NORTH KOREAN STRATEGIC STRATEGY:

COMBINING CONVENTIONAL WARFARE WITH THE ASYMMETRICAL EFFECTS OF CYBER WARFARE

By

Jennifer J. Erlendson

A Capstone Project Submitted to the Faculty of

Utica College

March, 2013

In Partial Fulfillment of the Requirement for the Degree

Master of Science – Cybersecurity – Intelligence and Forensics

© Copyright 2013 by Jennifer J. Erlendson

All Rights Reserved

Abstract

Emerging technologies play a huge role in security imbalances between nation states. Therefore, combining the asymmetrical effects of cyberattacks with conventional warfare can be a force multiplier; targeting critical infrastructure, public services, and communication systems. Cyber warfare is a relatively inexpensive capability which can even the playing field between nations. Because of the difficulty of assessing attribution, it provides plausible deniability for the attacker. Kim Jong Il (KJI) studied the 2003 Gulf War operational successes of the United States (U.S.) and the United Kingdom (U.K.), noting the importance of high-tech weapons and information superiority. KJI realized the only way to compete with the U.S.'technology and information superiority was through asymmetric warfare. During the years that followed, the U.S. continued to strengthen its conventional warfare capabilities and expand its technological dominance, while North Korea (NK) sought an asymmetrical advantage. KJI identified the U.S.' reliance on information technology as a weakness and determined it could be countered through cyber warfare. Since that time, there have been reports indicating a NK cyber force of 300-3000 soldiers; some of which may be operating out of China. Very little is known about their education, training, or sophistication; however, the Republic of Korea (ROK) has accused NK of carrying out cyber-attacks against the ROK and the U.S since 2004. Although NK is the likely culprit in the attacks, there is no forensic evidence to definitively identify NK as the attacker.

Acknowledgments

First and foremost, I would like to thank my family and friends for their patience and encouragement while I pursued this goal. I would also like to thank my coworkers who were always willing to provide their expertise, assistance, and humor when needed.

A special thank you to Professor Draz, for his time, patience, and mentorship; he made getting through the Capstone project possible. And finally, thank you to Professor Nichols and Professor Giordano for developing a fun and challenging Cybersecurity program.

Table of Contents

List of Illustrative Materials

North Korean Strategic Strategy: Combining Conventional Warfare with the Asymmetrical Effects of Cyber Warfare

Definition of the Problem

Every day the world is becoming more reliant upon technology and interconnected through the Internet. This reliance has added a new dimension to the conventional battlespace known as cyberspace. The U.S. government is striving to develop a national strategy that will allow it to achieve cyberspace superiority through a combination of military information superiority and technological modernization. Government and private sector digital assets could very well be at risk with NK's advancement in Computer Network Operations (CNO).

In his 2012 testimony to the U. S. Congress, General James D. Thurman (Thurman), Commander, U.S.- ROK Combined Forces stated,

> The newest addition to the NK asymmetric arsenal is a growing cyber warfare capability. NK employs sophisticated computer hackers trained to launch cyber infiltration and cyberattacks against the ROK and U.S. Such attacks are ideal for N K, providing the regime a means to attack ROK and U.S. interests without attribution, and have been increasingly employed against a variety of targets including military, governmental, educational, and commercial institutions (Thurman, 2012).

Purpose Statement

The purpose of this research was to assess the NK cyber capabilities, vulnerabilities, limitations, organization, and desired end state. This threat assessment reviewed open source reporting which identified income sources, state and non-state support, education and training, and infrastructure to conduct CNO. Three questions were researched:

1) How will Kim Jong-un (KJU) incorporate cyber warfare into NK's overall military and national security strategies?
2) What is NK's level of cyber warfare sophistication?
3) How does a NK cyber threat affect the U.S. posture and responsibility on the Korean peninsula?

Justifying the Problem

Testifying before the U.S. Senate Armed Services Committee in March 2007, General James Cartwright (Cartwright), then-Commander of U.S. Strategic Command (STRATCOM) made the following statement:

> However, not unlike the targets of pirates or train robbers of the past, America is under widespread attack in cyberspace. Our freedom to use cyberspace is threatened by the action of criminals, terrorists, and nations alike. Each seeks their own form of unique advantage, be it financial, political, or military, but together they threaten our freedom to embrace the opportunity offered by a globally connected and flattened world. The magnitude of cost, in terms of real dollars dedicated to defensive measures, lost intellectual capital and fraud cannot be overestimated, making these attacks a matter of great national interest. Unlike the air, land, and sea domains, we lack dominance in cyberspace and could grow increasingly vulnerable if we do not fundamentally change how we view this battle space (Cartwright, 2007).

KJI. After the 2003 Gulf War, former NK leader, KJI, studied the operational successes of the U.S. and the U.K., noting the importance of high-tech weapons and information superiority. In 2009, KJI stated, "modern warfare has now changed to an information technology war from the previous wars of bullets and fuel" (Yonhap News, 2011). He also stated, "Cyber

troops are my pride and audacity, together with the nuclear weapons" (2011). NK has voiced its intent to develop a cyber-capability; however, the extent of that capability is unknown.

Taking the lessons learned from the 2003 Gulf War, KJI realized the only way to compete with the U.S.' technology and information superiority was through asymmetric warfare. During the years that followed, the U.S. continued to strengthen its conventional warfare capabilities and expand its technological dominance, while NK sought an asymmetrical advantage. The former Assistant Secretary of Defense for Command, Control, and Intelligence, Art Money (Money) said, "The rest of the world realizes that you do not take the U.S. on in a military frontal sense, but you can probably bring it down or cause severe damage in a more oblique way" (Adams, 2001). KJI understood this concept and focused on the U.S.' weakness – the reliance on information technology which could be countered through cyber warfare.

KJU. KJI died in December 2012, leaving his twenty-something year old son, KJU as the "Great Successor." Relatively little was known about KJU or how he would lead the Kim regime – would he follow in his father's footsteps and strategic military strategy, or would he lead the country in a new direction. No one knew what to expect from this young, unknown leader.

The transition of leadership could not have come at a worse time for U.S.-NK relations. The U.S. had recently gotten NK back to the negotiation table regarding its nuclear program and the initial response was promising. Then on the day KJI's death was announced, NK conducted a short-range missile test. This may have been part of a routine drill or more likely it may have been part of a show of force as KJU carried on the Kim regime. Either way, it sent a foreboding message to the rest of the world.

In the hopes of calming tensions and fostering a good relationship on the Korean peninsula, NK and the U.S. signed the "Leap Day Deal" on February 29th, 2012. The U.S. agreed

to provide NK 240,000 tons of food and in return, NK would allow International Atomic Energy Agency (IAEA) inspectors back into the Yongbyon nuclear facility, and discontinue its uranium enrichment and missile testing (The Economist, 2012). This agreement provided a glimmer of hope that KJU was leading the country in a different direction. Nevertheless, 16 days later, NK announced it would commemorate the late Kim Il Sung (KIS), the "Great Leader's," 100th birthday, with a satellite launch. This launch was exactly the type of activity NK had just vowed not to conduct in return for the food aid. The launch was conducted on December 11th, 2012 and dashed all hope for peace on the Korean peninsula.

The international community voiced their concerns about the launch; the U.S. called it a highly provocative act which threatened the regional security and violated United Nations (UN) resolution. The UN Security Council (UNSC) also condemned the launch stating it was a "clear violation" of the UN resolutions, banning all missile and nuclear tests, imposed after NK conducted a series of nuclear tests in 2006 and 2009. China was also disappointed NK had gone through with the launch especially after having advised them not to (Miklaszewski & Boyle, 2012).

While NK says the intent of the launch was to put a Kwangmyongsong weather satellite into orbit, U.S. officials maintain the launch was a "thinly veiled attempt to test a three-stage ballistic missile capable of carrying a nuclear warhead as far as the U.S. West Coast" (Miklaszewski & Boyle, 2012). This was NK's first successful launch of a three-stage rocket and demonstrates NK's intent on acquiring an intercontinental ballistic missile, capable of carrying a nuclear warhead (BBC News, 2012). Just a year after KJI's death, KJU has conducted two long-range/ballistic missile launches. He appears to be utilizing the same policies as his father, continuing the same disregard for UN resolutions and international disdain.

KJU continued to disregard international pressure to abandon the nuclear program; from a satellite launch just two months ago, to a new round of nuclear tests on February 12th, 2013. Commenting on the tests, NK insisted they were a "self-defensive measure against continued hostility by America" (The Economist, 2013). Again the international community voiced their condemnation for the tests. In a surprise reaction, China, NK's only ally, supported the UNSC's proposal to strengthen existing UN sanctions against NK (The Economist, 2013). Despite these actions, NK told China it was prepared to conduct additional nuclear tests and a possible rocket launch to force the U.S. back to the negotiation table (Lim, 2013).

Prior to the latest nuclear tests, the ROK government stated it would "respond firmly if NK followed through with its threat to conduct a third nuclear test" (Open Source Center, 2013). ROK will likely use its position as the president of the UNSC to gain additional support from the international community and impose additional sanctions against NK. These actions highlight the NK's unwavering desire and KJU's determination to achieve his father and grandfather's goal of acquiring nuclear weapons. Combining a nuclear capability with cyber warfare and the unpredictable nature of NK could produce a worthy opponent for the U.S. and cause the ROK and U.S. governments to rethink their strategies on the Korean peninsula. Senior Korean defense officials have not ruled out the possibility of pre-emptive strikes as a possible countermeasure to NK fielding nuclear weapons (Chosun Ilbo, 2013).

Combining the asymmetrical effects of cyberattacks with conventional warfare can be a force multiplier; targeting critical infrastructure, public services, and communication systems. Cyber warfare is a logical choice for NK given its limited financial resources. CNO provides a much bigger 'bang for the buck;' a viable and sustainable military option. Cyber warfare is a

means to level the playing field for those that cannot match the U.S.'s conventional military strength. NK has the most to gain, and least to lose with the use of CNO.

Recent nuclear tests clearly indicate NK's intent to obtain nuclear weapons, but the possibility and extent of a cyber-capability is still relatively unknown. NK's development of a cyber-warfare capability would influence the U.S' response to state-sponsored cyber-attacks as well as the U.S. response to the stability of the Korean peninsula. NK would be a much greater threat in the region if it was capable of CNO.

NK was identified as the initiator for a number of cyberattacks against the U.S., ROK, and Japan between 2001 and 2011 (Appendix B). It is reasonable to believe the ROK would be NK's primary target. Technically, the two Koreas are still at war with each other and the ROK has weaker Internet security measures, lacks a military cyber warfare unit to counter attacks, and by infiltrating ROK systems, NK could conduct espionage activities against both ROK and the U.S. Because the U.S. supports the ROK, and is against NK acquiring nuclear weapons, it is also a logical target for NK.

If NK is able to acquire nuclear and cyber weapons, the U.S. will likely have to rethink its military strategy on the Korean peninsula. U.S. President Barack Obama commented on NK's April 2009 rocket launch, "Rules must be binding, violations must be punished, words must mean something" (Lind, 2012). The U.S., ROK, and Japan publically denounced NK's actions, yet there were no repercussions. U.S. President Barack Obama has continued the position of "strategic patience" in regards to NK (The Economist, 2012). In regards to the most recent tests, the U.S. Pentagon said NK's nuclear and missile programs were "a threat to U.S. national security and to international peace and security" (Lim, 2013).

Technology Dependency. The U.S.' reliance on technology makes it one of the most vulnerable to cyber warfare. In 2009, the U.S. Department of Defense (DoD) established U.S. Cyber Command (CYBERCOM) to take a proactive stance against espionage and criminal acts in cyberspace, while protecting and defending the DoD networks. CYBERCOM will

> direct the operations and defense of specified DoD information networks and prepare to, when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./allied freedom of action in cyberspace and deny the same to our adversaries (McMichael, 2010).

The information technology revolution has changed how Americans operate on a day-to-day basis; bills are paid online, emails or text messages are sent instead of "snail mailing" a letter, businesses and banks conduct transactions around the world in milliseconds, and our military relies heavily on technologically advanced weapons and assets. Cyberspace has been added as the fifth dimension to our conventional battlefield of air, land, sea, and space. We have expanded our military superiority into space with: reconnaissance, communication, weather, Global Positioning System (GPS), and early warning satellites. A loss, degradation, or theft of information from any one of these information technology systems could severely hamper military operations, as well as every sector of our economy (energy, transportation, banking, information technology (IT), emergency services, water, etc.) through this network of networks.

The U.S. is a society totally dependent on interlocking networks and nodes for communications, transportation, energy transmission, financial transactions, and essential government and public services. Disruption of key nodes by terrorists could cause havoc, untold expense, and perhaps even mass deaths. We are, in the jargon of the trade, a 'target-rich environment' (Leahy, 1990).

New Battlefield. Deputy U.S. Defense Secretary William J. Lynn (Lynn) III stated, "bits and bytes can be as threatening as bullets and bombs" (Pellerin, 2011). In 2009, cyberspace was declared a strategic national asset by U.S. President Obama and he requested a cyberspace policy review be conducted (Masters, 2011).

Technology and the Internet have transformed the conventional battle space from defined geographical locations to now include the vast, undefined and limitless cyberspace. Added to the ranks of conventional armies are zombie armies (botnets), and anyone else who is connected to the Internet and has the desire to wage a digital cyber war, regardless of their skill level.

Technological advancements have changed how quickly our adversaries are able to launch computer network attacks, exfiltrate data, and exploit digital weaknesses. The threats and adversaries are only a mouse click away from launching an attack on the U.S. "Nation-states and non-state actors, working alone or together, have greater access to actionable information, global finance, and destructive capabilities – including weapons of mass destruction" (Gannon, 2010). Regardless of their sophistication, individuals are able to launch, or assist in launching, cyberattacks against the U.S. with little possibility of attribution.

Cyber warfare is inherently asymmetrical; it has no boundaries, attribution is difficult, and the advances in technology are continuously changing the battlefield. Asymmetric warfare is "leveraging inferior tactical or operational strength against the vulnerabilities of a superior opponent to achieve disproportionate effect with the aim of undermining the opponent's will in order to achieve the asymmetric actor's strategic objectives" (Hess, Orthmann, & Cho, 2011).

Emerging technologies play a huge role in security imbalances within nation states, by providing plausible deniability to an attacker. They are able to conduct the attack while hiding behind emerging technology.

> Cyber-warfare [may be used] to disable a country's infrastructure, meddle with integrity of another country's internal military data, try to confuse its financial transactions or to accomplish any number of other possibly crippling aims, yet governments and national defense establishments at present have only limited ability to tell when they were under attack, by whom, and how they might respond (Tisdall, 2010).

Who the imbalance of power favors depends on what the method of attack is and what is targeted. The U.S. military's superior air power and the emerging technology in that area can deliver a powerful blow to most of our adversaries. However, the center of gravity for the air platforms is satellite communications for command and control; a well-placed cyberattack against a communication platform could cripple most of the U.S.' military assets. The U.S. has become so reliant on technology that any glitch in it could change the outcome of the conflict. How well the U.S. is able to defend an attack depends on how well they are able to war game possible attack scenarios and mitigate any associated risk.

Act of War. As of January 2013, U.S. Homeland Security Secretary Janet Napolitano (Napolitano) warned that a "cyber 9/11" was imminent and would target U.S. critical infrastructure (Charles, 2013). If this is true, the attacks would be transitioning from government entities and moving to the softer targets of the private sector. "We have seen cyber-attacks evolve from espionage attacks that steal intellectual property or monitor communication to disruptive or destructive attacks. Destructive and disruptive cyber-attacks are relatively uncharted – and troubling – territory," says Emilian Papadopoulos (Papadopoulos), Chief of Staff at Good Harbor Security Risk Management (Violino, 2013).

U.S. Secretary of Defense Leon Panetta (Panetta) stated, "A cyber-attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack on 9/11.

Such a destructive cyber terrorist attack could virtually paralyze the nation" (Williams, 2012). U.S. General Kehler (Kehler) and Secretary of Defense Lynn announced in July 2011 "any major cyber intrusion incident affecting the vital interests of the nation can be considered an act of war and could result in a conventional military answer" (Matei, 2011).

At the global level, there is not an international agreement as to what constitutes an act of cyber war, nor has it been well defined. "States are reluctant to treat cyber-attacks as acts of war and risk violating international law" (Carr & Shepherd, 2010). A cyber-attack can occur, but without attribution, there is little that can be done to retaliate against the attackers. Because of the nature of cyber-attacks it is virtually impossible to determine attribution during the attack. There is also the issue of state and non-state hackers committing the attacks.

International law forbids sovereign states to attack each other, but it does not address attacks committed by individuals against another sovereign state. Technically this could also be considered an act of war. The International Court of Justice has said that,

> States have a duty not to allow knowingly its territory to be used for acts contrary to the rights of other States. States are required under international law to take appropriate acts in order to protect the interests of other states from non-state actors within their borders (Carr & Shepherd, 2010).

International lawyers and sovereign states are aware of the cyber issues and are working to develop a clear definition of cyber warfare and what constitutes an act of war. In the interim, although it does not address all the issues, states are applying the traditional law of war to cyber warfare. The use of botnets could potentially be considered an act of war depending on what the target is what the intent of the attack is, and how much damage is caused. Emerging technology, Advanced Persistent Threats (APTs), and botnets are weapons of the new cyberspace battlefield.

