State Department, North Korea is a source country for men, women, and children trafficked for forced labor and commercial sexual exploitation and has been listed by the U.S. government as a "Tier 3" country for as long as it has been included in the State Department's Trafficking in Persons annual reports. As a Tier 3 country, North Korea reportedly does not comply with minimum standards for eliminating trafficking and is not making significant efforts to do so.
>
> It remains unclear to what extent DPRK profits from human trafficking activities as a source of revenue. However, the State Department indicates that North Korea directly contributes to labor trafficking by maintaining a system of force labor prison camps inside the country, where an estimated 150,000 to 200,000 prisoners are forced to log, mine, and tend crops. According to Mark Lagon, Director of the U.S. Office to Monitor and Combat Trafficking in Persons, the most common form of DPRK trafficking are North Korean women and children who voluntarily cross the border into China and are picked up by trafficking rings and sold as brides in China and elsewhere, including Russia and Mongolia. The 2007 Trafficking in Persons report further states that North Korean women and girls may also be lured out of DPRK with promises of food, jobs, and freedom, only to be forced into prostitution, marriage, or exploitative labor arrangements in China

Illicit Revenue and the DPRK's Official Stance

The DPRK receives an estimated annual income of $15 million to $100 million from counterfeiting, $80-160 million from cigarette counterfeiting, and a total annual criminal activities income of $500 million[75] to $1 billion.[76]

In the past several years, there have been few drug trafficking incidents directly linked to the DPRK government, leading the State Department to report in 2008 that DPRK drug trafficking "appears to be down sharply and there have been no instances of drug trafficking suggestive of state-directed trafficking for five years."[77] This could be due to increased international attention to the DPRK's activities, or because the DPRK has increased its use of criminal gangs instead of being directly involved in the distribution of its illegal products. In addition, the regime has sharpened its overtly anti-drug rhetoric and has increased arrests for distribution; however, most perpetrators appear to have simply payed out bribes as oppose to facing any form of severe punishment.[78]

It must be noted that the DPRK denies all such allegations of any state-sponsored criminal acts and has accused the US of counterfeiting its own currency in an attempt to frame the DPRK. International and regional powers have either declined to comment on the issue or expressed skepticism as to the DPRK's involvement in these types of activities, though recently it would appear that there has been a subtle shift towards supporting the US's allegations.[79]

Meanwhile, US officials have grown more certain in their conclusions; one State Department official testified to the Senate in 2006 that, "There's no doubt that the government of the [DPRK], the Korean Workers' Party, and the Korean People's Army are all involved in criminal activities."[80] In addition, there seem to have been recent attempts by the DPRK to control and cut back on drug trafficking, especially outside of the state's authority; reports also indicate increasing drug addiction inside the country:[81]

> An emerging genre of reports, yet to be substantiated, suggests that as state control of drugs in the DPRK becomes looser, a growing amount of stimulants for domestic sale and consumption are being produced privately by scientists in the DPRK and funded by private investors. Some reports suggest drug abuse is becoming widespread among senior military officials and also among the poor as a means to dull hunger.

> Others suggest that drug addiction is spreading among cadres such as the officer corps of the People's Army Security Department and high-ranking party officials. A scenario is being presented of drugs sold openly at farmers markets, at times being used instead of currency in transactions.

Weapons Sales

While the DPRK does import weapons components – such as a jet mill used for missile fuel in 1994 and a blocked shipment of power-control devices that could be used in uranium centrifuges or missile launches – the country also sells its ballistic missiles and related technologies to other countries. With the funds it receives from these weapons sales, the DPRK can further develop missiles.[82] There have also been reports of chemical and biological weapons assistance to Syria and Iran, though this is far from being conclusively substantiated.[83]

The US Department of Defense reports that,[84]

> North Korea uses a world-wide network to facilitate arms sales activities and maintains a core group of recipient countries including Iran, Syria, and Burma. North Korea has exported conventional and ballistic missile-related equipment, components, materials, and technical assistance to countries in Africa, Asia, and the Middle East. Conventional weapons sales have included ammunition, small arms, artillery, armored vehicles, and surface-to-air missiles.
>
> North Korea uses various methods to circumvent UNSCRs, including falsifying end-user certificates, mislabeling crates, sending cargo through multiple front companies and intermediaries, and using air cargo for deliveries of high-value and sensitive arms exports.

1. In early July 2013, Panamanian authorities stopped and inspected the North Korean flagged vessel Chong Chon Gang, finding hidden cargo including two MiG-21 fighter aircraft and associated engines, SA-2 and SA-3 SAM-related equipment, and unspecified missiles. Cuba issued a statement acknowledging ownership of the military equipment and claiming it was being sent to North Korea for overhaul.
2. In June 2011, the M/V Light, a vessel bound for Burma suspected of carrying military-related cargo, returned to North Korea after refusing a U.S. Navy inspection request.
3. In February 2010, South Africa seized North Korean-origin spare tank parts destined for the Republic of Congo.
4. In December 2009, Thai authorities impounded the cargo of a chartered cargo plane containing about 35 metric tons of North Korean weapons, including artillery rockets, rocket-propelled grenades, and SAMs.

The DPRK has exported approximately 500 ballistic missiles over the past 20 years, with over 80% of these exports taking place between 1987 and 1993. The country transferred 100-400 *Scud*-B missiles to Iran in 1987-1988, along with 25-40 to the UAE in 1989. Technical assistance in the production of *Scuds* was given to Iran and Libya; the latter also received an unknown number of *Scud*-Bs, which were further exported to Ethiopia, Burma, Congo, and Vietnam. Libya and Egypt both received technical help for *Scud*-C production, while the DPRK exported *Scud*-Cs to Iran, Yemen, Syria, and Libya.

It is likely that the DPRK also provided technical assistance to Iran for *Nodong* production and exported *Nodongs* to Pakistan, Libya, Syria, Iran, Iraq, and Egypt. Missile components and related items were found on a DPRK freighter headed to Libya in 1999, while another DPRK freighter transported *Scud* missiles to Yemen in 2002. Furthermore, 18 *Musudan* missiles were transferred to Iran in 2005.[85] Burma (Myanmar) has also reportedly received DPRK missile assistance and conventional missile exports, in contravention of UN sanctions on the DPRK.[86]

By 1993, the DPRK reportedly had contracts with Libya, Iran, and possibly Syria and Pakistan to sell the *Nodong* missile. In 2002, US and Spain intercepted a DPRK ship headed to Yemen with a cargo of 15 *Scud* missiles, conventional warheads, and 85 drums of inhibited red fuming nitric acid, used in *Scud* missiles.[87] However, DNI Dennis Blair testified to Congress in 2009 that,[88]

> Pyongyang is less likely to risk selling nuclear weapons or weapons-quantities of fissile material than nuclear technology or less sensitive equipment to other countries or non-state actors, in part because it needs its limited fissile material for its own deterrent. Pyongyang probably also perceives that it would risk a regime-ending military confrontation with the United States if the nuclear material was used by another country or group in a nuclear strike or terrorist attacks and the United States could trace the material back to North Korea. It is possible, however, that the North might find a nuclear weapons or fissile material transfer more appealing if its own stockpile grows larger and/or it faces an extreme economic crisis where the potentially huge revenue from such a sale could help the country survive.