Attribution remains a sticking point of determining if these actions should be considered an act of war or just individual hackers acting of their own free will.

Being able to contend with a multitude of threats simultaneously is one of the reasons why the U.S. is considered to be a superior military force. Technology has enabled the U.S. military to exploit our adversaries' weaknesses and has clearly identified a separation between those that have the technology and those that do not. While it may seem that the U.S. has the overall advantage in this respect, technology, while it is a great separator, it is also a great equalizer for military forces. The most technologically advanced U.S. weapons can also be neutralized through the employment of cyberattacks.

Kehler, Commander of U.S. STRATCOM said, "the new concerns surrounding space and cyberspace underscore the reality of the operating environment, that the threats and challenges we face in deterring adversaries are significantly different than the challenges we faced in the past" (Kehler, 2011). It is no longer a linear battlefield with military units facing off against one another. The threat comes from both state and non-state actors utilizing the technological dependencies and strengths of the U.S. against it. The U.S. relies heavily on the Internet and technology, not only for conventional warfare, but for normal day to day activities; any disruption to these activities could wreak havoc on the U.S. people and the economy.

Economic Impact. Although the study was conducted over twenty years ago, the National Research Council (NRC) was aware of the potential for cybercrime:

> We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable – to the effects of poor design and insufficient quality

> control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb (NRC, 1991).

Cybercrime is a type of cyber threat used by both states and non-state actors to cause economic instability. Cybercrime includes activities such as: electronic commerce theft, intellectual property rights or copyright infringement, privacy rights infringement, identity theft, credit card theft, unauthorized access to computer systems, phishing attacks, and stealing personally identifiable information (PII) to commit other criminal acts (Schell & Martin, 2006). Using cybercrime against the U.S. has become a very lucrative market. Research by the anti-virus (AV) company Symantec, reports that cybercrime costs the global economy over $388 billion a year.

In 2011, at least 74 million Americans were victims of cyber criminals. This malicious activity was estimated to cost the U.S. economy approximately $32 billion annually (Whittaker, 2011). Not only is attribution difficult in these cases, but bringing the individual(s) responsible to justice is nearly impossible. The crimes are often committed across national boundaries, the network traffic passes through many different nations, and the host country may not be inclined to transfer the criminal to the U.S. Having a computer with Internet access, basic to moderate computer knowledge and an individual or nation would be capable of waging an anonymous economic cyber war against the U.S. This makes cybercrime a very cost effective type of warfare against the U.S.; striking a strategic blow against one of the economic and technological superpowers.

> Information is as important as capital for businesses. No matter what kind of business you're in, networks and digital information underpin your operations. And when

networks are compromised or information is lost or misused, your business can suffer serious financial consequences (Cisco Systems, 2002).

"A recent Ponemon Institute (Ponemon) study on cybercrime cost, found that the median cost to respondent companies for cybercrime was $3.8M/year" (CipherPoint, 2012).This is a challenging and daunting task, requiring constant research, development, and training for the corporation's management and computer security staff.

Network security has become essential in recent years and will continue to be as more and more companies branch out to the Internet, and more data is stored electronically. Most companies are in some way integrated into the Internet, making not only their data vulnerable to attacks, but also personnel information. The Federal Bureau of Investigation (FBI) reports security breaches happen at a rate of thousands of attacks per day. Former FBI cyber security expert Shawn Henry (Henry) said, "Most major companies – like 94 percent – don't know that they have been hacked until a long time afterward" (Pitchford, 2012). The potential for reinfection is always present, as cyber actors modify, update, and share new attack vectors and vulnerabilities with other hackers.

Cyber Law. The legal system has not evolved as quickly to keep up with the emerging technology and the advances in intelligence collection capabilities. Intelligence leaders are also urging the U.S. Congress to act on a number of cyber laws to protect our U.S. based computer networks. They point out that cyber espionage is costing U.S. businesses approximately $300 billion a year in losses. Intrusions are attempted everyday on all sectors of our critical infrastructure. Zappos.com was hacked in 2012, affecting its 24 million customers; the cost of this intrusion has yet to be determined (Sullivan, 2012). Customers' PII, stolen from the

database, could be used to perpetrate additional criminal cyber activity in the future with socially engineered spear-phishing attacks.

International agreements are still being discussed and developed to determine how to deal with cyber events dealing with countries and non-state actors. Kehler addressed the need of fostering innovation and collaboration between private and government sectors to protect our information technology at the 2011 Cyber & Space Symposium.

> Protection of the information technology infrastructure is a huge problem that the government can't be expected to tackle on its own, nor can it ignore the private sector and expect them to figure it out on their own either. Whether it's the government or private sector, we're all connected. It will take a team effort to protect and defend our networks and critical infrastructures.

Knowledge Deficiencies

Closed Society. NK is a closed society, with very limited open source information available regarding its cyber capabilities. Much of what is known about NK's cyber capability has come from debriefing NK defectors. Within this hermit and reclusive country, where everything appears to be very compartmentalized, it seems unlikely for defectors to have access to, or knowledge about CNO capabilities.

Denial and Deception. Denial, deception, and misdirection are as old as warfare itself. The great military strategist Sun-tzu (Sun-tzu) said "all warfare is based upon deception" (Sawyer, 1994). NK and the Kim regime have proven to be masters of deception. These techniques are used by NK independently and jointly to gain a strategic cyber advantage. Disinformation by both Koreas further blurs the truth about NK's cyber capabilities.

> Disinformation can work well in cyberspace because, unlike handwritten materials, electronic data does not provide clues to deception in style and provenance (how it is obtained), and methods for detecting text inconsistencies do not work well for fixed-format audit records (Rowe, 2008).

Open source information. Credibility and reliability of open source information will be challenging to verify. Current ROK reporting suggests NK is conducting computer network exploitation (CNE), and computer network attacks (CNA) against South Korea. However, there is little to no forensic evidence to support this claim. South Korea's claim may be politically motivated to gain government funding for offensive cyber capabilities and/or ensure U.S. involvement on the Korean peninsula. NK may take advantage of the situation by not taking responsibility for the attacks, leaving the international community wondering if NK has a CNA capability.

KJU. If KJU's first year as the leader of NK is any indication of how he intends to continue to conduct business in the international community, it could be a very volatile future. So far he has shown complete disregard for regional stability and international sanctions. The young leader appears to be just as unpredictable, if not more so, than as his predecessors. With the recent threats to conduct more nuclear tests, the world will be watching for signs of increased instability and the proliferation of nuclear, biological, and chemical (NBC) weapons to and/or from NK. The instability/uncertainty in this region could have serious consequences for U.S. interests. All social instruments of national power (economic, political, military, psychological, and informational) will be leveraged to gain a strategic advantage in the region while KJU increases rhetoric, threatening ROK and U.S. nuclear destruction and possible cyber attacks.

Defining the Audience

By assessing NK's CNO capabilities through open source research, the intelligence community can gain additional analytical insights into the reclusive nation's posture and intent to use cyber warfare techniques to enhance its conventional warfare capabilities.

Literature Review

NK Infrastructure

For a disconnected, technology lacking, and reclusive country such as NK, cyber warfare seems like a very odd and unlikely scenario. However, that is exactly what provides the perfect environment to conduct cyber warfare. In contrast to the cost and massive infrastructure required for conventional warfare, a cyber-attack is very cost effective, relatively simple, anonymous, and most importantly a force multiplier. To conduct a basic cyber-attack all that is needed is a computer savvy individual, a computer, and an Internet connection. Another alternative is to outsource the attack to any number of cyber criminals in the world today. So called "cyber arms dealers," have created malicious code with advanced features for under $3,500, making cyber weapons available for purchase for even the poorest countries (Technolytics, n.d.) or individuals sympathetic to NK.

Telephones. NK has very little modern infrastructure for the estimated 24.5 million people living there (Central Intelligence Agency [CIA], 2013). An eyewitness reported hand-cranked phones were still in use in 2002 (Hayes, 2005). In 2005, NK reportedly had approximately 1.1 million telephone lines; most of which were installed in government offices and state-owned enterprises. Based on estimates, this would result in less than 5 phone lines per 100 people, and the general population would have less than 10% in individual households. Concerned with "information leakage" the NK government placed restrictions on phone usage

and disconnected lines from homes that exceeded a predetermined threshold; believing the phones were being used for illegal trading activities (Noland, 2008).

Cell phones. In 2003, a number of Chinese companies began building cellphone towers along the NK border. This led to increased use of pre-paid cell phones in NK along the Chinese border (Noland, 2008). Not long afterwards, cell phones were banned in 2004 when a cell phone was thought to have set off a railway explosion aimed at killing KJI as his train passed through the area. Cell phones were again banned for 100 days to mourn the death of KJI in December 2011 (Unnikrishnan, 2012).

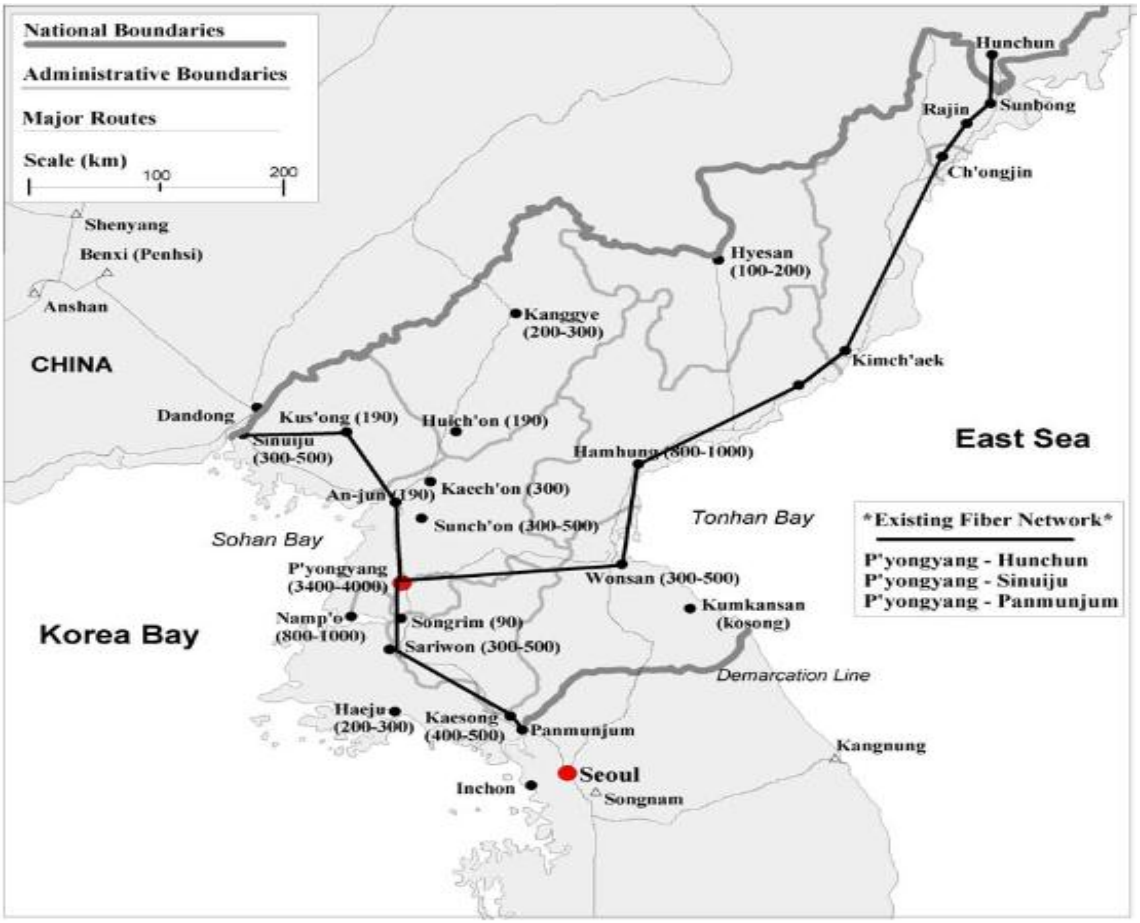
NK reportedly had 20,000 cell phones in 2004 and set a goal for mobile service throughout the country by 2007 (Lee, 2005). As of 2011, NK was ranked 155 in the world for having 1 million cellular telephones in use (CIA, 2012). With a population estimated at 24.5 million that averages to less than 4 cell phones per 100 persons.

NK has had an operational 3G cell phone network since 2009 and reports say it now covers 94% of the population yet the majority of the cell phone users are the ruling elite (Unnikrishnan, 2012). There are of course, restrictions to having a cell phone, all calls monitored, international calls and access to the Internet are banned (Martin, 2012). As of July 2011, there were approximately 1.18 million telephones and another 1 million cellular telephones in use (CIA, 2013). Appendix C shows a comparison between NK and ROK mobile telephone subscribers from 2008-2011. ROK is one of the most technologically connected countries in the world, whereas NK is one of the least connected, as evidenced in the tables.

Fiber Optic Cable. In 1990 an agreement was reached between NK and the UN Development Program (UNDP) to install 300 km of fiber optic cable between Pyongyang and Hamhung; the installation was complete in 1995 with 480 Pulse Code Modulation (PCM) lines

and six automatic exchange stations. The connection was extended to the Rason District and installed by the joint venture company, Loxley Pacific Company (Loxley). The company was owned by Thailand and the Korea Post and Telecommunications Corporation (Noland & Flake, 1997). Loxley was later allowed to operate a nationwide cellular network (Noland, 2008).

Figure 1: Existing NK Fiber Network



Source: Reproduced from: Telecommunications in North Korea: Has Orascom Made the Connection? (Noland, 2008).

In 2000, NK press reported the installation of fiber optic cable from Pyongyang to the port of Nampo, the North Pyeongan province. In March 2003, the NK's International Telecommunications Bureau created a system to send and receive emails via fiber optic cables

between Pyongyang and Beijing, China. Loxley completed the installation of 5,000 mainlines which provided capacity for 1,200 cell phones, 1,500 radio pager lines, and 80 public phones (Figure 9) (Lee, 2003). Although Loxley denies it, in 2003 it was accused of violating the restriction on the transfer of dual-use technologies for NK's enriched uranium nuclear weapons program (Lintner, 2006).

Satellite Communications. Satellite communication was made possible in 1986, when France assisted in establishing a branch of INTELSAT satellites for NK. Although NK has fixed line connections from Pyongyang to Beijing and Moscow, it relies on satellite networks for communication with Japan and the U.S. NK has been a member of the International Telecommunications Satellite Organizations since 2001 (Noland, 2008).

Intranet-Internet. Although seemingly disconnected from the rest of the world, NK possesses an extensive and well-developed Intranet to connect government offices across the country. NK began encrypting information and testing firewalls between the Intranet and Internet in 2001. This is believed to have been done in anticipation of the two networks eventually being connected, and to block hackers from the Intranet (Brown, 2004).

In May 2002, the ROK company Hoonnet, opened the first foreigners only Internet café, in Pyongyang. Then in 2003, another café was opened by ethnic Korean Chinese. Finally in 2004, NK opened an Intranet for the NK people (Noland, 2008). Use of the cafes was reportedly restricted in 2007 when it was thought to be a "threat to society" (Reuters, 2007). One of the greatest fears of NK is the threat of ideological and cultural infiltration. It is described as a type of cultural poisoning by "outsiders attempting to undermine the foundations of established communist state." NK Party lecture notes state, "The capitalist's ideological and cultural

infiltration will never cease, and the struggle against it will continue, as long as the imperialists continue to exist in the world…" (Eberstadt, 2013).

In 2007, the Internet Assigned Numbers Authority (IANA) assigned administrative control of the top level domain .kp to the Korea Computer Center (KCC), with technical operation performed by the KCC Europe, located in Germany (IANA, 2007). In 2011, Star Joint Venture (Star JV) petitioned IANA to delegate the .kp domain to the company, which IANA agreed to (IANA, 2011). The .kp domain is currently up and functioning with a limited number of websites.

NK's own Internet Service Provider (ISP) was launched in 2010 by Star JV a collaboration of NK's telecom ministry and Thailand's Loxley. Star JV reportedly handles all foreign residents in Pyongyang; while all domestic traffic was routed through the ISP, China Netcom. In April 2012, a second connection to China Netcom was announced using Intelsat; however, the majority of the network traffic still travels through China Netcom (North Korea Tech, 2012).

NK has begun to market their resources and products online with a handful of web pages. The majority of the websites are hosted on servers outside of NK by Japan, U.S., China, and Australia. Several of these sites are blocked in the ROK as determined by the ROK broadband connection. The NK hosted websites include Korea Central News Agency – NK's state-run news agency, Naenara, Air Koryo – NK's official airline, and Faster Korea – NK sports. Japan hosts nine websites which includes the Korea News Service, Korea Photo Service, and Elufa – a news video portal. The U.S. hosts at least seven websites with the majority relating to patent attorneys, trademark law, and business consultants (North Korea Tech, 2013).

NK Education. A NK defector, and former NK computer science professor, Kim Heung-kwang (Kim) graduated from Kim Chaek University of Technology (KCUT) in Pyongyang. After he completed his graduate studies in computer science, he spent 19 years teaching cyber warfare recruits at Hamheung Computer College and Hamheung Communist College. He said NK had procured more than 3,000 hackers; some were serving in NK, while others are abroad in China, Russia, and elsewhere (Yoon, 2011).

Primary – High School. Kim describes a pyramid-like structure to recruit the best and brightest students from the primary schools to attend the elite Kim Il Sung 1 and 2. Middle School and High School are combined into a six-year program. The students that graduate in the top of their class are sent to NK's top technology institutions, such as: Kim Il Sung University (Figure 13), KCUT, Pyongyang University of Computer Technology, Command Automation University (formerly Mirim University), Pyongsong Science University, Defense College, and National Academy of Sciences, and KCC. After completing university studies, they are sent abroad to either China or Russia to solidify their hacking and technical skills. When they return, they are placed in military units (Yoon, 2011).

As of 2007, Pentium 4 computers were in use at various middle and high schools for the gifted. Occasionally, specially designed computers were installed at Mirim College or KCC, as described by Jang Se-yul (Jang), a NK defector and former NK Army hacker. Jang also said the RGB would dispatch hackers undercover, posing as programmers, to China, Russia, and Europe. Their actual mission overseas was to "develop attack programs targeting their designated regions." Lastly, Jang said the attacks are never initiated from NK, because the attacks can easily be traced back to the few computer centers in NK (Yoon, 2011).

Mirim College. The name has changed over the years and is now officially named No. 144 Military Camp of the Chosun People's Army. It is known as a "secret" college or a "talented person" college because it is known to educate and train only the most talented soldiers of the People's Army. A NK defector named, "Cheong" (Cheong), claims to have served in a military base in Pyongyang and was very familiar with Mirim College and its activities (Lee & Kwon, 2011).

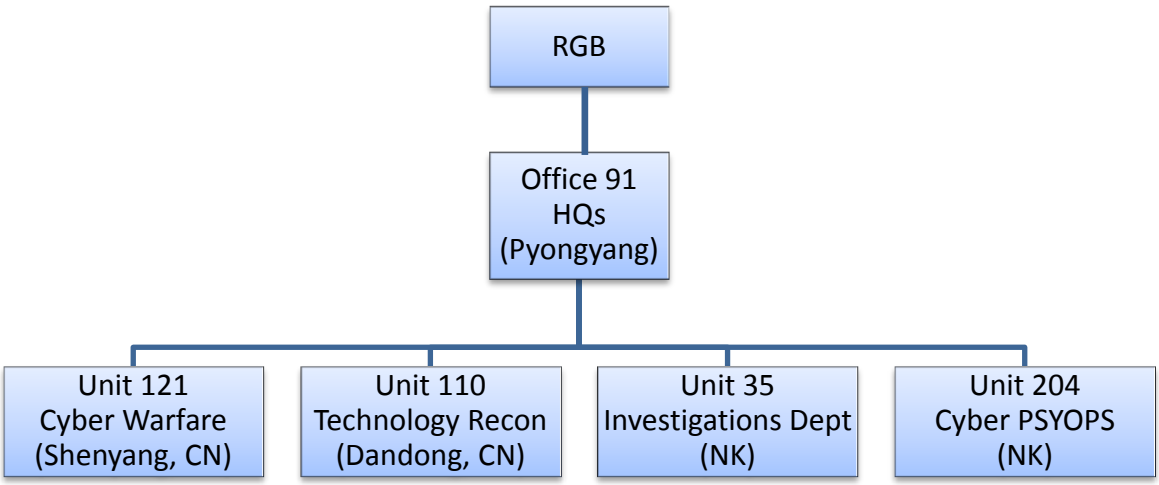
The undergraduate coursework is a five year program and the master's degree is a three year program in research. There are five professional areas of undergraduate study which include: electronic engineering, command automation, programming, technical reconnaissance, and computer science. Reportedly the command automation department teaches a class called, "South Chosun's Early Warning System and How to Respond to It" to learn offensive and defensive programming and hacking skills (Lee & Kwon, 2011). Mirim College graduates approximately100 cyber soldiers a year (Sin, 2009). The top graduating students are placed in one of the military cyber units (Lee & Kwon, 2011).

The defector, Cheong, also said the students received briefings from Soviet Union military academy professors until 1991. After that time, the students were taught by NK instructors who had studied at Frunze Military Academy in Moscow. This was short lived however, as many of the Frunze graduates were accused of espionage (Lee & Kwon, 2011).

KCC. The Center was established in 1990 and functions as an IT Company. It is thought to be the main agency carrying out the cyber-attacks against the ROK, according to a defector who had taught offensive cyber tactics in NK (Prakash, 2011). KCC is one of the top computer knowledge centers in NK and suspected of being involved in offensive cyber activities. KCC is also responsible for hosting and maintaining the Naenara website (North Korea Tech, 2012).

NK Military Cyber Units. Reporting on NK cyber units is sparse, relying on defectors for insight into the reclusive country. NK is reported to have anywhere between 300-3000 cyber soldiers. The ROK National Intelligence Service (NIS) believes NK has approximately 1,000 hackers working in the cyber units under the command of the General Reconnaissance Bureau (RGB). The RGB reports directly to the National Defense Council (NDC), the highest seat of power in NK (Vantage Point, 2011). According to defector reports, recruitment for the cyber army starts at a very young age. Children who show an aptitude for mathematics and science are placed in specialized schools and identified as potential cyber soldiers.

Figure 2: Possible NK Cyber Unit Structure



Source: Adapted from: Cyber Threat Posed by NK and China to ROK and USFK (Sin, 2009).

RGB. The RGB staff works directly for the General Staff Department of the Ministry of People's Armed Forces. The unit was created in 2009 reportedly to lead sabotage campaigns against the ROK. It is estimated to have 1,000 hackers (Korea Joongang Daily, 2012). It is responsible for collecting strategic, operational, and tactical intelligence for the Ministry of the People's Armed Forces (U.S. Library of Congress, 1993). Under the RGB, there are four suspected units of varying missions, degrees of capability, and number of personnel; they

include: Unit 121, Unit 110, Unit 35, and Unit 204. The existence of Office 91 was reported by a NK defector and may be the Headquarters element for the cyber units (Figure 3).

Office 91. According to an unnamed defector report from 2011, he was able to detail a cyber-unit named Office 91 that he had visited several times due to his relationship with cadre and traders there. The unit was located in two two-story buildings in Mangkyungdae-district of Pyongyang, NK. The buildings are 300m from the Ansan Bridge which crosses over the Botong River. In 2006, the defector said the unit consisted of a Colonel with a PhD, a Lieutenant Colonel – Party Secretary, Lieutenant Colonel – National Security Agency, and a staff of approximately 80 personnel in their 20s and 30s (Daily NK Online, 2011). The personnel had been selected from Kim Il Sung University, Chosun Computer University, and KCUT. Office 91 was affiliated with the May 18th Trading Company which would procure the equipment necessary for Office 91's work and provided the hackers with daily necessities (Daily NK Online, 2011).

Unit 121. The Korean People's Army (KPA) Joint Chiefs Cyber Warfare Unit is also known as Unit 121. This secretive unit is the largest cyber element with over 600 hackers and as reported by a defector, the best trained of all the cyber units (Clark & Knake, 2010). Reportedly it also has personnel working from the luxury, four-star Myohyang Hotel owned by the NK government, in Shenyang, China (Figure 4) (Sin, 2009). Unit 121's mission is the disruption of: the ROK's military command, control, and communications (C3) networks; dominate enemy's IT infrastructure, create social unrest, and inflict monetary damage (DefenseTech, 2007).

Unit 110. The Technology Reconnaissance Team or Unit 110 was suspected by the ROK National Intelligence Service (NIS) to be responsible for the 2009 DDoS attacks against the U.S. and the ROK. Reportedly the cyber unit is located in the Shanghai Hotel in Dangdong, just

across the NK/China border (Figure 14). Four floors are rented out to approximately 110 agents (Clarke & Knake, 2010).

Unit 35. Central Party's Investigations Department is the smallest cyber units. It handles internal security functions and external offensive cyber capabilities (Clarke & Knake, 2010).

Unit 204. Enemy Secret Department Cyber Psychological Warfare Unit has roughly 100 hackers specializing in information operations (IO) warfare (Clarke & Knake, 2010).

Figure 3: Possible Locations of NK Cyber Units

Source: Adapted from GoogleMaps.com (Google, 2013).

Import Restrictions & Funding

There are a number of sanctions and import restrictions against NK which would make it difficult to obtain the necessary technology needed for cyber warfare. In addition to the restrictions, NK is a desolate country that has faced economic and natural disasters requiring outside aid to feed its people. NK would have to develop ways to circumvent the import restrictions to fund its CNO capability.

COCOM. The Coordinating Committee for Multilateral Export Controls (COCOM) and the Wassenaar regulations place restrictions on NK importing dual-use technology. COCOM was originally signed in 1949 by the U.S. and 14 other countries after the end of World War II. In 1993, after the end of the Cold War, the U.S. Clinton administration proposed to dissolve the COCOM. The COCOM was officially dissolved March 31st, 1994, and was succeeded by the Wassenaar Arrangement in 1996 (U.S. House of Representatives, 1999).

Wassenaar Arrangement. The new organization was called the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (Wassenaar Arrangement) and was signed by 33 countries; as of January 2012 there are 41 members (Wassenaar, 2013). A core list of export controlled items is maintained; however, each member country is allowed "national discretion" to decide how they apply that list. This poses challenges for maintaining consistency across the member countries (U.S. House of Representatives, 1999).

One of the Wassenaar Arrangement objectives was to prevent states such as NK from obtaining "conventional weapons and other sensitive technologies." NK was considered a Tier-4 country which prohibited high performance computers (capable of 2,000 millions of theoretical operations per second (MTOPS) and above) from being exported there. Member nations voted to increase the level to 4,000 MTOPS; the U.S. was the only country to disapprove this change

(U.S. House of Representatives, 1999). Currently, a U.S. exporter is required to contact the U.S. Bureau of Export Administration (BXA) when exporting computers over 2,000 MTOPS. The BXA will inform the appropriate U.S. agencies, who then have 10 days to object to the shipment (Rajeswari, 2010).

Division 39. Division 39 has been described as the Achilles heel of NK because it reportedly earned over $5 billion for the Kim regime. The money is secured in overseas bank accounts in Switzerland and Macao. The secretive unit is a part of the Worker's Party created in the 1970s to fund KJI's political ambitions. Division 39 has both legitimate and illegitimate business aspects; Daesong Group is a Vienna-based bank, but also includes other businesses such as mining and seafood trade (Breen, 2012).

The illegal aspects of Division 39 include counterfeit U.S. currency, cigarettes, pharmaceuticals, and drug smuggling. NK people are often given quotas to fill and are required to send money and/or products back to Division 39 to support the regime (Breen, 2012). The group of NK hackers that ROK officials arrested in October 2011 reportedly was required to send a minimum of $500 a month back to Division 39 (Sapieha, 2011). In 2007 the U.S. State Department's Illicit Activities Initiative was prepared to indict NKs and investigate Division 39. The initiative was eventually closed for fear NK would walk away from the six-party talks regarding its quest for nuclear weapons (Breen, 2012).

According to a Japanese news agency, two Japanese nationals were indicted for allegedly exporting $108,000 worth of personal computers to KCC in NK. The 710 computers were shipped in July and December 2010 under falsified paperwork (North Korea Tech, 2012). This was in violation of Japan's trade sanctions against NK and the Wassenaar Arrangement.

Lee Soon Gi (Lee) was arrested in connection with the consignment of 1,843 computers exported to NK. Lee is the President of the Tokyo-based used PC dealer Popura-tec. There is evidence that he communicated with KCC officials and these messages "suggest the existence of a hacker unit in Pyongyang." This wasn't the first time Lee was arrested on suspicion of selling computers to NK; he was arrested in 2009 for shipping 100 computers. In total, it is estimated that he sold more than 7,200 computers to NK over the last several years (North Korea Tech, 2012).

Silibank. Silibank provides email exchange between NK and overseas. Silibank's parent organization is the Science and Technical Services (STS) of the Korea International Insurance Group which is also known as the 626 Technology Service Center. When the STS of the Korea International Insurance Group was created, it established three goals: to serve as a good example in the NK software industry; sees successful world companies as models; and the employees will be the real owners of projects (Figure 15).

Many of the employees of STS of the Korea International Insurance Group are graduates of the Pyongyang First Middle School and Kim Il Sung University – both known for producing cyber savvy individuals. The STS Group is located in an office on the fifth floor of the Chilbosan Hotel in Shenyang, China. In addition to managing Silibank, the STS Group also conducts Internet researches for NK, purchases technical books, computer hardware, and software, and then sends them to NK (North Korea Today Online, 2008).

Software Exports. Nosotek Joint Venture is a Pyongyang tech company with the motto "Secrecy. Skills. Dedication." The company acts as middleman or broker to pair up NK software designers with customers around the world. One such pairing led to the development of a mobile phone bowling application based on the American films *The Big Lebowski* and *Men in Black*.

Individuals from NK's General Federation of Science and Technology developed the game which was later published by Rupert Murdoch's News Corp and is available for download. Mr. Murdoch is the owner of the U.S. based Fox News (Campbell and Lim, 2010).

There is no reporting on how much NK makes from the software exports, it provides a means to strengthen computer programming skills, potentially lace the software with a backdoor or other malicious files, and provide funding to the Kim regime. Pak Ch'an-mo (Pak) of the P'ohang University of Science and Technology in ROK said the STS "is said to purchase some technical books from the U.S. through Amazon.com and also purchase many books from ROK and send them to NK" (North Korea Today Online, 2008).

Virtual 'Farming.' Five NK hackers were arrested in ROK for allegedly "farming" virtual gold through Massively Multiplayer Online role-playing (MMO) games for profit. The group worked out of Northern China using automated software and several unmanned computers, in a factory-like setup. After amassing large amounts of virtual gold, they would then sell the virtual gold for real cash.

Reportedly the group of 30 was required to send a minimum of $500 a month back to Division 39 in NK. The hackers were able to make an additional profit by selling the illegal MMO farming software to individuals in the ROK and China. (Sapieha, 2011). A senior officer with the International Crime Investigation Unit commenting on the attack said all the hackers had graduated from either KCC or Korea Neungnado General Trading Company (Choe, 2011). According to a ROK intelligence official, "NK's RGB has hired hackers with North Korean companies in China and mobilized them for earning foreign currency for the regime or cyber terrors against the ROK" (Korea Joongang Daily, 2012).

Computer Network Operations

The U.S. DoD defines CNO as having three subcategories: CNA, Computer Network Defense (CND), and CNE. CND is a defensive measure to protect against the offensive measures of CNA and CNE (Denning, 2007).

CNE. Cyber espionage can be described as a reconnaissance or probe of the enemy's network and systems to "collect information and identify vulnerabilities" (Wilson, 2007). Similar tools maybe used to conduct CNA and CNE, however, Wilson distinguishes between CNA and CNE tools based on their effects. CNE tools collect information, while CNA tools seek to disrupt or destroy the target system. "Not all CNE precedes attacks or even signals a future intent to attack, but CNE forms a critical first step to effective network attacks" (2007).

CNE information that is useful for CNA includes, the type of operating system (OS), hardware, software, anti-virus and security patch installation histories, IP address of connected devices, operator identities, and information on delivery of computer components to the target facility (Wilson, 2007). These details assist the attacker in customizing the attack or malware to exploit any weaknesses or vulnerabilities within the target system. CNE can also include economic espionage which is defined as:

> Foreign power-sponsored or coordinated intelligence activity directed at the U.S. government or U.S. corporations, establishments or persons, designed to obtain unlawfully or clandestinely sensitive financial, trade, or economic policy information, proprietary economic information, or critical technologies, or, to influence unlawfully or clandestinely sensitive economic policy decisions (O'Malley, 1998).

Economic espionage can be a very powerful tool used by adversaries to gain an advantage against their competitor and/or enemy. Sophisticated attackers desire quiet,

unimpeded access to the computer systems and data they take over. They must stay hidden to maintain control and gather more intelligence, or refine preparations to maximize damage (Wilson, 2005).

CNA. CNA focuses on activities to disrupt, deny, degrade, and/or destroy computer networks and the information that resides on them. This is the type of activity that most people are familiar with when discussing computer attacks or intrusions. Types of CNA include: spear phishing campaigns, DDoS attacks, intrusions, spamming, and site defacements.

DDoS attacks use a series of botnets to conduct the assault. A botnet is created by an individual that first infects other computers by sending out a virus or worm with a malicious payload. Once installed, the bot executes its payload and reaches out or beacons to the command and control server. This is usually an Internet Relay Chat (IRC) server or specific channel on an IRC network. This protocol allows for real time chat both public and private. The bot is now under the centralized command and control (C2) of the 'bot master' or 'bot herder.' The bot master can then sell the services of his bots to individuals wanting to do conduct any of the activities listed below. Once the bot master has a task i.e. spam or DDoS attack, commands will be sent to a group of bots to execute.

The advance of globalization has enabled, amplified, and accelerated threats stemming from: international terrorism, weapons of mass destruction (WMD) proliferation, failed states, and illegal drug trafficking. These threats, among others, move at increasing speeds due to technology and across geographic and organizational boundaries, blurring the distinction between foreign and domestic threats, and between strategic and tactical events Office of the Director of National Intelligence (ODNI) (ODNI, 2007).