The economic desperation of the regime, especially in an atmosphere of increasing international sanctions, could increase the country's level of acceptable risk – perhaps resulting in nuclear smuggling, as previously discussed.

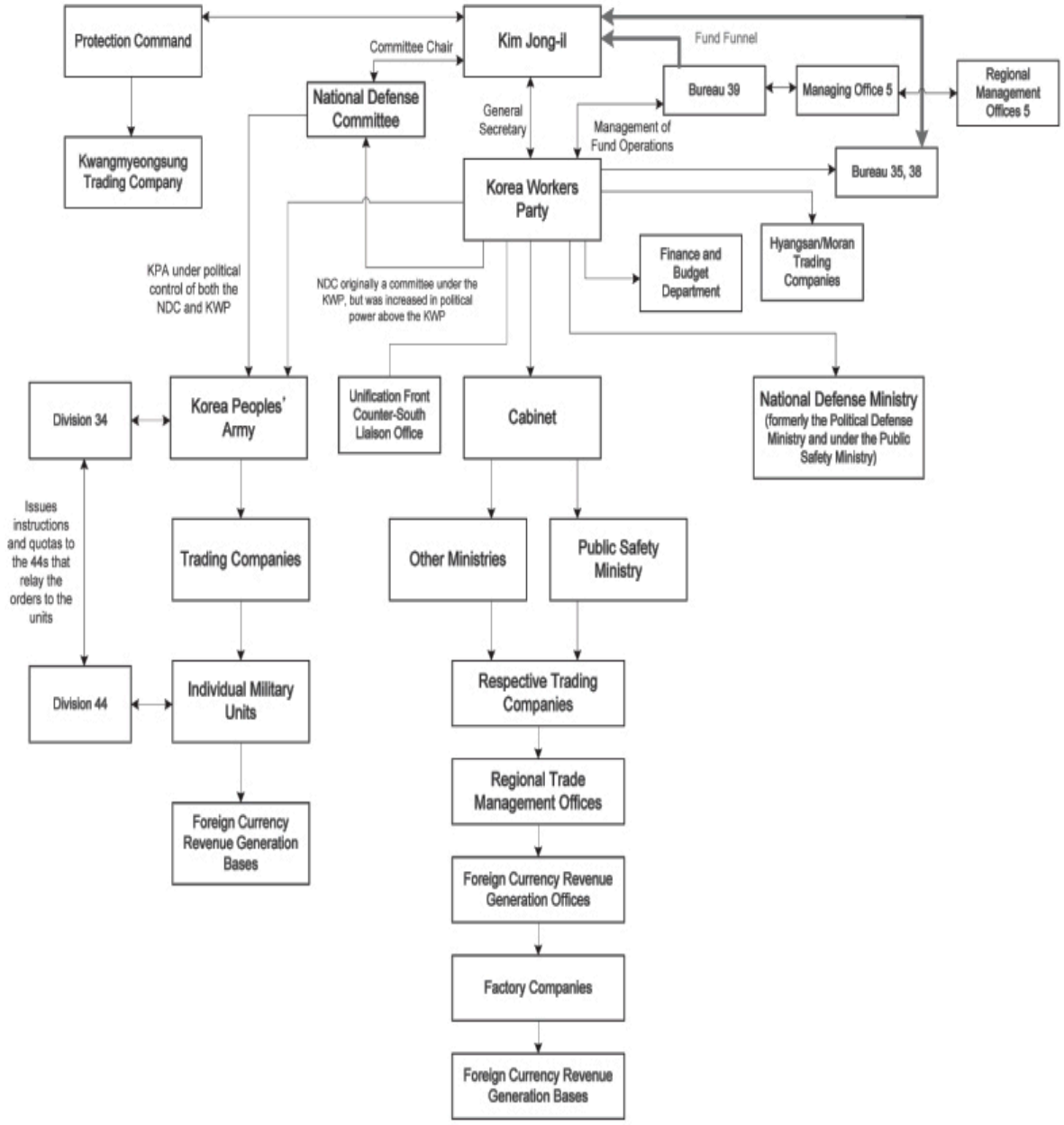
If the DPRK does decide to engage in such activities, it would have the channels and capacity to do so. Experts state that the North has the capability to make either "plutonium metal or plutonium oxide powder, the two most likely forms for transport;" it would then be possible to shield six palm-sized pucks of plutonium from sensors. And while the US and its partners have increased the pressure on the DPRK's Navy through Proliferation Security Initiative (PSI) interdictions, overland and air smuggling routes have also been developed that can be used for proliferation purposes. Furthermore, while there were 11 PSI interdictions in 2004, there are an estimated 65 nuclear smuggling events annually – if the North wanted to proliferate nuclear materials, it would likely be successful in at least some of its attempts.[89]

North Korea has continued its export of conventional arms, such as MANPADs, artillery rockets, and RPGs, to non-state actors. Footage from Syrian rebels appears to show rebels firing the Bulsae-2, a North Korean version of the Russian 9K111 Fagot anti-tank guided missile.[90] The Syrian regime was also apparently still receiving missile components and technology from North Korea as recently as 2013.[91]

UN sanctions have made it increasingly difficult for the DPRK regime to rely on arms sales as a steady source of income. Following the 2006 nuclear test, the UNSC imposed an arms embargo on North Korea that covered all major conventional weapons and ballistic missiles. After the 2009 test, this was expanded to all weapons except small arms, which were subsequently banned after the 2016 nuclear test.[92]

Despite these restrictions, the DPRK has tried to continue arms shipments through increasingly sophisticated sanction work arounds, such as "document falsification, cargo concealment, strategic attempts to take advantage of lax regulations on transshipment and business ownership structure, employment of foreign-based individuals to assist with financial transactions, and the use of front and shell companies". These methods have allowed North Korea to continue its export of "tanks, air-defense systems, artillery systems, and rocket-propelled grenades (RPGs), as well as shells and ammunition", in addition to running a weapons refurnishing business focused on old Soviet equipment.[93] However, it is unclear how expansive or profitable this arms trading is for the regime, especially given the recent tightening of sanctions.

Figure III.5: The DPRK's Legal, illegal, and Illicit Activities Network (2010)



Source: John Park, "North Korea, Inc.: Gaining Insights into Regime Stability in North Korea from Recent Commercial Activates," in Paul Rexton Kan, Bruce E. Bechtol Jr, Romert M. Collins, *Criminal Sovereignty: Understanding North Korea's Illicit International Activities*, Strategic Studies Institute, March 2010, 2.