Suspected NK Cyber Attacks

Attribution in cyber-attacks is inherently difficult to attain. Cyberspace provides a level of anonymity where cyber sleuths are able to cover and mask their tracks, leaving the victim only with suspicions of who may have committed the attack. That being said, there is very little definitive evidence which ties NK to a series of cyber-attacks against the ROK and the U.S. However, the latest attack in 2011, has a high probability of being initiated by NK, as found by the security firm McAfee. This lends credibility to the possibility of NK having a cyber-warfare capability. As has been stated previously, this type of attack would greatly benefit NK through a cost effective means of enhancing its national security strategy.

In an effort to prepare for a conventional warfare and/or harass their enemies, NK is likely to use cyber warfare to their advantage. Using CNE to conduct cyber espionage as well as testing their enemies network defenses and responses through CNA. NK can bolster their position and support by using the Internet for political propaganda. The following are a series of reported cyber-attacks which the ROK and/or the U.S suspect NK of either conducting or supporting through another nation-state or cyber criminals.

August 2004. The earliest reported attacks suspected of being initiated by NK came in 2004. Cyber attackers "tapped into 33 of 80 military wireless communications networks used by 14 different ROK units during Corps level field exercises and the ROK-U.S. combined Ulchi-Focus Lens (UFL) exercise" (Sin, 2009).

June 2005. At the Defense Information Protection Conference, Dr. Byeon Jae-jeong (Byeon) of the ROK Defense Ministry's Agency for Defense Development (ADD) warned that NK's cyber army of hackers "has the capacity equal that of the U.S. CIA." He went on to say,

"Simulation on NK's information warfare capabilities reveals that Pyongyang could damage the C2 center of U.S. PACOM, the power grid of the U.S. mainland" (The Chosun Ilbo, 2005).

July 2006. A ROK intelligence official stated that NK's Unit 121 "has hacked into the ROK and U.S. Defense Department" causing much damage, but did not elaborate further (Sidney Morning Herald, 2006).

October 2007. ROK officials made a statement accusing NK of testing a "logic bomb" on the ROK (Klingner, 2009). A logic bomb is "hidden code instructing a computer virus to perform some potentially destructive action when specific criteria are met" (Bernadette & Clemens, 2006).

July 2009. On July 4th, McAfee identified a DDoS attack against the U.S. using approximately 150,000 botnets to conduct the attack; the majority of which were located in the ROK. On July 8th, the botnet began a spam campaign with the subject "Memory of…" from the address "Independence," had the word "last" in the body of the message, and had an empty memory.rar attachment. Then on July 10th, the botnet updated itself with destructive components. It first compressed the files with a gzip algorithm, encrypted the files, and then proceeded to delete the user's files. Any attached storage devices had the first 512 bytes overwritten with a string beginning with "Memory of Independence Day." McAfee also noted the malware used a Korean character set (McAfee, 2011).

BKIS, a Vietnamese security firm, assisted in the analysis of this event and concluded there were 166,908 bots used in the attack located in 74 different countries. The top countries involved were: the ROK, U.S., China, Japan, Canada, Australia, Philippines, New Zealand, UK and Vietnam (Appendix D). Although the botnet had a high degree of sophistication, the malware was considered amateurish. The malware was based on the old virus "MyDoom" and

appeared to be a patchwork of scripts rather than custom coding. There was also evidence to suggest it was written to target Korean-language systems or the author used a Korean-language email template (Carr & Shepherd, 2010).

July 2009. A DDoS attack targeted 21 ROK government sites and 14 overseas, including the U.S. (Korea JoongAng Daily, 201) on July 7th, 2009. Investigators identified 435 different servers in 61 countries for this attack (Paganini, 2013). A Seoul military network was compromised and a computer password was stolen. The attacker was then able to exfiltrate sensitive data related to toxic-chemical manufacturers (Harlan & Nakashima, 2011). The malicious files were transferred using peer-to-peer network sharing sites (Korea JoongAng Daily, 2011).

This was likely part of the July 4th attack; however it was unknown at the time and reported separately in the ROK media. Appendix E shows the level of DDoS activity occurring on July 4th-5th; three activity spikes were identified.

November 2009. The ROK military investigated the possibility of NK obtaining OPLAN 5027, the reported ROK-U.S. strategic plan in the event of war on the Korean peninsula. An ROK military officer used an unsecure USB memory stick to download the document. The ROK Defense Ministry spokesman said the 11 page document did not contain sensitive information and was intended to brief military officials. An editorial in the ROK Chosun Ilbo newspaper noted "If NK hackers can infiltrate the South's cyber borders at will, then all those troops and weapons protecting the country along the border are useless" (McCurry, 2009).

March 2011. On March 4th, McAfee detected a DDoS attack against the ROK, targeting ROK government websites as well as the U.S. Forces Korea (USFK) network. At first glance, McAfee believed it was just another simple DDoS attack; however, upon further review, "several

things make this particular combination of targets, malware, and botnet activity different from many we've analyzed" (McAfee, 2011).

McAfee determined the attack had a clearly defined set of targets and a finite operational window that was preconfigured to 10 days. At the expiration of the 10 days, the malware would destroy the host computer, which would then require a full rebuild of the OS, applications, and data. The analysts found it unusual that the botnets in this attack were only configured to perform DDoS attacks instead of having multiple capabilities. Also a multi-tier botnet architecture was used to ensure operational resiliency and mitigate interruption (McAfee, 2011).

This architecture was sophisticated in that it ensured resiliency through the use of various name server tiers. The infected computer or bot would communicate with several first-tier C2 servers. If one of the servers was taken down, the bot would simply change to a different first-tier server. The second-tier servers were ultimately in control because they were more difficult to detect. The bots also used multiple encryption ciphers to make static analysis difficult and require the analyst to reverse engineer the malware.

McAfee found similarities with this attack and the July 2009 attack. Both attacks had the capability to compress and encrypt the files prior to deletion, although this capability was not enabled during the 2011 attack. There were a total of 14 targets that were the same across the 2009 and 2011 attacks. The March 2011 attacks took place 20 months to the day from the 2009 attacks. Based on the similarities, McAfee concluded the attacks originated from the same adversary, although who that is remains unknown.

Over 100,000 zombie computers were used in the NK attack on the Nonghyup banking system on 4 March 2011 (Korea JoongAng Daily, 2011). Email accounts of students and alumni of Korea University were accessed in the attack (Paganini, 2013). The attack targeted 40

government and corporate websites to include the ROK Defense Ministry and the presidential office (Harlan & Nakashima, 2011).

ROK Cyber Terror Response Center investigated this incident and concluded, "The origin of the attack was the same as the July 7th, 2009 attack." NK's Ministry of Posts and Telecommunications was identified as the July 2009 attacker by the ROK NIS (Korea JoongAng Daily, 2011).

At least three DDoS attacks against Incheon International Airport occurred in March 2011 (Paganini, 2012). The attacks may have been part of the overall March 4th -14th, 2011 DDoS attack against the ROK, however it is unknown.

Mr. Cho (Cho), an ROK video game distributor traveled to Shenyang, China in September 2009 to meet RGB agents posing as members of a NK trading company. Cho was allegedly aware of their identity and collaborated with them to develop malicious gaming software to be sold in the ROK. Cho purchased the software for a third of what it would have cost in ROK. (Korea JoongAng Daily, 2012).

Cho sold the software to ROK online gaming operators. The malicious software was launched when the game was played; infecting the computer and turning it into a zombie for a future DDoS attack (Korea JoongAng Daily, 2012). It is estimated that 500,000 pieces of PII were stolen and sent back to NK (Arirang News, 2012). Investigators surmise the stolen data was used by NK to target the Incheon International Airport in DDoS attacks in March 2011 (Korea JoongAng Daily, 2012).

April 2011. Banking, ATM, credit card & online transactions were affected on April 12th, 2011 in another suspected DDoS attack. McAfee said this attack had a "close resemblance" to the 2009 attack, but were more sophisticated. This attack may have been an attempt to test the

ROK response (Prakash, 2011). Nonghyup's network was reportedly hacked by NK paralyzing all of its banking and automated teller machine (ATM) services. This was considered a higher level attack which targeted the central networking system (Mok, 2012).

The Nonghyup intrusion began when a contractor accidentally downloaded a malicious program onto a laptop; providing a backdoor for the hacker to access the system at any time. Over a period of time the hacker accessed the system and placed additional malware on Nonghyup's network. Execution of the malware on April 12th, 2011 launched a DDoS attack crippling the banking network, disabling ATMs and online services for 30 million customers for several days. In the aftermath of the attack, Nonghyup spent $476 million to increase its network security by 2015. Analysts that studied the incident concluded NK was the most likely culprit. ROK prosecutors also said the attack was "staged from China, a common tactic because it allows NK hackers to avoid leaving a digital trail back to their nation (Harlan & Nakashima, 2011).

Investigators traced the activity back to NK servers used in previous attacks and one belonging to the Chinese government. They concluded the activity came from the RGB. The Seoul Central Prosecutors' Office in charge of the investigation said this attack was similar to the attacks on the ROK government and business websites in 2009 and March 2011 (Shaver, 2011).

May 2011. ROK reports NK cyber-attack paralyzed one of its largest banks (ABC, 2012). No further information was found regarding this attack.

August 2011. Five ROK hackers were arrested for creation and distribution of illegal programs. ROK police allege the group hired at least 30 NK hackers to assist hacking into an online gaming server to steal critical data (Yonhap News Agency, 2011).

September 2011. Again in September 2011 there was another "glitch" at the Incheon International Airport. A flight data processor was affected and caused a disruption with at least

18 airline departures from the airport. Police are still investigating the cause of this incident (Korea JoongAng Daily, 2012).

June 2012. On June 7th, 2012, NK reportedly conducted a cyber-attack against the JoongAng Ilbo, one of the top three ROK newspapers, selling an estimated 1.96 million copies. The actor gained access to the newspaper's administrator account and then moved laterally within the company to the production section two days later. From there the actor defaced the JoongAng Ilbo by placing a white cat grinning on the front page with the words, "Hacked by IsOne" (Paganini, 2013).

The ROK National Police Agency's Cyber Terror Response Center verified the attack came from NK by tracing one of the IP addresses used in the attack back to NK's Ministry of Posts and Telecommunications (Paganini, 2013). The IPs were based in China, but were rented by the Korea Post and Telecommunications Corp (Rahn, 2013). This same IP address had accessed the newspaper's main server repeatedly several months prior to this attack. Investigators believe that was probably an act of cyber espionage and reconnaissance (Paganini, 2013).

The National Police Agency's Cyber Terror Response Center stated,

> The first hacking attack on the server was nearly timed with the NK Army's warning on April 23rd, 2011 of provocation that a 'revolutionary force will take action soon.' It seems that the North made meticulous preparations once it singled out a particular media outlet for the cyber-attack (Paganini, 2013).

June 2012. A report by the Korean security firm AhnLab, identified a zero-day exploit designed to manipulate a vulnerability in the Korean-language word processing software. Emails contained a malicious HWP (Hangul Word Processor) attachment disguised as a government

document with various titles such as: “The Strategic Approach to North Korean Nuclear Issue,” “Agenda for Unification of North and South Korea Conference,” “Improving the Department of Defense System Engineering of XX University,” and “Technology for National Defense System.” Opening the attachment launched the malware and infected the victim’s computer. The malware would then collect the Operating System (OS) and hardware information, and record web access. After obtaining the information the malware would send the data to the command and control server (Infosecurity, 2012). This attack has not been linked to NK; however, it is interesting to note the targeting of the ROK government.

Evaluating the Threat

The 2003 U.S. Naval Postgraduate School study developed a generic methodology to assess foreign cyber threats. Four areas were used to assess a country’s CNO capabilities and intent to conduct cyber warfare: information technology industry and infrastructure, academic and research community, government and foreign relations, and hacking and cyber-attacks.

The first category, IT industry and infrastructure, assessed the country’s IT infrastructure to include access to international IT supply chains and foreign partnerships. The academic and research community focused on the higher education faculty and students of CNO studies and research, and IT skills at all educational levels.

In 2007, an independent think tank, Technolytics Institute, in conjunction with two U.S. government security management consulting organizations Intelomics and Spy-Ops, created a cyber-threat matrix (Table 5). Six potential U.S. cyber adversaries were assessed: China, Iran, Libya, NK, Russia, and Syria. To determine the threat level, the study took into account each country’s estimated military spending, level of weapon sophistication, intent, and current capabilities.

NK's estimated military spending in 2007 was $5.2 billion (Coleman, 2007). The NK military spending has steadily increased since then despite the economic crisis in the 1990s and dwindling economy in the mid-2000's (Grevatt, 2011). The Korean Institute Defense Agency's (KIDA) latest reporting indicates NK's defense budget was near $9 billion, while its gross national income was $25 billion in 2009. Based on these figures, NK spends approximately one-third of its income on its military (Reuters, 2011). The U.S. Department of Defense estimated NK's 2009 defense spending was over 22% of its Gross Domestic Product (GDP), while others estimated it to be at least 40 percent (Cordesman, 2011). Although experts disagree on NK's defense spending, it spends a considerable amount more than ROK. Comparatively, ROK spent 2.6 percent of its GDP in 2008 (Cordesman, 2011).

Table 1: Cyber Threat Matrix

Country	Estimated Military Spending	Intent	Estimated Threat	Current Capability	Basic Data Weapons	Intermediate Data Weapons	Advanced Data Weapons
China	$55.50	5.0	High	4.2	Yes	Yes	Yes
Iran	$9.70	4.0	Elevated	3.4	Yes	Limited	No
Libya	$1.30	3.0	Moderate	2.5	Yes	No	No
NK	$5.30	3.0	Elevated	2.9	Yes	Limited	No
Russia	$44.30	5.0	High	4.0	Yes	Yes	Yes
Syria	$8.50	3.0	Moderate	2.2	Yes	No	No
Estimated Military Spending is in Billions of U.S. Dollars							
Rating Scale: 1=Low, 2= Limited, 3=Moderate, 4=High, 5=Significant							

Source: Reproduced from: *Cyber Threat Posed by North Korea and China to South Korea and USFK* (Sin, 2009).

Data or cyber weapons, were categorized as basic, intermediate, and advanced. Basic data weapons could include: viruses, Trojans, DDoS attacks, brute force attacks, hacking, and cyber espionage. Cyber weapons were categorized as advanced, if they utilized advanced techniques to limit detection and increase persistence on a system, making them more difficult to identify and

destroy (Carroll, 2007). Overall, NK was assessed to have a basic cyber weapon capability; limited access to intermediate level weapons, and no advanced weapon capability. However, it was also noted that malicious code with advanced features could be purchased for as little as $3,500 thereby giving any country the potential to obtain advanced level cyber weapons (Carroll, 2007).

The last two categories were intent to use cyber weapons and current capability level. On a scale of 1 to 5, with 1 being low and 5 being significant, NK was assessed to have a 3.0 or moderate level of intent and 2.8 for current capabilities (Coleman, 2007). Although NK has not confirmed the use of cyber weapons, ROK has routinely and openly accused NK of conducting cyber-attacks against the south.

The estimated cyber threat was then calculated based on the totality of the categories. The potential cyber adversaries were given a rating of moderate, elevated, or high. As a result, NK was given an overall estimated cyber threat level of elevated (Coleman 2007).

John C. Mallery (Mallery) of the Massachusetts Institute of Technology (MIT) Computer Science & Artificial Intelligence Laboratory (CSAIL) developed a different type of cyber threat matrix (Table 2). He identified eight different categories of cyber threat actors that were either politically or financially motivated. This then influenced the type of target they were interested in, as well as the means and resources needed to achieve the targets (2011).

Using this threat matrix, NK fills a number of different cyber threat actors based on their suspected level of sophistication, intent, and objectives or targets. Cybercrime has become a lucrative business in recent years and includes small scale criminals, criminal enterprises, and black markets for cybercrime. Each of these groups is financially motivated and targets: cyber fraud, theft, IP theft, illicit content, scams, crime for hire, and hijacked resources. The resources

range from low-level to the mobilization of cybercrime networks utilizing black markets, reconnaissance, various cyber tools and exploits with extensive expert-level planning (Mallery, 2011).

Table 2: Threat Actors and Capabilities

Threat Actors	Motive	Targets	Means	Resources
Nation States During War Time	Political	Military, intelligence, infrastructure, espionage, reconnaissance, influence operations, world orders	Intelligence, military, broad private sector	Fully mobilized, multi-spectrum
Nation States During Peace Time	Political	Espionage, reconnaissance, influence operations, world orders	Intelligence, military, leverages criminal enterprises or black markets	High, multi-spectrum, variable skill sets below major cyber powers
Terrorists, Insurgents	Political	Infrastructure, extortion	Leverage black markets?	Limited, low expertise
Political Activists or Parties	Political	Political outcomes	Outsourcing?	Limited, low expertise
Black Markets For Cyber Crime	Financial	Hijacked resources, fraud, theft, IP theft, illicit content, scams, crime for hire	Tools, exploits, platforms, data, expertise, planning	Mobilizes cyber crime networks
Criminal Enterprises	Financial		Reconnaissance, planning, diverse expertise	Professional, low end multi-spectrum, leverage of black markets
Small Scale Criminals	Financial		Leverages black markets	Low, mostly reliant on black markets
Rogue Enterprises	Financial	IP theft, influence on sectoral issues	Outsourcing to criminal enterprises?	Sectorial expertise, funding, organization

Source: Reproduced from: *Straw man architecture for an international cyber data sharing system* (Mallery, 2011).

In August 2011, five suspected NK cyber criminals were arrested in ROK for an illicit gaming operation. In just over a year and a half, the group reportedly generated over $6.4 million. According to the ROK police report, the detainees were expected to send $500 a month back to Pyongyang. The ROK police also stated that they suspected "NK is mass mobilizing computer experts for hacking, and they are heavily involved in cybercrimes" (Lee, 2011).

The next category is political activists or parties. This is of course a politically motivated threat actor targeting political outcomes (Mallery, 2011). This type of activity requires low-level

expertise and could possibly be outsourced. This activity could include web defacement, DDoS attacks, and malware.

Up until this point the threat actors could be either state or non-state sponsored threat actors. The last two categories relate to nation states as threat actors either during peacetime or during conflict. Both of these actors are politically motivated and are essentially focused on the same targets, using the same means and resources. One could argue that the only difference between the two categories is the official declaration of war. Although there is an understanding of what constitutes a conventional act of war, the international community has yet to agree to on what constitutes a cyber-act of war. In this day and age the first shots fired are likely to be non-kinetic.

The Sandia National Laboratories (SNL) created a generic threat matrix to characterize and differentiate operational threats (Table 3). Being able to accurately and consistently measure threats leads to a better understanding of the threats and thereby improving analysis. SNL's Operational Threat Assessment (OTA) methodology uses the generic threat profile. The goal of this matrix is to fully describe the threat without assigning a specific label to it. SNL found that by applying a label to a threat, it also attached preconceived notions about the threat i.e. hackers, hacktivists, or script kiddies. This also provided common terminology to identify potential attack vectors and possible mitigation methods against the attacks.

The profile is based on two main threat categories; commitment and resources. Combined, these two attributes assist analysts in understanding the threat's willingness and ability to engage in cyber warfare. Commitment is defined by the level of intensity, stealth, and time. The resources category consists of technical personnel, knowledge of cyber or kinetic warfare, and access. The threat level ranges from 1 to 8, with 1 being the most capable of

achieving the goal and 8 being the least capable. SNL points out that level 8 may be able to achieve the same effects; however techniques used could be more vulnerable to detection and destruction than a level 1 threat actor.

Table 3: Threat Profile

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	KNOWLEDGE		ACCESS
					CYBER	KINETIC	
1	H	H	Years to Decades	Hundreds	H	H	H
2	H	H	Years to Decades	Tens of Tens	M	H	M
3	H	H	Months to Years	Tens of Tens	H	M	M
4	M	H	Weeks to Months	Tens	H	M	M
5	H	M	Weeks to Months	Tens	M	M	M
6	M	M	Weeks to Months	Ones	M	M	L
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L

Source: Reproduced from: *Generic Threat Matrices* (SNL, 2009)

Discussion of the Findings

The purpose of this research was to assess the NK cyber capabilities, vulnerabilities, limitations, organization, and desired end state. This threat assessment reviewed open source information and reporting to identify income sources, state and non-state support, education and training, and infrastructure to conduct CNO. The impact of an NK CNO capability would change NK military tactics and its national security strategy. Similarly, it would also change the U.S.' strategic military strategy on the Korean peninsula, but could also impact the U.S. mainland and critical resources.

NK's communication infrastructure was the first area reviewed and assessed. Without the proper infrastructure there would be little possibility of NK being able to conduct CNO from within NK; it would either have to outsource the CNO activity, or conduct the attacks from another country. Assessing the various forms of communication systems within NK also indicates how advanced NK is technologically.

The CIA reported there were approximately 1.1 million telephone lines and an additional 1 million cell phones for a population of 24.5 million people. That results in less than four cell phones per 100 people. Unnikrishnan also reported NK has had an operational 3G cellular network since 2009, yet the majority of the cell phone users were the ruling elite. Pyongyang is the center of the Kim regime and as such, is likely to be the where the majority of the telephones and cell phones are concentrated. Communication across the country is important for the regime to maintain control and keep the country in order. Martin noted that phone calls and usage were monitored; while Noland also reported that the NK government disconnected phones when it believed people were using telephones for illegal trading activities.

The Kim regime is overly paranoid about the possibility of losing control and therefore feels the need to monitor phone conversations and usage. The NK government views an increase in telephonic activity as an indicator of illegal activity occurring and its people are attempting to circumvent the government. By restricting who has access to phones, the NK government is able to control the population and the flow of information into and out of the country. The Kim regime feeds its people only the information that supports the NK government and their way of life. Without the influence of social media, NK has so far prevented a revolutionary revolt by its people.

Noland conducted an extensive study in 2008 regarding the telecommunications within in NK. He found that the UNDP had installed 300 km of fiber optic cable and the Loxley Pacific company had completed 5,000 mainlines. Noland also reported that NK has fiber optic cable connecting Pyongyang to its military units on the ROK border, the main sea port in Nampo, and to two Chinese towns on the NK/China border, Hunchun and Dandong. His reporting also indicated that Pyongyang was connected to Beijing and Moscow via fiber optic cable. It is not surprising that NK would be directly connected to its only two allies in the region.

Fiber optic cable provides robust, high-speed communication that can easily be hidden or disguised from other intelligence collection platforms. That being said, a fiber optic network provides an interesting challenge to understanding how it impacts NK's technological ability and infrastructure. There is no real way to know the full extent of NK's fiber optic network other than what has been reported. Although Noland does not mention the vast tunneling network in NK, it could allow NK to conceal the expansion of their fiber optic network.

Noland reported on the fiber optic connection between Pyongyang and the two Chinese border cities Dandong and Hunchun. Of note, the ROK NIS suspects Dandong is the location of one of NK's military cyber units accused of attacking ROK and U.S. targets in 2009. The possibility of having a NK cyber unit in China provides an additional layer for CNO attribution anonymity.

NK expanded its communication network from telephones, to cellphones, and fiber optic cable to the Intranet and Internet. Noland noted the first Internet café was opened to foreigners in 2002, and was eventually expanded to the local population in 2004. Connectivity for the NK people was short lived however, as the NK government once again saw the connection to the outside world as a threat to its society. NK's continuous struggle against the imperialists was

noted by Eberstadt. The Internet provided a means for the imperialists to infiltrate and corrupt the NK ideology. NK is in a constant battle to keep the outside world at bay, even to the detriment of its own people.

Without constant monitoring by the NK government, the Internet could be a potential instigator for public unrest. North Korea Tech identified several different NK websites hosted on their own .kp domain. It is interesting to note, as much as NK wants to keep out the imperialists, it is now trying to market NK goods and services to the outside world through the Internet. The websites maintained by the NK government were noted to be very basic and not of technologically advanced.

Overall, the NK communication infrastructure has the potential to be used for CNO activities. NK maintains its own top-level domain, a handful of basic websites, and has a fiber optic Internet connection to Beijing. This connection is important because it provides high speed communication, it is difficult for outside intelligence agencies to monitor, and it provides a means to conduct CNO.

The educational system and training was also examined to determine if computer science was being taught and if so, the level of sophistication, and areas of concentration. The general NK population does not have the ability to access computers or the Internet to educate themselves on CNO activities; therefore the NK government would need to specifically focus on educating CNO operators.

The educational system and training was reported on by a number of different defectors. There appears to be a consensus across the reporting on the structure of the educational system and teaching of computer science. The defectors discussed how young students who excelled in math and science were identified as exceptional students and tracked for advanced studies.

However, what was left unknown was how the NK educational system compares to the ROK or the rest of the world.

There are several issues with the NK defectors' reporting. Firstly, although the defector Kim reportedly graduated from KCUT and spent 19 years teaching cyber warfare, he does not provide much detail on the location of overseas training other than in China, Russia, and "elsewhere." Given his direct level of access to the cyber warfare recruits, one would expect him to have more information regarding the locations and type of overseas training they were receiving.

Secondly, there is an issue with the understanding of cyber terminology and interview translations. Kim states NK had procured more than 3,000 "hackers" serving around the world. "Hackers" could be a general term for anyone that worked with computers or it could mean the individuals that are conducting CNO attacks. It would be reasonable to believe it was the former, thereby accounting for the high number of cyber warfare soldiers reported by Kim. However, with Kim's background in cyber warfare one would expect that he would know and understand the CNO terminology. Additionally, it is unknown how the information was conveyed or translated during the interview.

And finally, the limited amount of corroborated reporting by the defectors. Another defector, Jang, did corroborate Kim's reporting of NK hackers serving around the world. He further elaborated stating that they were dispatched as programmers with the mission to learn about their target country. However, there was no other reporting to corroborate Jang's other claim that cyber-attacks did not originate from NK. It is possible the attacks are originating from NK; however it seems unlikely that NK's CNO capabilities would be sophisticated enough to not leave evidence linking the attack back to NK.

Another defector Cheong claimed he had knowledge of the secretive Mirim College and its students being taught by Russian professors until 1991. The topic taught by the Russian professors was not identified in the reporting, however it was implied that it was CNO related. This does not coincide with the reporting of KJI studying the U.S and U.K successes from the 2003 Gulf War. KJI made the statements about the importance of asymmetrical warfare against a technological advanced enemy, and from that point forward KJI supposedly focused on cyber warfare. Although Russian professors may have taught at Mirim College, the true nature of their teachings is unknown.

Computer science is most likely being taught to NK students. The level of the training is unknown; however, it would be reasonable to believe the students would have enough training to be able to conduct simple CNA or CNE activities, such as DDoS attacks and open source reconnaissance of a target. Although uncorroborated, foreign instructors could increase the level of CNO sophistication.

In 2011, KJI said cyber troops were his pride and audacity, yet there was not a lot of additional reporting of him discussing the ability. CNO is a logical and economically wise choice for NK to pursue; it would enhance NK's potential to be a threat to the U.S. and the Korean peninsula. In contrast to the cost of conventional and nuclear weapons, CNO provides a more cost effective option and still challenges the U.S.' military superiority.

Although KJI spoke of cyber units on occasion and the ROK accused NK of cyber-attacks, little other information exists on the sophistication and composition of the units. The detailing of the military units relied heavily on debriefing defectors that had knowledge of the units and their activities. Each of the units was described by a single source, which could not be verified or validated. Some of the units were reported on by several different news agencies or

authors, however there is the potential for circular reporting, which gives the appearance of having multiple sources when there is really one. This may have been an intentional technique used by NK to cause confusion and misperception regarding the capability.

Unit 121 was reported to be the largest, best trained, and most secretive NK cyber unit. Yet, the number of personnel, the unit mission, and specifics about a specialized unit of "elite" hackers operating out of a four-star hotel in China is publically known. Office 91 was identified as the potential headquarters element of NK's cyber units. The defector provided details about the unit in 2011; however, the last time he was at the unit was in 2006. The timeframe of his initial debriefing is unknown; however, five years between events may have affected the accuracy of his reporting.

As mentioned previously, the total number of NK cyber soldiers is questionable as well. Using Clarke's and Sin's reported personnel numbers: Office 91 has ~85 personnel, Unit 121 has over 600 personnel, Unit 110 has another 110 personnel, Unit 204 has ~100, and Unit 35, the smallest has less than 100. In total, that is less than 1,000 hackers, yet sources have reported a total strength between 500-3000 hackers. Units may have been misidentified; there may have been duplication of reporting; and unit number may have been inflated or misjudged by the source. If NK is producing 100 cyber soldiers a year and has been doing so for the past several years, there should be over 1,000 cyber soldiers. The forensic evidence to support the existence of a 1,000+ CNO element, operating for years from NK does not exist.

The understanding of the number and experience level of the NK military cyber elements remains limited. This is evidenced by the vast disparity in the estimated number of personnel (300-3000) conducting CNO, the makeup of the units and their location. The reporting is either based on defector estimates and/or ROK NIS speculation. There is also the possibility of the

ROK government inflating the suspected NK unit strength to warrant continued support from the U.S. military forces.

The Wassenaar Arrangement placed a number of restrictions on NK, limiting the NK's access to dual-use technologies. High capacity computers were one of the items prohibited by the Wassenaar Arrangement, yet there are reports of a Japanese man being arrested for providing several thousand computers to NK. The author does not believe this was an isolated incident and given NK's ability to procure and utilize other banned items, there is a high probability of CNO type equipment within the country.

Funding a cyber military would certainly be more cost effective than a conventional military force. Breen discussed Division 39 as being NK's Achilles' heel because of the amount of money it had raised for the Kim regime, as well as the legal and illegal businesses tied to it. The U.S. government had intended on investigating some of its activities; however, it was discontinued for fear of NK walking away from the six-party talks.

Other funding for the Kim regime is raised through front companies such as Silibank, software exports, and virtual farming. As reported by North Korea Today, Silibank is located in the same hotel in Shenyang, China as NK's cyber element, Unit 121. The company also purchased technical computer books and Internet searches for NK.

Campbell and Lin reported on the sale of computer software designed by NK. There is no reporting on how much NK made from the sale, however it provides another means to provide funds back to the Kim regime. Software sales also provide a means to distribute malicious files which would provide a backdoor into victim systems for further CNO activities.

Sapieha and the Korea Joongang Daily both reported on a group of cyber criminals that had developed software to "farm" virtual gold through an MMO game for profit. The virtual gold

would be sold for real currency. As reported, this was a collaborative effort between NK and China; with a factory-like set up in northern China. This was a very profitable endeavor for both the individuals and the Kim regime.

Attribution is extremely difficult with cyber-attacks. There were a number of attacks on both the U.S. and ROK since 2006. Although the origin of the attacks was not definitively identified, both the U.S. and the ROK accused NK. The types of targets, the use of Korean language template or email, the hodgepodge of scripting, does suggest it was executed by someone with a moderate level of CNO capability. The likely culprit is NK.

Then after the July 2009 DDoS attacks against the U.S. and ROK, McAfee conducted a study to determine the origin of the attacks. McAfee's assessment was based on the types of targets, the use of a Korean language template or email, and the hodgepodge style of scripting. The results were inconclusive; however, the activity suggests it was executed by someone with a moderate level of CNO capability. The likely culprit is NK. Until this report was published, there was no forensic evidence linking the numerous cyber-attacks back to NK; it was all just speculation.

Using the McAfee report as a baseline to assess NK's overall cyber capability would be a stretch; however, it does provide some insight into the type of activity and level of sophistication. McAfee noted the scripting was not fluid, but appeared to be a hodgepodge of different scripts combined. There was also a sophistication discrepancy between the DDoS attack itself, and the C2 architecture. It was a very simplistic attack, yet the C2 had built in redundancy to prolong the attack and was fairly robust. This may suggest different entities working on the same project with different levels of proficiency. Or as McAfee suggested, it was an attempt to test the ROK and U.S. responses to the attacks.

After reviewing information on the various infrastructure sections, education, and attacks, threat matrices can be useful in assessing the overall threat capability of a country. Sin used the cyber threat matrix, which focused on the estimated military spending was an interesting angle. According to Sin's matrix, the NK government spends a large portion of its GDP budget on the military. This budget would allow NK to either fund their own CNO capability, pay a "cyber arms dealer" to obtain malware, or pay another state or non-state actor to conduct the attacks for them. This matrix was from 2009 and rated NK's intent a 3.0 on a 5.0 scale. Today, based on current events and the change in leadership, NK's intent should be rated at a 4.0. This however, would still give NK an estimated threat level of Elevated.

Mallery's threat actors and capabilities matrix broke the threat down into two different motives – political and financial. It was interesting to see that there was not a lot of difference between the targets of a nation state during peace time or war time. So what is the difference? What is considered an act of war? The matrix did not address the possibility of nation states leveraging criminal enterprises, rogue enterprises, or political activists to achieve their desired end state; nation states and non-state actors were viewed as two distinct entities.

The threat profile provided by SNL focused on commitment and resources. For NK and based on the research, it would be assessed to be a moderate cyber level threat 2. NK would be assessed to have a moderate level of intensity, a high level of stealth, years to decades of time, tens of ten for personnel, moderate cyber knowledge and moderate access. Another key piece to this matrix would be the leadership and the likelihood of using the capability. JKU is proving to be a wildcard with little to lose.

The research was limited in several ways. NK is a reclusive and paranoid country; afraid of information leaking into and out of the country. As such, the rest of the world knows very

little about the true status of the country. The information that is available is singular in nature. It is unknown if the sources were vetted and/or validated. We are left with only the source's accounts of what they saw, experienced, or even possibly were told to say regarding the conditions within NK. Information may have been lost or misinterpreted during translation. The technical terms used when discussing CNO may be very unfamiliar to some sources. The source may have misinterpreted an electronic warfare military unit for a cyber-hacking unit.

Attribution is difficult to determine in CNO. It is also difficult to determine if it is a state or non-state actor committing the cyber-attacks. Cyberspace has no boundaries. An individual with access to a computer is able to launch an attack against anyone from almost anywhere in the world. It is difficult to tie that one act back to an individual, let alone back to a specific state which endorsed the attack. Support (education, supplies, training, etc.) from other countries not only would increase NK's overall capability, it also makes attribution more difficult.