ROK Weapons Sales

Because of force structure reductions and the corresponding likely lack of increase in domestic procurement demand, the ROK is promoting export of military equipment. Sales abroad reached $2.4 billion in 2011[94] – higher than the goal of $1.6 billion thanks to the success of the T-50 Golden Eagle aircraft – while domestic sales were $7 billion.[95]

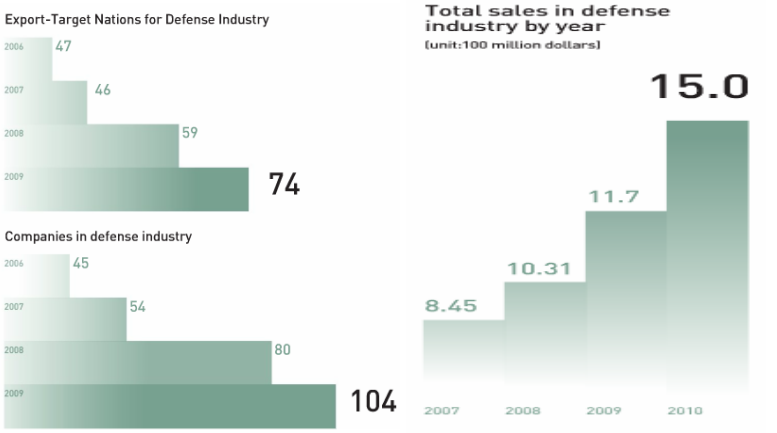
The ROK aims to be among the world's top 8 exporters by 2015[96] and by 2017 total ROK defense exports are forecast to be $10 billion.[97] Items exported include aircraft engine and wing assemblies, small-caliber munitions, tank production technology, submarine combat systems, and wheeled armored vehicles.[98]

Figure III.6 shows the increase in numbers of ROK weapons sales and defense companies over the past several years, along with total defense industry sales. The ROK is hoping to link defense exports with civilian industries like shipbuilding, exploiting existing export strengths. Regarding ROK military exports, the IISS reported,[99]

> South Korea's aerospace industry is the least developed sector, although the co-development of the T-50 trainer and the FA-50 light fighter variants show longer-term potential. Indonesia signed a contract in May 2011 for 16 T-50s, and the Philippines selected it in August 2012. The largest potential market is in the US, where the air force's T-X trainer competition (for up to 350 aircraft) could provide a major boost to the T-50.
>
> In naval systems, South Korea already produces Aegis destroyers and its own LHDs. In February 2012, Daewoo Shipbuilding won a contract to build four military oilers for the UK Royal Navy and also won a US$1.1bn contract to build four submarines for Indonesia. South Korea has established capacity in manufacturing armoured vehicles, such as the XK-2 tank and K9/10 self-propelled howitzers, which Seoul hopes to export. Lower labour costs, precision engineering, and South Korea's military experience have boosted defence-industrial prospects.

By 2014, South Korean defense exports had reached $3.6 billion, with an average yearly growth rate of 31 percent for the previous five years. This made the ROK the 13th largest exporter of major arms in 2014. [100] Export numbers slid slightly to $3.49 billion in 2015, but still showed a marked improvement from the historic profile of South Korea's more domestically focused defense industry.[101]

Figure III.6: The ROK Defense Industry in 2010



Source: Republic of Korea Armed Forces, "Innovation Makes Us Powerful," ROK Ministry of National Defense, 2010, 34-5.

DPRK: Cyber, Electronic Warfare, and SIGINT Capabilities

There are a variety of other North Korean paramilitary and covert activities that also deserve mention. The DPRK has a significant intelligence program directed towards the ROK:[102]

> North Korea's intelligence resources are focused primarily on South Korea and are dedicated to influencing public opinion, collecting sensitive information on U.S. and Republic of Korea government and military targets, and in some cases assassinating high-profile defectors and outspoken critics of the North Korean regime. North Korean intelligence officers and agents for years have infiltrated South Korea by posing as defectors. Firsthand accounts of confessed North Korean agents describe long-term strategies that can involve many years of living in South Korea as sleeper agents before being tasked with a mission. North Korean intelligence activity is likely greatest in East Asia; however, the full extent of activity outside the Korean peninsula is unknown.

Cyber

As note earlier, DPRK cyber warfare capabilities are a growing problem – and one demonstrated by its attacks on Sony in December 2014. Former US Forces Korea Commander James Thurman testified in front of the House Armed Services Committee in March 2012 that "North Korea employs sophisticated computer hackers trained to launch cyber infiltration and cyber attacks against Korea and the United States," showing that the DPRK has stepped up its efforts to enhance its cyber-attack capacity in recent years.

The IISS summarizes the DPRK's cyber capabilities and history as follows:[103]

> Since the 1970s, the North Korean military (the Korean People's Army – KPA) has maintained a modest electronic warfare (EW) capability. As a result of strategic reviews following Operation Desert Storm, the KPA established an information warfare (IW) capability under the concept of 'electronic intelligence warfare' (EIW). Complementing these EIW developments, the KPA is believed to have expanded its EW capabilities with the introduction of more modern ELINT equipment, jammers and radars. In 1998, Unit 121 was reportedly established within the Reconnaissance Bureau of the General Staff Department to undertake offensive cyber operations. Staff are trained in North Korea but some also receive training in Russia and China. In early 2012, activity attributed to Pyongyang included jamming the global positioning systems of aircraft using Seoul's main international airports, as well as those of vessels in nearby waters for two weeks. North Korea also continued to launch distributed denial of service attacks on South Korean institutions and pursue cyber infiltration against military and other government agencies.

The DOD reported in May 2013 that,[104]

> North Korea probably has a military computer network operations (CNO) capability. Implicated in several cyber attacks ranging from computer network exploitation (CNE) to distributed denial of service (DDoS) attacks since 2009, the North Korean regime may view CNO as an appealing platform from which to collect intelligence.
>
> - North Korea was allegedly behind two separate cyberattacks in 2013, which targeted South Korean banking, media, and governmental networks, resulting in the erasure of critical data.
> - According to a ROK newspaper, Seoul's Central Prosecutor's office attributed to North Korea a CNO activity on the ROK's National Agricultural Cooperative Federation (Nonghyup Bank) servers in April 2011. Through remote execution, actors rendered the bank's online services inaccessible and deleted numerous files concerning customer bank accounts while removing all evidence of CNO activity in the bank's servers.
> - In the years spanning 2009-2011, North Korea was allegedly responsible for conducting a series of distributed denial of service (DDoS) attacks against ROK commercial, government and military websites, rendering them inaccessible.

> Technical attribution of cyberspace operations remains challenging due to the internet's decentralized architecture and inherent anonymity. Given North Korea's bleak economic outlook, CNO may be seen as a cost-effective way to modernize some North Korean military capabilities. As a result of North Korea's historical isolation from outside communications and influence, it is likely to employ Internet infrastructure from third-party nations.

The DPRK is believed to have a cyber warfare unit called "Number 121," composed of 3,000 elite hackers who break into networks for information and spread viruses – similar to espionage and vandalism, not warfare. The DPRK is also believed to train these experts as part of its computer warfare strategies at the electronic warfare department of a military technician training center.[105]

Two DPRK defectors who claimed to have been part of the cyber warfare department reported in 2011 that the department was vast, highly professional, and recruited hackers straight out of primary school. They are sent to Russia or China for training and receive special treatment by the DPRK – like housing or other privileges for their families and themselves. This is in part to reduce the temptation to defect, as they have access to the internet – unlike most other DPRK citizens – and thus know of the relative prosperity enjoyed by most other countries.[106]

One defector provided five reasons why the DPRK had decided to focus energy and resources into developing a cyber warfare program: cyber military strength is cost effective, provides higher utility than other forces, the DPRK is confident of its software development capabilities, it sees the internet as inherently weak and thus an easy target, and cyber warfare is asymmetrically advantageous for the DPRK. As the country is almost entirely not connected to the internet, it is much less exposed to such attacks – as opposed to the ROK, which is one of the most connected societies in the world.[107]

The DPRK is suspected of having been behind major cyber-attacks on the ROK in 2008, when the DPRK shut down approximately 400 computers at Lee Myung-bak's presidential transition office, and in 2009, when the websites of governmental institutions such as the National Assembly and the Presidential Office were paralyzed in a distributed denial-of-service (DDoS) attack.[108]

The 2009 attack involved 435 different servers in 61 countries.[109] The ROK's Seoul Central District Public Prosecutors' Office announced in May 2011 that its investigation into a network failure of Nonghyup bank in March 2011 showed the issue was caused by a cyber-attack in which North Korea was involved.[110] Another early 2011 attack paralyzed the websites of 40 public and financial institutions, including the presidential office. In 2012, a major South Korean newspaper, JoongAng Ilbo, was also attacked. [111]

The DPRK is also suspected to be behind another attack on March 20, 2013 when a hacking attack originating from a Chinese IP address paralyzed approximately 32,000 computers at the ROK's two largest public broadcasters, a news cable channel, and three large banks.[112] The broadcasters attacked were on a list of ROK media firms denounced by the DPRK in 2012 for the right-wing manipulation of ROK public opinion.[113]

The ROK traced the IP address of the hacker to a registration in Ryugyong-dong in Pyongyang (the capital of North Korea), and the hacker first accessed the ROK websites weeks before the March 2013 attack. The methods used in the attack were similar to those used by the DPRK's Reconnaissance General Bureau, which has in the past led hacking attempts against the ROK.

To undertake the attack, 76 pieces of malicious code were used; 18 bits of code have been identified as exclusively used by DPRK hackers in previous attempts. The attack also involved routing through the US, ROK, and eight other countries in an apparent attempt to disguise its

identity; 49 infiltration routes were used (25 local; 24 foreign), of which 22 were IP addresses the DPRK has used before in attacks.[114]

From 2008-2012, ROK public institution websites have received 73,030 hacking attempts – though the vast majority have not been conclusively tied to DPRK. ROK officials also say that DPRK computers were used to distribute malicious software by accessing ROK financial firms' networks 1,590 times between June 2012 and April 2013.[115]

In April 2013, the 'hacktivist' group Anonymous claimed to have initiated "Operation Free Korea," a series of cyber-attacks on the DPRK. The group first hacked the DPRK's China-based website Uriminzokkiri.com, took control of the related Flickr and Twitter accounts, and posted a warning, a manifesto, a series of demands, and a wanted poster of Kim Jong-un with a pig snout and Mickey Mouse on his chest.[116]

The group claimed to have stolen 15,000 membership passwords to the Uriminzokkiri website, releasing personal details of these accounts. Other, smaller pro-DPRK sites were also hacked, with personal details of members released. Any ROK citizens whose information is found on these membership lists could face criminal prosecution.[117]

Anonymous also initiated a DDoS attack of DPRK-related websites like Uriminzokkiri.com and Air Koryo on Kim Il-sung's birthday in early April 2013. One hacker belonging to the group was interviewed by an ROK news agency, saying, "Anonymous members not only want to attack the government's homepage, but will try to steal personnel data of North Korean leaders, and even hack into the North's nuclear facilities." Although there is no evidence the group has gotten into DPRK servers or intranet, they claim to have plans to do so.[118]

A 2014 report by Hewlett-Packard on North Korea cyber-capabilities highlights the difficulties that arise from the nature of the internet in North Korea.[119]

> North Korea's Internet infrastructure and the regime's strict control over its use ensures that there are no rogue actors and that all officially sanctioned actors exercise careful OPSEC and PERSEC practices in order to prevent inadvertent information leaks. In other words, there was no significant identifying information in the form of an OSINT trail left behind by the actors. This hinders collection of original, actionable threat intelligence and individual actor attribution.
>
> Today North Korea's air-gapped networks and prioritization of resources for military use provide both a secure and structured base of operations for cyber operations and a secure means of communications. North Korea's hermit infrastructure creates a cyber-terrain that deters reconnaissance. Because North Korea has few Internet connections to the outside world, anyone seeking intelligence on North Korea's networks has to expend more resources for cyber reconnaissance.

The report drew from several government, media, and scholarly sources in order to draw a picture of the groups and institutions within North Korea that execute and support its cyber-warfare capabilities.

1. Unit 35 – "The Central Party Committee oversees the Central Party Investigative Group, also known as Unit 35. Unit 35 is reportedly responsible for technical education and training of cyber warriors. The Unification Bureau's132 Operations Department is responsible for cyber-psychological warfare, organizational espionage, and oversight of Unit 204."
2. Unit 204 – "Unit 204's responsibilities include planning and execution of cyber-psychological warfare operations and technological research."
3. Psychological Operations Department of the North Korea Defense Commissions – This institution also engages in cyber-psychological warfare.