There are also different anonymizers and tools available to hide or disguise your activity on the Internet. The botnet architecture sophistication in the 2009 attack used C2 server's located in 61 different countries. Although the ROK has publically announced their suspicions of NK conducting several of the attacks against the U.S. and ROK, the forensic evidence is not there to support it. In the case of the 2011 attack, the attack was either based off a Korean email template or was targeting Korean emails; that does not automatically implicate NK in the attack.

Without definitive proof that NK conducted the attacks, it is difficult to fully assess NK's level of CNO sophistication. In any event, NK will likely use the ROK's accusations to their advantage; counter the ROK statement stating the "Capitalists are out to get them," and/or not acknowledge the situation and let the ROK and U.S. believe NK has a powerful CNO capability that could wreak havoc on the ROK's critical infrastructure. It is almost a win-win situation for

NK. NK does not have to have a real CNO capability because anytime the ROK is attacked, they automatically blame NK.

There is also the aspect of the ROK government and what they want out of the situation. The U.S. has over 13,000 troops stationed in the ROK and by adamantly accusing NK of the attacks; the ROK knows the U.S. will protect its troops. The U.S. feels it has an obligation to the ROK as long as NK is a threat. Obviously with NK's recent nuclear tests, it remains a threat, and adding a CNO capability would make that an even greater threat to the ROK and the U.S.

Recommendations and Conclusions

Recommendations for Future Research

Defending the U.S. homeland is a strategic national interest and in 2009 U.S. President Obama expanded that definition to include cybersecurity. Every day cybersecurity is becoming more complex and critical, overlapping with private and public sectors. U.S. CYBERCOM and the Department of Homeland Security (DHS) are responsible for securing .mil and.gov domains respectively, yet our critical infrastructure remains vulnerable to attacks. "Companies regularly have absorbed losses incurred by security breaches rather than reveal weaknesses in cyber security systems, all in the name of protecting reputations and shareholder values" (Etzioni, 2011).

The U.S.' reliance on technology makes it one of the most vulnerable to cyber warfare. Cyber warfare is inherently asymmetrical; it has no boundaries, attribution is difficult, and the advances in technology have changed how we fight. Combining the asymmetrical effects of cyberattacks with conventional warfare can be a force multiplier; targeting critical infrastructure, public services, and communication systems. A review of critical infrastructures should be conducted to identify those areas most vulnerable to cyber-attacks. A partnership between the

U.S. government and the public and private sectors is needed to protect U.S. vital interests and assets. The private sector has the network security expertise and ultimately is the one to develop security mechanisms to protect U.S. systems. Additionally, U.S. Cleared Defense Contractors (CDC) and subcontractors should be mandated to report intrusions, as sensitive information may have been compromised in an attack.

In 2011, the Obama administration proposed combining "security infrastructure" that would include public and private sectors (2011). Addressing the public and private sector vulnerabilities is critical in defending the U.S. from cyber-attacks. As demonstrated by the suspected NK CNO attacks against the ROK and U.S., a simple DDoS attack can wreak havoc with the public and cause them to lose faith in their government. Overall, attacks against the government sectors are targeting the much more vulnerable private and public sectors.

Further research should be conducted on the evolving NK cyber threat by obtaining technical data from the various incident response centers. This data can confirm the where the attack originated from, provide insight into the level of sophistication, and possibly confirm the presence of a NK cyber warfare unit. Based on the research, NK currently has a basic to moderate CNO capability. Once NK obtains nuclear weapons, we could expect KJU to increase his efforts to develop a viable CNO capability. While he is pursuing that goal however, NK will continue to develop and incorporate CNO activities into the overall NK strategic military strategy.

Cyber warfare is a logical choice for NK given its limited financial resources. "NK employs sophisticated computer hackers trained to launch cyber infiltration and cyberattacks against the ROK and U.S." (Thurman, 2012). The lack of attribution provides another incentive for the attacks. KJU will seek advantages that will support his national strategic goals of regime

sustainment and economic survivability. KJU's priority is obtaining nuclear weapons; however, he will also continue to pursue a CNO capability. Based on recent events, NK is close to obtaining a nuclear warhead. Once they have a nuclear weapon, the pursuit of obtaining a capable CNO capability will have a much higher priority.

Additional areas for future research are defector reports, outside support, incident analysis, and funding. Defectors are the only ones able to provide firsthand accounts of activities within NK. As much as possible their reporting should be validated and deconflicted to provide a more accurate picture of NK cyber activities. It is unlikely NK is pursuing a CNO capability completely on its own; it is likely using alliances with China for technical support, educational materials, instructors, equipment, malicious software, and infrastructure. NK is connected to China via fiber optic cable and reportedly has at least one cyber unit located in China, this leads one to believe that China is providing support either wittingly or at least turning a blind eye to what NK is doing. Additional research should be focused on this unique relationship to determine if NK is acting on its own, and/or China's level of involvement. As noted in the research, an individual was arrested for attempting to sell restricted items to NK. It is unlikely this was a onetime event and there may be others currently selling technology and restricted items to NK. By focusing on this area, one could get a better understanding of the type and quantity of equipment NK has to conduct CNO activities.

Funding is another area of interest requiring additional research. Although CNO is relatively cheap compared to conventional military weapons, it still requires funding. This research would coincide with obtaining the technical attribution information. It would assist in determining who is conducting the attacks – possibly an outside source was hired to conduct CNO activities on NK's behalf, or even a NK sympathizer acting on their own. Analysis of the

malicious software used in attacks could identify the originator, determine if NK is developing their own malware, incorporating open source malware, or working with a third party to develop customized malware. All of these areas will assist in developing a more thorough threat picture.

Research Limitations

This research was limited in several ways. NK is a reclusive and paranoid country; afraid of information leaking into and out of the country. As such, the outside world does not know the real status or conditions within NK. The majority of the information that was available was singular in nature and it was unknown if the sources were vetted and/or validated. We are left to believe the source's accounts of what they saw, experienced, or even possibly were told to say regarding the conditions within NK. Information may have been lost or misinterpreted during translation. The technical terms used when discussing CNO may be very unfamiliar to some sources. The source may have misinterpreted an electronic warfare military unit for a cyber-hacking unit.

Forensic attribution is the final key element missing from this study. Attribution is difficult to determine; any individual with access to a computer is able to launch an attack against anyone from almost anywhere in the world. It is difficult to tie one particular cyber act back to an individual, let alone back to a specific state which endorsed the attack. Although the ROK and the U.S. have suspicions attributing the attacks to NK, there is no forensic evidence linking the reported attacks back to NK.

The botnet architecture sophistication in the 2009 attack used C2 server's located in 61 different countries. Although the ROK has publically announced their suspicions of NK conducting attacks against the U.S. and ROK, the forensic evidence is not there to support it.

Although the 2011 attack was based off a Korean email template or was targeting Korean emails, does not automatically implicate NK in the attack.

Without definitive proof that NK conducted the attacks, it is difficult to fully assess NK's level of CNO capability. In any event, NK will likely use the ROK's allegations to their advantage by countering with either increased rhetoric denying the accusations or by not even acknowledging the situation. By doing so, NK allows the ROK and U.S. to believe it has a powerful CNO capability that could wreak havoc on the U.S. and ROK's critical infrastructures. It is almost a win-win situation for NK; regardless of NK's CNO capability, the ROK immediately accuses NK and NK remains relevant in the international community.

Another factor to consider is the needs of the ROK government. By attributing cyber-attacks to NK and over estimating/exaggerating the strength of the NK cyber capability, the ROK government keeps the U.S. involved on the Korean peninsula. The U.S. has over 13,000 troops stationed in the ROK and by adamantly accusing NK of the attacks; the U.S. feels obligated to protect the ROK as long as NK is a threat. Obviously with NK's recent nuclear tests, it remains a threat, and adding a CNO capability would make that an even greater threat to the ROK and the U.S.

Conclusion

Every day the world is becoming more reliant upon technology and interconnected through the Internet. This reliance has added a new dimension to the conventional battle space, known as cyberspace. The U.S. government is striving to develop a national strategy that will allow it to achieve cyberspace superiority through a combination of military information superiority and technological modernization. Government and private sector digital assets could very well be at risk with NK's advancement in CNO.

The purpose of this research was to assess the NK cyber capabilities, vulnerabilities, limitations, organization, and desired end state. This threat assessment reviewed open source reporting which identified income sources, state and non-state support, education and training, and infrastructure to conduct CNO.

NK has the minimal infrastructure necessary to conduct CNO from within NK. If the alleged attacks are attributed to NK and are used to assess the level of sophistication, NK's CNO is rated as moderate. However, the attacks were not of an elevated level of sophistication that would indicate an "elite" group of cyber warriors of the same caliber as the CIA as claimed by the ROK Defense Ministry Agency for Defense Development. Although it is reasonable to believe educational programs are in place to groom and develop potential cyber soldiers, the quality and standard of those programs are unknown. And finally, the lack of attribution favors NK. The world knows so little about NK, that there is always the possibility, however slight, that they are conducting the attacks. The attacks do not need to be overly complex as a simple DDoS attack against critical infrastructure can cause a lot of chaos.

KJU and the NK regime will incorporate CNO into overall military and national security strategies. It will be used as another tool of manipulation to gain humanitarian and economic aid; bolster the NK people's sense of national pride; and use it as a bargaining chip to resume the six-party talks. NK has developed a cycle where they will cause a provocation anticipating an international reaction. This reaction will lead to negations where NK will receive some sort of humanitarian and/or economic aid. This will be followed by a slight lull in activity until NK again needs or wants something from the U.S. The ultimate end state for NK is to be recognized as a nuclear power; at which time KJU believes he has the right to negotiate one on one with the U.S. Adding a CNO capability would provide an additional layer of protection from the outside

world and counter the U.S.' military power. NK has nothing to lose in a cyber confrontation; it is not technologically dependent like the U.S.

It does not take a lot of sophistication to conduct a DDoS attack, especially against unprotected critical infrastructure, to cause havoc, or for people to lose faith in their government's ability to protect them. If the attacks against the Incheon International Airport or the banking industry were conducted by NK, it created a lot of chaos in the ROK. People were unable to access their bank accounts for almost a week and panic quickly ensued. Add to the chaos the GPS jamming at the Incheon International airport. Those are simple attacks which can have a large psychological impact on the population.

Undoubtedly NK is not as technologically advanced as, or connected to, the rest of the world. Information and knowledge are power. The Kim regime is highly concerned about "information leakage" into and out of NK. Information leaking out of NK could alert the rest of the world of the true conditions within NK, causing the regime to collapse. Information leaking into NK about the real world could also cause an internal uprising that would also overthrow the government.

Continued attacks against the ROK, U.S. mainland, and USFK forces on the Korean peninsula will cause the U.S. government to react. The U.S. will have to reassess its level of protection provided to the ROK, as well as a reassessment of network and physical security within U.S. networks and between U.S. and ROK networks. There are serious concerns if NK is able to gain access to U.S.-ROK strategic war plans. The attacks previously identified, demonstrated an overall weakness of the private sector's ability to protect critical infrastructure.

There are three different possible scenarios or hypothesis based on the research material. The first is the best case scenario in which NK does not have a CNO capability at all. The

suspected attacks were conducted by another unknown entity and the ROK used the allegations to maintain support from the U.S. and condemn NK. Although NK has some infrastructure to support the capability, it is rudimentary and inconsistent. Nevertheless, NK will continue to develop the CNO capability, but the majority of its attention is focused on obtaining a nuclear weapon.

NK having a viable CNO capability without the assistance of outside sources is the worst case scenario. NK could conduct CNO the U.S. and ROK without the fear of retaliation because it is not as technologically connected as the rest of the world. The U.S. would have to either rely on sanctions or declare NK's actions an act of war. The sanctions to date have had little effect on influencing NK's actions. It is unlikely the U.S. would pursue military action against NK, but would again send NK a strongly worded response.

The most likely scenario is that NK has a basic to moderate level of CNO sophistication; however lacks the technology and experience to be a lethal cyber threat on its own. NK therefore relies on outside sources and support for funding, equipment, training, and implementation. If defector reports are true and NK cyber elements are located in Shenyang and Dandong, China, it is highly unlikely that it is without China's knowledge. This scenario increases the difficulty of assigning attribution to the attacks allowing NK to claim plausible deniability, increases the sophistication and lethality of the attacks, and essentially uses NK as a proxy to conduct CNO against the U.S.

References

ABC Asia Pacific News. (2012, June 7). South Korean military accuses north of cyber warfare. Retrieved August 27, 2012 from http://abcasiapacificnews.com/stories/201206 /3520592. htm?desktop

Adams, J. (2001, May/June). Virtual defense: The weakness of a superpower. *Foreign Affairs*. Retrieved February 13, 2013 from http://www.foreignaffairs.com/print/57037

Arirang News. (2012, June 4). N. Korea's game software turns many pc's into zombie pc's. Retrieved August 27, 2012 from http://www.arirang.co.kr/News?News_Print.asp?type =news&nseq=130965

BBC News. (2012, December 18). North Korea satellite 'tumbling in space'. BBC News. Retrieved February 16, 2013 from www.bbc.co.uk/news/world-asia-20769324

Bernadette, S., & Clemens, M. (2006). *Webster's new world ® hacker dictionary*. Indianapolis: Wiley Publishing, Inc.

Breen, M. (2012). Kim Jong-Il: North Korea's dear leader who he is, what he wants, what to do about him. Singapore. John Wiley & Sons. Singapore Pte Ltd.

Carr, J., & Shepherd, L. (2010). *Inside cyber warfare, mapping the cyber underworld*. O'Reilly MediaCarr, J., & Shepherd, L. (2010). Responding to international cyber attacks as acts of war. In M. Loukides, *Cyber Warfare* (pp. 45-75). Sebastopol, California: O'Reilly Media, Inc.

Carroll, W. (2007, December 17). Cyber threat matrix. Defense Tech. Retrieved February 14, 2013 from http://defensetech.org/2007/12/17/cyber-threat-matrix/

Cartwright, J. (2007). Gen James Cartwright, USMC, statement before the strategic forces subcommittee, senate armed services committee, 28 march 2007, 4-5

Choe, S.H. (2011, August 4). Seoul warns of latest North Korean threat: An army of online gaming hackers. Retrieved August 27, 2012 from http://www.nytimes.com/2011/08/05/world/asia/05korea.html?_r=r1&pagewanted=print

Chosun Ilbo. (2013, February 5). N. Korean nuclear test keeps outside world guessing. *Chosun Ilbo*. Retrieved February 9, 2013 from http://english.chosun.com/site/data/html_dir/2013/02/05/2013020500613.html

Clarke, R. A., & Knake, R. (2012). *Cyber war, the next threat to national security and what to do about it*. New York N.Y.: Ecco.

Coleman, K.G. (October 2007). World war iii: A cyber war has begun. Retrieved February 14, 2013 from http://www.scribd.com/doc/915267/Cyber-War-Released

Coleman, K.G. (October 2007). World war iii: A cyber war has begun. Retrieved February 14, 2013 from http:// www. scribd.com/doc/915267/Cyber-War-Released

Cordesman, A.H. (15 February 2011). The Korean military balance: Comparative Korean forces and the forces of key neighboring states. Center for Strategic & International Studies. Retrieved February 14, 2013 from http://csis.org/files/publication/110201_Korea MilitaryBalanceMainRpt.pdf

Daily NK Online. (2011, June 01). No. 91 'hackers hq' revealed. *Daily NK Online*. Retrieved February 13, 2013 from http://www.dailynk.com/english/read.php?cataId=nk00100&num=7772

Damballa. (n.d.). Advanced persistent threats (apt). Retrieved February 3, 2013 from http://www.damballa.com/knowledge/advanced-persistent-threats.php

DefenseTech (2007). Inside dprk's unit 121. Retrieved August 27, 2012 from http://defensetech.Org/2007/12/24/inside-dprks-unit-121/

Denning, D. E. (2007). Assessing the computer network operations threat of foreign countries. In J. Arguilla & D. Borer (Eds.), *Information strategy and warfare: A guide to theory and practice.* New York: Routledge.

Eberstadt, N. (2013). Western aid: The missing link for North Korea's economic revival. In K. Park & S. Snyder (Eds.), *North Korea in Transition.* Plymouth: Rowman & Littlefield Publishers, Inc. Economist, The. (2012, March 1). North Korean nuclear progress: Leap of faith. Retrieved February 13, 2013 from http://www.economist.com/blogs/banyan/2012/03/north-korean-nuclear-progress

Economist, The. (2013, February 16). North Korea's nuclear test: Fallout. Retrieved February 16, 2013 from http://www.economist.com/news/asia/21571938-chagrin-his-neighbours-young-despot-appears-determined-continue-his-familys-atomic

Eroraha, I. (2010). *Netsecurity.com.* Retrieved February 3, 2013 from http://netsecurity.com/marketing/ NetSecurity_ComputerForensicsShow_2010_Keynote_Real-World_Computer_Forensics_Challenges_Facing_Cyber_Investigators_041920.pdf

Etzioni, A. (2011). Cybersecurity in the private sector. Retrieved March 7, 2013 from http://icps.gwu.edu/files/2011/10/cyber.pdf

Gannon, J. (2010). The transformed global threat environment. *Yale Journal of International Affairs, 5*(2). Retrieved August 30, 2012 from http://yalejournal.org/2010/07/the-transformed-global-threat-environment/

George, R. (2008). The art of strategy and intelligence. In R. J. Heuer, & R. Z. George, *Pyschology of intelligence analysis* (pp. 107-110). Washington: Georgetown University Press.