4. Unit 121 - Unit 121, North Korea's premier hacking unit, was estimated to consist of 3000 personnel in 2012. South Korea's Yonhap News Agency increased that number to 5900 in July 2014. Of these 5900 personnel, about 1200 of them are professional hackers. Yonhap stated that 100 cyberwarriors per year were trained at North Korea's Mirim University, though the source for this information could not be corroborated.[120] While the quality of this training cannot be precisely verified, it is known that the North Korean school system places heavy emphasis on mathematics, which has led North Korea to feel confident of its abilities to nurture capable programmers, cryptographers, and security researchers. "Unit 121 comprises both an intelligence component and an attack component. Unit 121's headquarters is in the Moonshin-dong area of Pyongyang, near the Taedong Rivber. It also has components that conduct operations from within China. One of Unit 121's command posts is Chilbosan Hotel in Shenyang, the capital of Liaoning Province, which borders North Korea." [121]

5. Lab 110 – "Both Unit 121 and an entity known as Lab 110 are reported to maintain technical reconnaissance teams responsible for infiltrating computer networks, hacking to obtain intelligence, and planting viruses on enemy networks."[122]

6. Office 225 / The 225th Bureau – This institution is "responsible for training agents, infiltration operations in South Korea, and creation of underground political parties in order to incite disorder and revolution."[123] It plays a more traditional intelligence and psychological operations role, rather than focusing on cyber operations."

7. No. 91 Office – "The No. 91 Office, an office responsible for hacking operates out of the Mangkyingdae-district of Pyongyang."

8. Korea Computer Center (KCC) - KCC is "North Korea's leading government research venter for information technology. KCC has eleven regional information centers and eight development and production centers. Other countries with KCC branch offices include China, Syria, Germany, and United Arab Emirates. KCC has a vested interest in Linuz research and is responsible for the development of North Korea's national operating system, Red Star OS."[124] "In 2011, South Korean police arrested five individuals, including one Chinese national, for allegedly collaborating with North Korean hackers affiliated with the Korea Computer Center to steal money via online games. According to South Korean reports, the culprits used an auto-player to quickly progress in the massively multiplayer online role-playing game (MMORPG) "Lineage" and were able to use the game's market to obtain real currency. In 2013, South Korean officials released information stating they had found evidence that North Korea was using games as a medium for infecting machines and launching cyber-attacks. North Korea had used game downloads to infect 100,000 South Korean machines for a botnet used to launch a distributed denial of service (DDoS) attack against Incheon Airport. This clever tactic sought to leverage a seemingly innocent game as a force multiplier in order to amplify the effects of a DDoS attack on a critical infrastructure target. However, in this case, there was little impact on the target."

9. Ministry of State Security - "The Ministry of State Security (MSS), also known as the State Security Department, is North Korea's primary counterintelligence service. It is considered an autonomous agent of the regime and reports directly to leader Kim Jong Un….the MSS also reportedly has a communications monitoring and computer hacking group."[125]

10. Reconnaissance General Bureau (RGB) – "The RGB has a role in both traditional and cyber operations. In the past, the RGB has sent agents on overseas military assistance missions to train insurgent groups. The RGB reportedly has a special operations forces (SOF) element118 and oversees six bureaus that specialize in operations, reconnaissance, technology and cyber matters, overseas intelligence collection, inter-Korean talks, and service support. Two of these bureaus have been identified as the No. 91 Office and Unit 121."

11. Chongryon and the Liaison Department of the Worker's Party- This department "oversees a faction of ethnic North Koreans residing in Japan who are critical to North Korea's cyber and intelligence programs. This group, which was established in 1955, is referred to by various names including the Chosen Soren, Chongryon, and the General Association of Korean Residents in Japan… The Chongryon's underground group known as the Gakushu-gumi, or "the study group", gathers intelligence for North Korea and helps the regime procure advanced technologies."[126]

In December 2014, Sony suffered a cyber-attack that broke into Sony's computer network and revealed internal emails and information. The attack was attributed to North Korean retaliation for

a comedy film that Sony produced about American journalists being tasked by the CIA to kill Kim Jong-un. North Korea denied any involvement, but praised it. Experts believe the hackers may have been inside Sony's network for months. Hackers threatened violence at any theaters that showed the movie, which eventually led Sony to cancel showing the film.[127]

As a result of many recent cyber-attacks, the Sony incident became the catalyst for the Obama administration to establish a new agency under the Director of National Intelligence.[128] The Cyber Threat Intelligence Integration Center, as articulate in a Presidential Memorandum released on February 25, 2015, will "provide integrated all-source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting US national interests".[129]

In 2015, the hacking group previously implicated in the Sony breach launched a series of attacks against several Asian banks, stealing billions of dollars. If instigated by the DPRK government, the attacks would constitute the first occurrences of a nation-state engaging in cyber-attacks for financial gain. [130]The next year, North Korea was implicated in stealing the personal consumer data of South Korean citizens, as part of their pursuit of foreign currency. This matched a longstanding pattern of DPRK cyber-attacks on South Korean government, banking and media systems.[131]

Electronic Warfare and SIGINT

Jane's notes that since the mid-1990s, the DPRK has increased its electronic warfare (EW) efforts as one of the primary components of an asymmetric warfare strategy against the US and the ROK. The administration and training of all EW and signals intelligence (SIGINT) assets in the Army is overseen by the Electronic Warfare Bureau (EWB). The DPRK keeps a police battalion at the DMZ, composed of eight to 12 police companies, that is in charge of a variety of ground-surveillance equipment – such as thermal and infrared imaging devices, acoustic and seismic sensors, and radar. The police force also has a basic SIGINT collection ability, especially at the Joint Security Area at Panmunjom.[132]

Deployed near the DMZ, division-level SIGINT/EW units have responsibility for operations, spanning from their forward line to 15-30 km behind the US/ROK force deployment. At the corps level, SIGINT/EW battalions have responsibility for up to a 75-150 km depth. In addition, EWB independent units also likely support corps and division efforts.[133]

> In August 2010, users of Global Positioning System (GPS) in the northwest section of the ROK, including sections of the West Sea, experienced an unexpected degradation or loss of signal. Subsequent investigation revealed that the cause for this was jamming - presumably by the KPA - from an emitter located in the area around Kaesong.
>
> While the DPRK has intermittently conducted jamming operations against ROK/US military and commercial broadcasts over the years this was the first major incident of GPS jamming. The KPA reportedly acquired GPS jamming equipment from Russia during the 1990s or early 2000s and subsequently modified it and began manufacturing two different systems. Subsequent reports indicated that the KPAs GPS jammers were mobile units mounted on "electronic warfare vehicles."
>
> Following the November 2010 attack upon the island of Yonp'yong-do the ROK Army deployed UAVs to monitor KPA activities. The KPA, however, reportedly jammed the UAV's navigation system, rendering them ineffective. More jamming occurred in March 2011 during the joint ROK-US 'Ulchi Freedom Guardian' exercises, when the KPA engaged in random GPS jamming harassment by sporadically jamming at five to 10 minutes intervals.
>
> The jamming originated from the area of Haeju, Kaesong and Kumgang-san and had a range of approximately 100 km. During March 2011 and the again for 16 days in May 2012 the KPA conducted GPS jamming

> operations along the west coast, north of Seoul. The May incident effected the operations of 670 commercial airliners and 110 vessels in the Yellow Sea. These operations are believed to have conducted by elements of the Reconnaissance General Bureau.

ROK Cyber Defense

As has been touched upon earlier, South Korea has been increasing its asymmetric capabilities in order to better defend against new forms of DPRK attacks. In terms of cyber capabilities, the IISS report stated,[134]

> South Korea established a Cyber Warfare Command Centre in early 2010, with over 200 personnel, in the wake of a substantial distributed denial of service attack in 2009. The new centre responds to the attention given to cyber and information security by the National Intelligence Service and the Defense Security Command. South Korea published an 'Internet White Paper' in 2009.

Other sources indicate the ROK plans to add 1,000 personnel to its Cyber Warfare Command Center over the 2013-2017 period. Increasing personnel and attention to this area is part of a much broader cyberwarfare effort by the ROK's National Intelligence Service and the Defense Security Command.[135]

The DPRK has accused South Korea and the US of carrying out cyber-attacks on DPRK websites;[136] one DPRK state-run paper stated in March 2013, "It is nobody's secret that the U.S. and south Korean puppet regime are massively bolstering up cyber forces in a bid to intensify the subversive activities and sabotages against the DPRK…They are seriously mistaken if they think they can quell the DPRK's voices of justice through such base acts."[137]

In response to DPRK cyber-attacks, the US and South Korea held the first Korea-US National Defense Cyber Cooperation Working Group (CCWG) in February 2014. This group provided an "opportunity for the two countries to share information about cyber threats and enhance the all-around cooperation of cyber policy, strategy, doctrine, personnel and training," according to the South Korean Defense Ministry.[138] This will likely be an early step in South Korea's efforts to consolidate its cyber strategy. The Korea Institute for Defense Analysis noted that:[139]

> …because the South Korean cyber security system is decentralized, each department establishes its own organization and strategies. The differences among the departments in terms of approaching cyber security makes it impossible to streamline policy in an efficient manner. Additionally, because of this decentralized structure, post-incident management for recurrence prevention is difficult to accomplish, which thereby renders inefficient any comprehensive, preventative policymaking.

[1] Republic of Korea, Ministry of National Defense, 2010 Defense White Paper, 30.
[2] IISS, *Military Modernization 2013*, 270.
[3] Due to secrecy and limited open source information, all available personnel figures are rough estimates.
[4] IHS Jane's: Defence & Security Intelligence Analysis, "Jane's World Armies: North Korea," *IHS Jane's*, October 18, 2012.
[5] Republic of Korea, Ministry of Defense, *2014 Defense White Paper.*
[6] Office of the Secretary of Defense, *Military and Security Developments Involving the Democratic People's Republic of Korea, 2015*, 12.
[7] IISS, *Military Balance, 2016*. Note that the word "sniper" can also mean "sharpshooter" or "marksman."
[8] IHS Jane's: Defence & Security Intelligence Analysis, "Jane's World Armies: North Korea," *IHS Jane's*, 2016.
[9] Ibid.
[10] Ibid.
[11] Ministry for Unification and Institute for Unification Education, *Understanding North Korea*, ROK Government, 2012, 129.
[12] IHS Jane's: Defence & Security Intelligence Analysis, "Jane's World Armies: North Korea," *IHS Jane's*, 2016.
[13] Ibid.
[14] IHS Jane's, "Jane's Sentinel Security Assessment – China and Northeast Asia: North Korea," *IHS Jane's*, July 2, 2014, Article 3, 12.
[15] Ministry for Unification and Institute for Unification Education, *Understanding North Korea*, ROK Government, 2012, 129-31.
[16] Global Security.org, "Korea Demilitarized Zone Incidents," http://www.globalsecurity.org/military/ops/dmz.htm.
[17] Ibid.
[18] See IHS Jane's: Defence & Security Intelligence Analysis, "Jane's World Armies: North Korea," October 18, 2012.
[19] Global Security.org, "Korea Demilitarized Zone Incidents."
[20] Ibid.
[21] IHS Jane's: Defence & Security Intelligence Analysis, "Jane's World Armies: North Korea," IHS Jane's, October 18, 2012.
[22] Ibid.
[23] Barbara Demick, "Thousands of North Korean tunnels hide arms secrets," *Los Angeles Times,* November 13, 2003.
[24] IHS Jane's: Defence & Security Intelligence Analysis, "Jane's World Armies: North Korea," *IHS Jane's*, October 18, 2012.
[25] Ministry for Unification and Institute for Unification Education, *Understanding North Korea*, ROK Government, 2012, 123-5.
[26] IHS Jane's: Defence & Security Intelligence Analysis, "Jane's World Armies: North Korea," *IHS Jane's*, October 18, 2012.
[27] Ibid.
[28] Ibid.
[29] "N. Korea Has World's Largest Artillery Force: US," American Foreign Press, April 24, 2009.
[30] Republic of Korea, Ministry of Defense, *2014 Defense White Paper.*
[31] Joseph S. Bermudez Jr., "The Yonp'yong-do Attack, November 23, 2010, Pt II," *KPA Journal* 1, no. 12.
[32] Ibid.
[33] Barbara Demick, "Seoul's Vulnerability Is Key to War Scenarios," *Los Angeles Times*, May 27, 2003.
[34] IISS. *Military Balance, 2016*.
[35] "Spotlight on S. Korea's Special Forces," *The Chosun Ilbo* (English edition), January 24, 2011, http://english.chosun.com; "S. Korea's Special Forces 'Vastly Outnumbered' by N. Korea's," *The Chosun Ilbo* (English edition), January 6, 2011, http://english.chosun.com; "History of Special Operations Command Korea" United States Eighth Army website (2010), http://8tharmy.korea.army.mil/.
[36] Ibid.
[37] Ibid.
[38] Hannah Fischer, *North Korean Provocative Actions, 1950–2007*, Congressional Research Service, April 20, 2007.
[39] US State Department, *Country Reports on Terrorism 2011*, July 2012, 42-43.

[40] US State Department, "North Korea," *Country Reports on Terrorism 2015*.
[41] "N. Korea, Iran strike mineral resources-for-oil deal," Yonhap News Agency, April 25, 2013.
[42] Office of the Secretary of Defense, *Military and Security Developments Involving the Democratic People's Republic of Korea, 2013*, 17, 20-22.
[43] Sheena Chestnut, "Illicit Activity and Proliferation: North Korean Smuggling Networks," *International Security* 32:1, 2009, 99.
[44] Ibid., 102.
[45] US State Department*, Country Reports on Terrorism 2011*, July 2012, 43-45.
[46] US State Department, "South Korea," *Country Reports on Terrorism 2011*, April 2012, 42-43.

[47] Sheena Chestnut Greitens, "Illicit: North Korea's Evolving Operations toEarn Hard Currency", Committee for Human Rights in North Korea, 2014.