Grevatt, J. (20 Jan 2011) Analysts reveal ‘real’ North Korea 2009 defence budget. Janes. Retrieved February 14, 2013 from http://www.janes.com/products/janes/defence-security-report.aspx?id=1065928818

H-Security. (2012, August 31). South Korea to upgrade its cyber defence. Retrieved September 4, 2012 from http://www.h-online.com/security/news/item/South-Korea-to-upgrade-its-cyber-defence-1696592.html

Harlan, C. & Nakashima, E. (2011, August 29). Suspected North Korean cyberattack on a bank raises fears for S. Korea, allies. Washington Post. Retrieved August 29, 2011 from http://www.washingtonpost.com/world/national-security/suspected-north-korean-cyber-attack-on-a-bank-raises-fears-for-s-korea-allies/2011/08/07/gIQAvWwIoJ_story_1.html

Hayes, P. (2005) DPRK information strategy: Does it exist? In A. Mansourov. (Ed.), *Bytes and Bullets.* Honolulu: Asia-Pacific Center for Security Studies.

Hess, K. M., Orthmann, C. H., & Cho, H. L. (2011). *Introduction to law enforcement and criminal justice* (10 ed.). New York, NY: Demar Publication. Retrieved February 3, 2013 from http://books.google.com/books?id=aCGtxnozpqkC&pg=PA382&dq=leveraging+inferior+tactical+or+operational+strength+against+the+vulnerabilities+of+a+superior&hl=en&sa=X&ei=BiUPUZ61O8SO2AXIioGwAw&sqi=2&ved=0CDgQ6AEwAg#v=onepage&q=leveraging%20inferior%20tactica

Hofbauer, J., Hermann, P., & Raghavan, S. (Oct 2012). Asian defense spending, 2000-2011. Report of the CSIS defense-industrial initiatives group. Retrieved February 14, 2013 from http://csis.org/files/publication/121005_Berteau_AsianDefenseSpending_Web.pdf

Infosecurity. (2012, July 9). Cyber threat targets South Korean government. Retrieved August 29, 2012 from http://www.infosecurity-magazine.com/view/26870/cyber-threat-targets-south-korean-government/

IANA. (2007). IANA report on the delegation of the .kp top-level domain. Retrieved February 19, 2013 from http://www.iana.org/reports/2007/kp-report-11sep2007.html

IANA. (2011). Redelegation of the .kp domain representing the democratic people's Republic of Korea to star joint venture company. Retrieved February 19, 2013 from http://www.iana. org/reports/2011/kp-report-20110401.html

Kehler, C. (2011). Opening remarks. *USSTRATCOM Deterrence Symposium 2011.* Omaha. Retrieved February 3, 2013 from http://www.stratcom.mil/speeches/ 2011/73/2011_ USSTRATCOM_Deterrence_Symosium_-_Opening_Remarks/

Klingner, B. (2009, July 08). [Web log message]. Retrieved September 17, 2012 from http:// blog. heritage.org/2009/07/08/north-korea-may-be-behind-cyber-attack-on -us-and-south-korea/

Korea Joongang Daily. (2012, June 5). Incheon airport cyberattack traced to Pyongyang. Korea JoongAng Daily. Retrieved February 18, 2013 from http://koreajoongangdaily.joinsmsn .com/ news/article/article.aspx?aid=2953940

Korea JoongAng Daily. (2011, April 7). Cyberattack last month traced to North Korea. Retrieved August 29, 2011 from http://koreajoongangdaily.joinsmsn.com/news/article/option/ article _print.aspx

Lee, H. (2005). Information technology progress in North Korea and its prospects. In A. Mansourov. (Ed.), *Bytes and Bullets.* Honolulu: Asia-Pacific Center for Security Studies.

Lee, J. (5 August 2011). Police: North Korean hackers targeted South Korean game sites. CNN. Retrieved February 14, 2013 from http://www.cnn.com/2011/WORLD/asiapcf/08/05/skorea.cyber.crime/index.html

Lee, S., & Kwon, E. (2011). A look at Mirim College, hotbed of cyber warfare. *The Daily NK*. Retrieved August 27, 2012 from http://www.dailynk.com/english/ read.php?cataId=nk02900&num=7656

Lewis, J. A. (2010, September 7). Speak loudly and carry a small stick: The North Korean cyber menace. *38 North*. Retrieved February 13, 2013 from http://38north.org/2010/09/speak-loudly-and-carry-a-small-stick-the-north-korean-cyber-menace/print/

Library of Congress (1993). A country study: North Korea. Retrieved February 22, 2013 from http://lcweb2.loc.gov/cgi-bin/query/D?cstdy:1:./temp/~frd_hxT3::

Lim, B.K. (2013, February 15). Exclusive: North Korea tells china of preparations for fresh nuclear test – source. Reuters. Retrieved February 16, 2013 from http://www.reuters.

Lind, J., (2012, April 12) Why North Korea gets away with it: Pyongyang's skillful deterrence. *Foreign Affairs*. Retrieved February 14, 2013 from http://www.foreignaffairs.com/articles/137399/jennifer-lind/why-north-korea-gets-away-with-itcom/article/2013/02/15/us-korea-north-nuclear-idUSBRE91E0J820130215

Mallery, J.C. (2011). Straw man architecture for an international cyber data sharing system. Retrieved February 14, 2013 from http://www.syssec-project.eu/media/page-media/23/bic2011-06-mallery.pdf

Martin, A. (2012, July 27). Mobile phones proliferate in North Korea. *The Wall Street Journal*. Retrieved September 4, 2012 from http://online.wsj.com/article/SB10001424052702304458604577487572176127932.html

Mandiant. (2011). Advanced persistent threat: When compromise is no longer an option. *Mandiant*. Retrieved February 3, 2013 from http://www.mandiant.com/services/advanced_persistent_threat

Masters, J. (2011, May 23). Confronting the cyber threat. *Council on Foreign Relations*. Retrieved August 30, 2012 from http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577

McCurry, J. (2009, December 18). North Korean hackers may have stolen us war plans. *The Guardian*. Retrieved August 30, 2012 from http://www.guardian.co.uk/world/2009/dec/18/north-south-korea-hackers

McMichael, W. (2010, May). DOD cyber command is officially online. *Army Times*. Retrieved September 10, 2012 from http://www.armytimes.com/news/2010/05/military_cyber_command_052110/

Miklaszewski, J. & Boyle, A. (2012, December 12). North Korean satellite 'tumbling out of control,' us officials say. NBC News. Retrieved February 16, 2013 from http://worldnews.nbcnews.com/_news/2012/12/12/15866530-north-korean-satellite-tumbling-out-of-control-us-officials-say?lite

Mok, Y.J. (2012, June 12). North incrementally ups cyber ante? Retrieved August 29, 2012 from http://www.dailynk.com/english/read_print.php?cataId=nk00400A&num=9354

Noland, M. (2008). Peterson Institute for International Economics. *Telecommunications in North Korea: Has orascom made the connection?*. Retrieved February 13, 2013 from http://www.iie.com/ publications/papers /noland1208.pdf

Noland, M., and Flake, G. (1997). Opening attempt: North Korea and the rajin-sonbong free economic trade zone. *Journal of Asian Business,* 13 (2): 99-116.

North Korea Tech (2012). Japan ties exported pcs to internet attacks. Retrieved August 29, 2012 from http://www.northkoreatech.org/2012/03/14/japan-ties-exported-pcs-to-internet-attacks/

North Korea Tech. (2012). Japan indicts two over pc exports to North Korea. Retrieved August 29, 2012 from http://www.northkoreatech.org/2012/02/02/japan-indicts-two-over-pc-exports-to-north-korea/

North Korea Tech (2012). DPRK gets second link to internet. Retrieved August 30, 2012 from http://www.northkoreatech.org/2012/04/08/dprk-gets-second-link-to-internet/

NRC. (1991). *Computers at risk: Safe computing in the information age*. Washington: National Academies Press, 1991, 7

O'Malley, E. (1998) Economic espionage act. *The Intelligencer,* Fall 1998.

Office of the Director of National Intelligence (ODNI). (2007). *United States intelligence community (IC) 100 day plan for integration and collaboration.* Retrieved August 30, 2012 from www.fas.org/irp/dni/100-day-plan.pdf

Open Source Center. (2013, February 5). Seoul resolved to respond firmly to dprk nuclear test, seeking strong international response. *Open Source Center*

Paganini, P. (2012, June 11). Concerns mount over North Korean cyber warfare capabilities. Retrieved February 13, 2013 from http://www.infosecisland.com/blogview/21577-Concerns-Mount-over-North-Korean-Cyber-Warfare-Capabilities.html

Paganini, P. (2013, January 18). Cyber warfare between Koreas, a warning for any cyber power. Retrieved on February 18, 2013 from http://securityaffairs.co/wordpress/11834/ intelligence/cyber-warfare-koreas-warning-cyber-power.html

Pellerin, C. (2011, July 14). DOD releases first strategy for operating in cyberspace. *American Forces Press Service*. Washington, DC. Retrieved September 11, 2012 from http://www.defense.gov/news/newsarticle.aspx?id=64686

Prakash, R. (2011, December 8). North Korea's cyber skirmishes. Observer Research Foundation. Retrieved August 27, 2012 from http://www.orfonline.org/cms/sites/orfonline/modules/analysis/AnalysisDetail.html?cmaid=28431&mmacmaid=28432

Rahn, K. (2013, January 01). NK behind cyber attack on newspaper. *The Korea Times*. Retrieved February 13, 2013 from http://www.koreatimes.co.kr/www/news/nation/2013/01/116_128966.html

Rajeswari, P. (2010) U.S. export control policy and Wassenaar arrangement. Retrieved February 22, 2013 from http://www.idsa-india.org/an-jun8-10.html

Reuters. (2007). Nation bans karaoke bars, internet cafes? 11 July. Retrieved February 20, 2013 from http://www.reuters.com/article/2007/07/11/us-korea-north-karaoke-idUSSEO2320620070711

Reuters. (2011). North Korea spends about a third of income on military: Group. Reuters. Retrieved August 20, 2012 from http://ca.reuters.com/article/topNews/idCATRE70H1BW20110118.

Rowe, N. (2008). Deception in defense of computer systems for cyber-attack. In L. Janczewski, & A. M. Colarik, *Cyber Warfare and Cyber Terrorism* (p. 97). Hershey, PA: Information Science Reference

Sawyer, R. D. (1994). *The Art of War.* Barnes & Noble, Inc.

Schell, B., & Martin, C. (2006). *Hacker Dictionary.* Indianapolis: Wiley Publishing, Inc.

Sin, S. (2009). *Cyber threat posed by North Korea and China to South Korea and U.S. forces korea*. Retrieved August 20, 2012 from http://www.scribd.com/doc/15078953/Cyber-Threat-Posed-by-North-Korea-and-China-to-South-Korea-and-US-Forces-Korea

Sullivan, B. (2012). Zappos says hacker may have accessed info on 24 million customers. NBC News. Retrieved February 13, 2013 from http://redtape.nbcnews.com/_news/2012/01/16/10163952-zappos-says-hacker-may-have-accessed-info-on-24-million-customers?lite

Sydney Morning Herald. (2006, July 12). N Korea operates cyber warfare unit to disrupt S Korea's military command: Official. *The Sydney morning herald*. Retrieved September 12, 2012 from http:// www.smh .com.au/news/Technology/NKorea-operates-cyber-warfare-unit-to-disrupt-SKoreas-militarycommand official/2006/07/12/1152637718059.html

Symantec. (2012, April). 2011 Trends. *Internet Security Threat Report, 17*.

Thurman, J. D. (2012). Statement of General James D. Thurman commander, United Nations command; commander, united states-republic of Korea combined forces command; and commander united states forces Korea. *House Committee on Appropriations Committee on Military Construction, Veterans Affairs, and Related Agencies.* Retrieved February 3, 2013 from http://http://appropriations.house.gov/uploadedfiles/03.29.12_milconva_commander_unc_cfc_usfk_-_general_james_d._thurman_-_testimony.pdf

Tisdall, S. (2010, February 3). Cyber warfare is 'growing threat'. *The Guardian*. Retrieved February 3, 2013 from http://www.guardian.co.uk/technology/2010/feb/03/cyber-warfare-growing-threat

U.S. House of Representatives. United States House of Representatives, Select Committee.

(1999). *U.S. national security and military/commercial concerns with the people's republic of china* (Report 105-851). Retrieved February 14, 2013 from http://www.house.gov/coxreport/cont/gncont.html

Unnikrishnan, K. (2012, January 30). North Korea to punish cellphone users as war criminals. Digital Journal. Retrieved February 17, 2013 from http://digitaljournal.com/print/article/318692

Violino, B. (2013, January 28). *InfoWorld.* Retrieved February 5, 2013 from http://www.infoworld.com/print/211438

Wang, P., Sparks, S., & Zou, C. C. (2007). *An Advanced Hybrid Peer-to-Peer Botnet.* Retrieved February 9, 2013 from http://static.usenix.org/event/hotbots 07/tech/full_papers/wang/wang_html/

Wassenaar Arrangement. (2013). Participating states. Retrieved February 22, 2013 from http://www.wassenaar.org/participants/index.html

Waugh, R. (2011, December 7). *DailyMail.co.uk.* Retrieved February 3, 2013 from http://www.dailymail.co.uk/sciencetech/article-2070690/How-worlds-cyber-super-weapon-attacked-Iran-threatens-world.html

Whittaker, Z. (2011). Cybercrime costs $338bn to global economy; more lucrative than drugs trade. *Between the Lines*.

Williams, M. (2012, October 12). *infoworld.com.* Retrieved February 5, 2013 from http://www.infoworld.com/print/204734

Wilson, C. (2005). *Computer attack and cyberterrorism: Vulnerabilities and policy issues for congress.* Washington, D.C.: Congressional Research Service, April 1, 2005, p. 37.

Wilson, C. Congressional Research Service, (2007). I*nformation operations, electronic warfare,*

and cyberwar: Capabilities and related policy issues (Order Code:RL31787)

Yonhap News Agency. (2011, August 4). Police say N. Korean hackers involved in S. Korean online crime. Retrieved February 18, 2013 from http://english.yonhapnews.co.kr/north korea /2011/08/04/0401000000AEN20110804006800315.HTML

Yonhap News Agency. (2011, August 14). Pyongyang denies suspected hacking involving north koreans. Retrieved February 18, 2013 from http://english.yonhapnews.co.kr/northkorea/ 2011/08/14/99/0401000000AEN20110814002300315F.HTML

Yonhap News Agency. (2011, August). North Korea's move toward cyber warfare. *Vantage Point*, pp. 2-5.

Yoon, Sangwan. (2011, June). North Korea recruits hackers at school. *Aljazeera.* Retrieved February 18, 2013 from http://www.aljazeera.com/indepth/features/2011/06/2011620815 43573839.html

Appendices

Appendix A – Glossary

Advanced Persistent Threat (APT): Advanced persistent threat (APT) refers to a sophisticated, organized, and prolonged attack on the "Defense Industrial Base, financial industry, manufacturing industry and research industry" (Mandiant, 2011). The APT usually has identified a specific target and designs malware to exploit trusted connections to access and compromise the targeted system. One of the key components of an APT attack is for the intrusion to remain invisible for as long as possible and maintain its remote control capability.

Back Door: A software bug or some undocumented software feature that a cracker leaves behind, after exploiting a system, to be able to reenter at a later point in time. Note, however, that back or trap doors can be a function of poor software design; that is, during its development, a programmer may have built in a software bug that was not removed when the software was put in production. The unwitting consumer who purchases the software becomes, in a sense, a target-in-waiting for a crack attack (Schell & Martin, 2006).

Bot or Robot: A remote-controlled software program that acts as an agent for a user. Bots can be doing clandestine things even when the computer owner thinks the computer is inactive. Bots are favored tool of cybercriminals because the software on the PC and the unauthorized network activity are difficult to detect (Schell & Martin, 2006).

Botnet: (ro**BOT NET**work) Also called a "zombie army," a botnet is a large number of compromised computers that are used to generate spam, relay viruses or flood a network or Web server with excessive requests to cause it to fail (see denial of service attack). The computer is compromised via a Trojan that often works by opening an Internet Relay Chat (IRC) channel that

waits for commands from the person in control of the botnet. There is a thriving botnet business selling lists of compromised computers to hackers and spammers (PC Mag, 2013).

Computer Network Attack (CNA): A category of "fires" (weapon system to create specific lethal or nonlethal effects on target) employed for offensive purposes in which actions are taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems/ networks themselves. The ultimate intended effect is not necessarily on the target system itself, but may support a larger effort, such as information operations or counter-terrorism, e.g., altering or spoofing specific communications or gaining or denying access to adversary communications or logistics channels (DoD Cyberspace Glossary, 2013).