[48] Daniel Wertz and Ali Vaez, "Sanctions and Nonproliferation in North Korea and Iran: A Comparative Analysis," Federation of American Scientists, June 2012, 7, 13; Sheena Chestnut, "Illicit Activity and Proliferation: North Korean Smuggling Networks," *International Security* 32:1, 2009, 83-94; Liana Sun Wyler and Dick K. Nanto, *North Korean Crime-for-Profit Activities,* Congressional Research Service, 2.
[49] Sheena Chestnut, "Illicit Activity and Proliferation: North Korean Smuggling Networks," *International Security* 32:1, 2009, 85-95.
[50] Ibid., 85-6.
[51] Paul Rexton Kan, Bruce E. Bechtol Jr, Romert M. Collins, *Criminal Sovereignty: Understanding North Korea's Illicit International Activities*, Strategic Studies Institute, March 2010, 10-11.
[52] Liana Sun Wyler and Dick K. Nanto, *North Korean Crime-for-Profit Activities,* Congressional Research Service, 3-4.
[53] Paul Rexton Kan, Bruce E. Bechtol Jr, Romert M. Collins, *Criminal Sovereignty: Understanding North Korea's Illicit International Activities*, Strategic Studies Institute, March 2010, 10-11.
[54] Sheena Chestnut, "Illicit Activity and Proliferation: North Korean Smuggling Networks," *International Security* 32:1, 2009, 90-93; Paul Rexton Kan, Bruce E. Bechtol Jr, Romert M. Collins, *Criminal Sovereignty: Understanding North Korea's Illicit International Activities*, Strategic Studies Institute, March 2010, 2-7.
[55] "N Korean leader has over $1 billion in slush funds abroad: report," Yonhap News Agency, April 25, 2013.
[56] Sheena Chestnut, "Illicit Activity and Proliferation: North Korean Smuggling Networks," *International Security* 32:1, 2009, 90-93; Paul Rexton Kan, Bruce E. Bechtol Jr, Romert M. Collins, *Criminal Sovereignty: Understanding North Korea's Illicit International Activities*, Strategic Studies Institute, March 2010, 2-7.
[57] Paul Rexton Kan, Bruce E. Bechtol Jr, Romert M. Collins, *Criminal Sovereignty: Understanding North Korea's Illicit International Activities*, Strategic Studies Institute, March 2010, 17-18.
[58] Sheena Chestnut, "Illicit Activity and Proliferation: North Korean Smuggling Networks," *International Security* 32:1, 2009, 88-91; Paul Rexton Kan, Bruce E. Bechtol Jr, Romert M. Collins, *Criminal Sovereignty: Understanding North Korea's Illicit International Activities*, Strategic Studies Institute, March 2010, 8-9, 18.
[59] Ibid.
[60] Liana Sun Wyler and Dick K. Nanto, *North Korean Crime-for-Profit Activities,* Congressional Research Service, 6.
[61] Paul Rexton Kan, Bruce E. Bechtol Jr, Romert M. Collins, *Criminal Sovereignty: Understanding North Korea's Illicit International Activities*, Strategic Studies Institute, March 2010, 10.

[62] Sheena Chestnut Greitens, "Illicit: North Korea's Evolving Operations toEarn Hard Currency", Committee for Human Rights in North Korea, 2014.

[63] Sheena Chestnut, "Illicit Activity and Proliferation: North Korean Smuggling Networks," *International Security* 32:1, 2009, 88-91.
[64] Paul Rexton Kan, Bruce E. Bechtol Jr, Romert M. Collins, *Criminal Sovereignty: Understanding North Korea's Illicit International Activities*, Strategic Studies Institute, March 2010, 15-16; Liana Sun Wyler and Dick K. Nanto, *North Korean Crime-for-Profit Activities,* Congressional Research Service, 11.
[65] Ibid.
[66] Liana Sun Wyler and Dick K. Nanto, *North Korean Crime-for-Profit Activities,* Congressional Research Service, 12-3.
[67] Sheena Chestnut, "Illicit Activity and Proliferation: North Korean Smuggling Networks," *International Security* 32:1, 2009, 89-96.

[68] Sheena Chestnut Greitens, "Illicit: North Korea's Evolving Operations to Earn Hard Currency", Committee for Human Rights in North Korea, 2014.

[69] Paul Rexton Kan, Bruce E. Bechtol Jr, Romert M. Collins, *Criminal Sovereignty: Understanding North Korea's Illicit International Activities*, Strategic Studies Institute, March 2010, 12-14, 18.
[70] Liana Sun Wyler and Dick K. Nanto, *North Korean Crime-for-Profit Activities,* Congressional Research Service, 8.

[71] Sheena Chestnut Greitens, "Illicit: North Korea's Evolving Operations to Earn Hard Currency", Committee for Human Rights in North Korea, 2014.

[72] Brian R. Moore and Riza De Los Reyes, "What's Behind North Korea's Recent Counterfeiting?" *The Diplomat*, July 06, 2016.

[73] Ibid., 13-14.
[74] Ibid., 14-15.
[75] Sheena Chestnut, "Illicit Activity and Proliferation: North Korean Smuggling Networks," *International Security* 32:1, 2009, 92.
[76] Liana Sun Wyler and Dick K. Nanto, *North Korean Crime-for-Profit Activities,* Congressional Research Service, 3.
[77] Ibid., 5.

[78] Sheena Chestnut Greitens, "Illicit: North Korea's Evolving Operations to Earn Hard Currency", Committee for Human Rights in North Korea, 2014.

[79] Sheena Chestnut, "Illicit Activity and Proliferation: North Korean Smuggling Networks," *International Security* 32:1, 2009, 95-6.
[80] Ibid.
[81] Sheena Chestnut, "Illicit Activity and Proliferation: North Korean Smuggling Networks," *International Security* 32:1, 2009, 97; Liana Sun Wyler and Dick K. Nanto, *North Korean Crime-for-Profit Activities,* Congressional Research Service, 7.
[82] Sheena Chestnut, "Illicit Activity and Proliferation: North Korean Smuggling Networks," *International Security* 32:1, 2009, 97; Japanese Ministry of Defense, *Defense of Japan 2012*, 19.
[83] Sheena Chestnut, "Illicit Activity and Proliferation: North Korean Smuggling Networks," *International Security* 32:1, 2009, 100.
[84] Office of the Secretary of Defense, *Military and Security Developments Involving the Democratic People's Republic of Korea, 2013*, 21-22.
[85] It should be kept in mind that these export approximations are all reported – thus, the reports might not be true. At the same time, there could also be significant missile exports that were not reported; Markus Schiller, *Characterizing the North Korean Nuclear Missile Threat*, RAND, 2012, xiii, 38.
[86] Emma Chanlett-Avery and Ian E Rinehart, *North Korea: U.S. Relations, Nuclear Diplomacy, and Internal Situation*, 17; Liana Sun Wyler and Dick K. Nanto, *North Korean Crime-for-Profit Activities,* Congressional Research Service, 3.
[87] NTI, "North Korea: Missile," updated February 2013, http://www.nti.org/country-profiles/north-korea/delivery-systems/.
[88] Dennis C Blair, *Annual Threat Assessment of the Intelligence Community*, Senate Select Committee on Intelligence, February 12, 2009.
[89] Sheena Chestnut, "Illicit Activity and Proliferation: North Korean Smuggling Networks," *International Security* 32:1, 2009, 93, 104-109.
[90] Jeffrey Lewis, "Oryx Blog on DPRK Arms Exports," Arms Control Wonk, June 25, 2014, http://lewis.armscontrolwonk.com/archive/7370/oryx-blog-on-dprk-arms-exports.

[91] NTI "Syria", updated November 2014, http://www.nti.org/learn/countries/syria/delivery-systems/

[92] "UN arms embargo on North Korea", SIPRI, March 7, 2016.

[93] Sheena Chestnut Greitens, "Illicit: North Korea's Evolving Operations to Earn Hard Currency", Committee for Human Rights in North Korea, 2014.

[94] Japanese Defense Ministry, *Japanese National Defense 2012*, 24.

[95] IISS, *Military Balance 2013*, 272-3.
[96] Japanese Defense Ministry, *Japanese National Defense 2012*, 24.
[97] IISS, *Military Balance 2013*, 272-3.
[98] The Republic of Korea Armed Forces, "Innovation Makes Us Powerful," ROK Ministry of National Defense, 2010, 35.
[99] IISS, *Military Balance 2013*, 272-3.

[100] Joyce Lee and Tony Munroe, "South Korea seeks bigger role in global arms bazaar", *Reuters,* April 22, 2015.

[101] Jon Grevatt, "South Korean defence exports over USD3 billion in 2015", HIS 360, January 19, 2016.

[102] Ronald L. Burgess Jr., "Annual Threat Assessment," February 16, 2012, 9.
[103] IISS, *Military Balance 2013,* 312.
[104] Office of the Secretary of Defense, *Military and Security Developments Involving the Democratic People's Republic of Korea, 2013*, 9, 11.
[105] Ji Myung-kil, "Washington Reacts to Cyber Attack in South Korea" Arirang News, March 21, 2013; Park Bo-ram, "N. Korea's state-sponsored hackers emerge as global threat," Yonhap News Agency, March 21, 2013; Spencer Ackerman, "Pentagon Warns North Korea Could Become a Hacker Haven," *Wired*, May 2, 2013.
[106] Max Fisher, "South Korea under cyber attack: Is North Korea secretly awesome at hacking?," *Washington Post*, March 20, 2013.
[107] Ibid.
[108] Park Bo-ram, "N. Korea's state-sponsored hackers emerge as global threat," Yonhap News Agency, March 21, 2013.
[109] Kim Kwang-tae, "N. Korea's hacking capabilities advance," Yonhap News Agency, April 11, 2013.
[110] Japanese Ministry of Defense, *Defense of Japan 2012*, 15.
[111] Park Bo-ram, "N. Korea's state-sponsored hackers emerge as global threat," Yonhap News Agency, March 21, 2013.
[112] Choe Sang-hun, "North Korea Threatens U.S. Military Bases in the Pacific," *New York Times*, March 21, 2013.
[113] Park Bo-ram, "N. Korea's state-sponsored hackers emerge as global threat," Yonhap News Agency, March 21, 2013.
[114] Kim Kwang-tae, "N. Korea's hacking capabilities advance," Yonhap News Agency, April 11, 2013.
[115] Park Bo-ram, "N. Korea's state-sponsored hackers emerge as global threat," Yonhap News Agency, March 21, 2013; Kim Kwang-tae, "N. Korea's hacking capabilities advance," Yonhap News Agency, April 11, 2013.
[116] Marcus Noland, "What Goes Around Comes Around: Operation Free Korea," Peterson Institute for International Economics, April 24, 2013.
[117] Ibid.
[118] Ibid.
[119] HP Security Research, "Profiling an enigma: The mystery of North Korea's cyber threat landscape," *HP Security Briefing*, Episode 16, August 2014, 3, 25.
[120] "N. Korea doubles number of cyber warriors over 2 years: sources," Yonhap News Agency, July 6, 2014.
[121] HP Security Research, "Profiling an enigma: The mystery of North Korea's cyber threat landscape," *HP Security Briefing*, Episode 16, August 2014, 21, 26.
[122] Ibid., 21.
[123] Office of the Secretary of Defense, *Military and Security Developments Involving the Democratic People's Republic of Korea, 2013*, 14.
[124] HP Security Research, "Profiling an enigma: The mystery of North Korea's cyber threat landscape," *HP Security Briefing*, Episode 16, August 2014, 11.
[125] Ibid., 20.
[126] Ibid., 23.
[127] Eric Tucker and Rami Abdollah, "Digital Dilemma: How Will US Respond to Sony Hack," ABC News, December 18, 2014, http://abcnews.go.com/Technology/wireStory/korea-unprecedented-cyberattack-sony-27678943.
[128] Ellen Nakashima, "New agency to sniff out threats in cyberspace," *Washington Post*, February 10, 2015.
[129] The White House, "Presidential Memorandum—Establishment of the Cyber Threat Intelligence Integration Center," February 25, 2015, http://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat.

[130] Nicole Perlroth and Michael Corkery, "North Korea Linked to Digital Attacks on Global Banks", *New York Times,* May 26, 2015.

[131] Cheo Sang-Hun, "North Korea Stole Data of Millions of Online Consumers, South Says", *New York Times,* July 28, 2016.

[132] IHS Jane's: Defence & Security Intelligence Analysis, "Jane's World Armies: North Korea," *IHS Jane's*, October 18, 2012.
[133] Ibid.
[134] IISS, *Military Balance 2013*, 312.
[135] IISS. *Military Balance, 2013*.
[136] Ji Myung-kil, "Washington Reacts to Cyber Attack in South Korea" *Arirang News*, March 21, 2013.
[137] Choe Sang-hun, "North Korea Sees South and U.S. Behind Cyberstrikes," *New York Times*, March 15, 2013.
[138] Chul Hwan Kim, "Strengthened Korea-US joint response to cyber threats," *Korea Defense Daily*, February 19, 2014, http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_47261&boardSeq=O_61294&titleId=&id=mnd_eng_030100000000.
[139] Young-do Kim et al., "Major Issue of the National Cyber Security System in South Korea, and its Future Direction," *Korean Journal of Defense Analysis* 25, no. 4 (December 2013), 449.