Computer Network Exploitation (CNE): Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data about target or adversary automated information systems or networks. See also computer network attack (DoD Cyberspace Glossary, 2013).

Cyber Attack: A successful one is general seen as targeting vulnerable computers and making them malfunction or resulting in disrupted flows of data that disable businesses, financial institutions, medical institutions, and government agencies. Cyber-attacks can also target applications and databases.

Cyber Espionage: Unauthorized spying by computer. That term generally refers to the deployment of viruses that clandestinely observe or destroy data in the computer systems of government agencies and large enterprises (PC Mag, 2013).

Cyberspace: The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid (DoD Cyberspace Glossary, 2013).

Cyber Warfare: An armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber-attack, cyber defense, and cyber enabling actions (DoD Cyberspace Glossary, 2013).

Cybercrime: Criminal activity or a crime that involves the Internet, a computer system, or computer technology (Dictionary.com, 2013).

Distributed Denial of Service (DDoS). A DDoS attack is an attempt to make a computer or network resource unavailable to its intended users by saturating the target machine with external communication requests, until it is unable to respond to legitimate traffic. This causes a slow response from the system until it is rendered effectively unavailable (Armoraid, n.d.).

Distributed Denial of Service (DDoS): A cyber-attack in which a cracker bombards a targeted computer with thousands (or more) of fake requests for information causing the computer to run out of memory and other resources and to either slow down dramatically or to stop. The cracker uses more than on (typically hundreds or thousands) of previously cracked computers connected to the Internet to start the attack. These computers are called "zombies," indicating that they operate under somebody else's control who has evil intentions. The multiple origins of the attack make it difficult to defend against (Schell & Martin, 2006).

Domain Name System (DNS): A hierarchical system of naming hosts and placing the TCP/IP hosts into categories. The DNS is a way of translating numerical Internet addresses into word

strings to computer and network names. For example, the host name re.internic.net is also known as 198.41.0.13 (Schell & Martin, 2006).

Hacker: In the positive sense of the word, a *hacker* is an individual who enjoys learning computer system details and how to capitalize on his or her capabilities. This term often incorrectly used for **"cracker"** which refers to someone who engages in unethical or illegal computer exploits (Schell & Martin, 2006).

Internet Fraud: Encompasses a wide range of online criminal activities that deliver harm to the targets such as credit card fraud, online auction fraud, unsolicited email (Spam) fraud, and online child pornography. In the U.S., the Internet Fraud Complaint Center (IFCC), a partnership between the FBI and the National White Collar Crime Center (NW3C), was created to address Internet fraud (Schell & Martin, 2006).

Internet Service Provider (ISP): Also sometimes called an Internet Access Provider (IAP), it is a company that provides clients access to the Internet. For a fee, clients receive a software package, a username, a password, and an access phone number. Equipped with a modem or ISDN device, the client can then log on to the Internet. The client can browse the World Wide Web (WWW) or send and receive email (Schell & Martin, 2006).

Logic Bomb: Hidden code instructing a computer virus to perform some potentially destructive action when specific criteria are met (Schell & Martin, 2006).

Malicious Code: Programs such as viruses and worms designed to exploit weaknesses in computer software replicate and/or attach themselves to other software programs on a computer or network. Because they are designed to cause harm to a computer's or a network's operation, viruses and worms are known as malicious code. In short, malicious code not only propagates

itself but also typically causes damage to a computer system – such as denying access to legitimate users, altering or deleting data, or deleting complete file systems and disks.

Malware: Comes in many forms and can be any program or source code producing output that the computer owner does not need, want, or expect. For example, malware can be a remote access Trojan horse that can not only open a back door to a remote computer but also control someone's computer or network from a remote location. Malware includes viruses, worms, Trojan horses (that can, for example, spy on the system and display ads when the user least expects it), and malicious active content arriving through email or Web pages visited. These forms of malware normally run without the knowledge and permission of the user (Schell & Martin, 2006).

Snail Mail: Regular posted mail (Schell & Martin, 2006).

Spam: E-mail that is not requested. Also called "junk e-mail," "gray mail," "unsolicited commercial e-mail" (UCE) and "unsolicited bulk e-mail" (UBE), the term is both a noun (the e-mail message) and a verb (to send it). Spam is mostly used to advertise products and sometimes to broadcast political or social commentary. Spam may also be an acronym for "sales promotional advertising mail" or "simultaneously posted advertising message." (PC Mag, 2013).

Spear phishing: Cyber-attack that is targeted at a single organization. Usually, the attack is hidden in an email that seems to come from a trusted sender within the targeted organization (Schell & Martin, 2006).

Trapdoor: Undocumented software features that allow a user to gain computer access to or greater privileges through its use. These features may be a software bug or something added by a programmer during software development that was not removed when the software went into

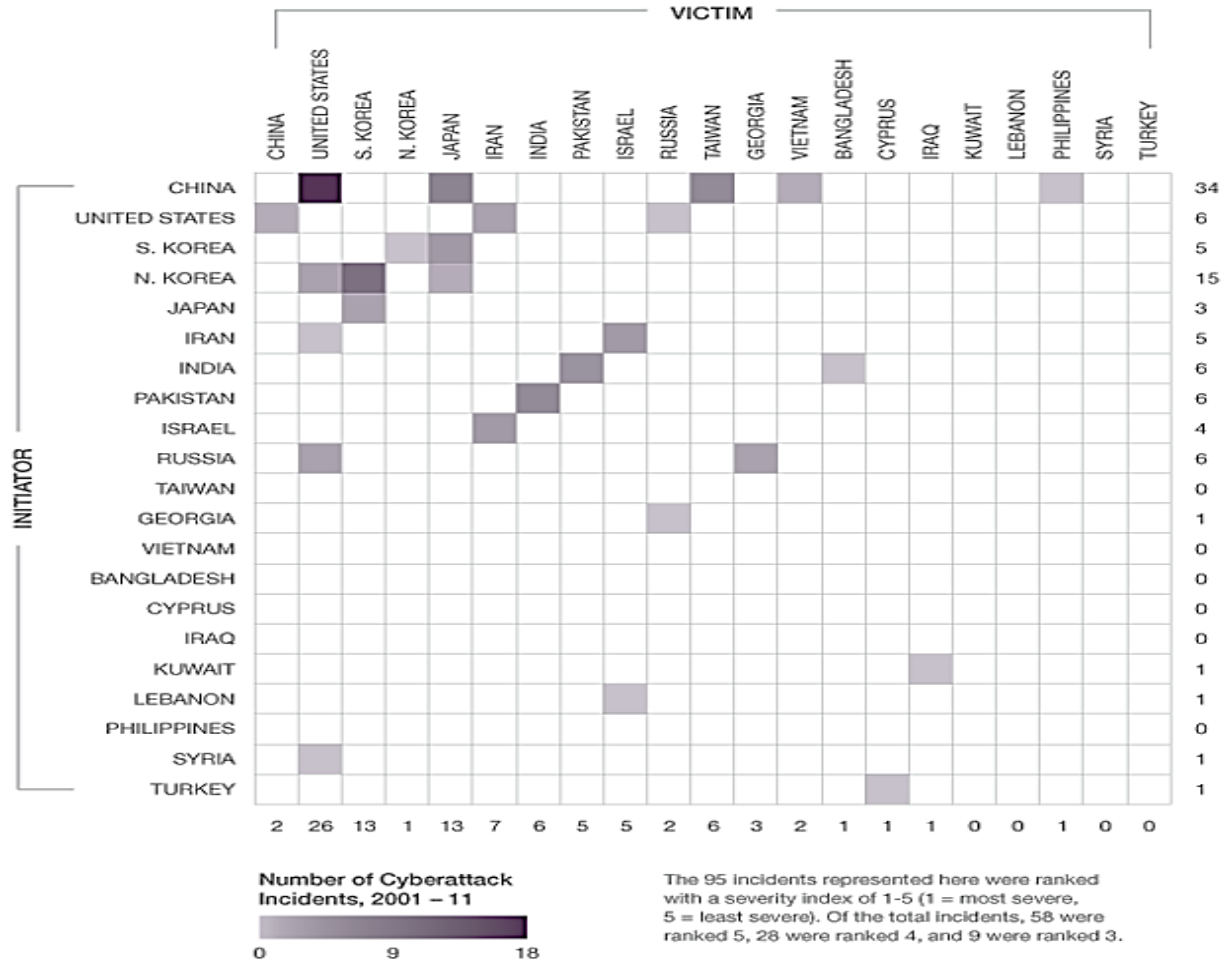
production. A trap door, often considered to be a synonym for "back door," is frequently used by crackers to facilitate exploits (Schell & Martin, 2006).

Virus: Can be a harmful, self-replicating program usually hidden in another piece of computer code, such as an email message. However, some virus infections are purely host based, so they do their "black magic" only locally (Schell & Martin, 2006).

Worm: A self-replicating, self-contained software program that does not need to be part of another program to propagate. A virus, in contrast, attaches itself to and becomes part of another executable program. Worms as well as viruses typically contain some kind of malicious payload besides the propagation and infection mechanism (Schell & Martin, 2006).

Zombie: A computer program used in DDoS attacks. A cracker plants software programs or scripts on large computers having high-speed connections to the Internet. These "planted" machines are controlled by the cracker through zombie processes. Zombies lie in wait until the cracker sends them some signal telling them to bombard a targeted site. When the command is received, the zombies send thousands or more fake requests for information to the server – all at the same time. In an attempt to handle so many information requests, the targeted computer soon runs out of memory and other critical resources, causing it to slow down greatly or to come to a halt (Schell & Martin, 2006).

Appendix B – Number of Cyber Attacks 2001-2011



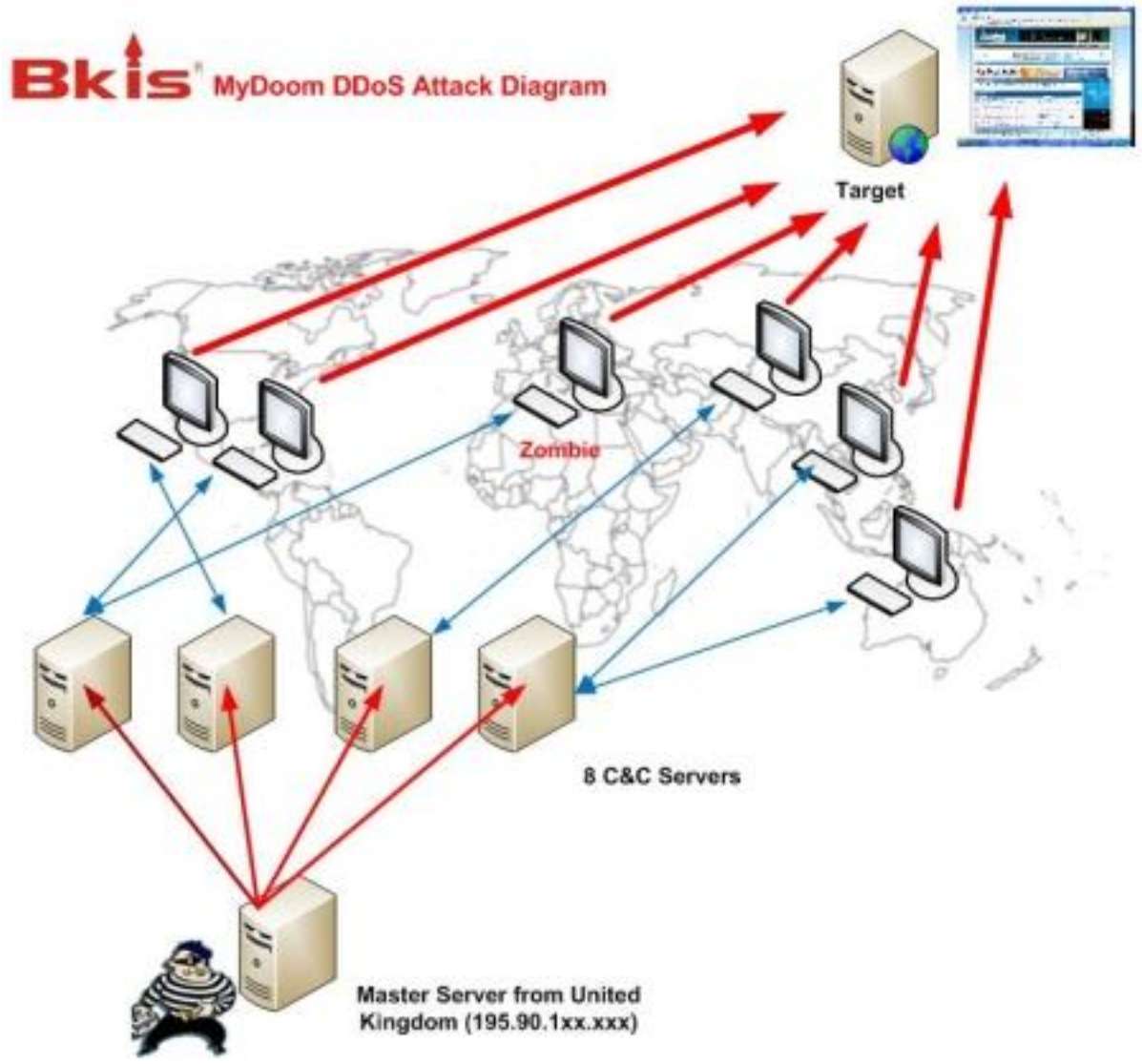
Source: Reproduced from: *The Fog of Cyberwar* (Valeriano & Maness, 2012)

Appendix C – NK and ROK Mobile Telephone Subscriber Comparison

Country	Number of Mobile Telephone Subscribers per 100 Population			
	2008	**2009**	**2010**	**2011**
NK	0	.28	1.77	4.09
ROK	95.54	99.95	105.36	108.50

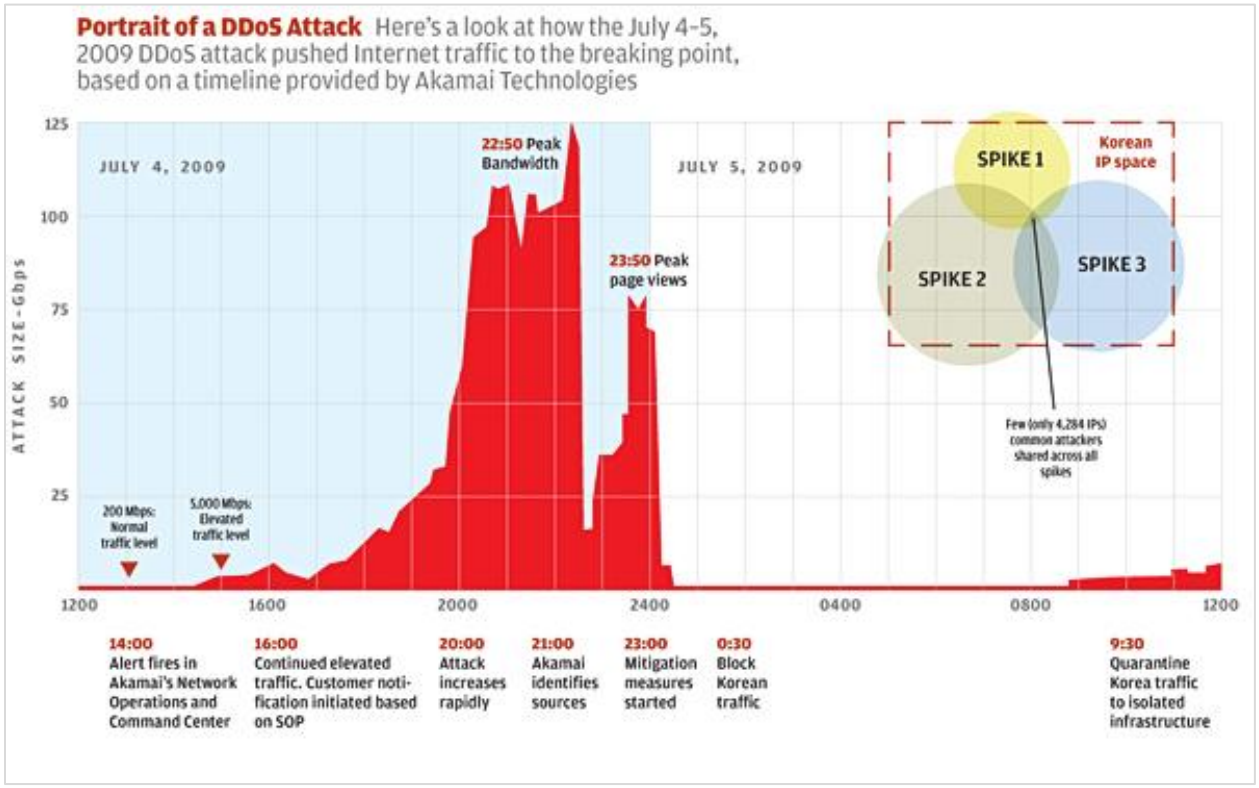
Source: Reproduced from: UN Statistical Database (UN, 2013).

Appendix D – 2009 DDoS Attack Against ROK and U.S.



Source: Reproduced from Korea and US DDoS attacks: The attacking source located in United Kingdom (Bkav, 2009)

Appendix E – 2009 DDoS Attack



Source: Reproduced from: *The DDoS Attack Survival Guide* (Brenner, 2010)