North Korean leader Kim Jong-un inspects the Sci-Tech Complex 28 October 2015 in Pyongyang, North Korea. (Photo released by North Korea's Korean Central News Agency)

North Korean Cyber Support to Combat Operations

1st Lt. Scott J. Tosi, U.S. Army

As recently as 2014, some Western cyber experts were describing the cyber capabilities of North Korea (the Democratic People's Republic of Korea, or DPRK) with apparent indifference, such as Jason Andress and Steve Winterfield in *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, who characterized the DPRK's capability to carry out cyberattacks as "… questionable, but [it] may actually exist."[1] The well-known November 2014 cyberattack attributed to the DPRK, executed against Sony Corporation as a response to the film *The Interview,* helped change perceptions in the United States of DPRK cyber capabilities—from a minor local nuisance directed at South Korea (the Republic of Korea, or ROK) to a major global strategic threat.[2]

While the DPRK has been considered a major strategic cyber threat since the attack on Sony, consideration also should be given to the potential tactical use of cyber capabilities as an extension of its warfighting strategy.

> … the real purpose of the DPRK's military policy and political aggressiveness has become to control and subdue its own population and retain power …

The less familiar tactical use of cyberattacks as a means of warfighting poses a greater threat to ROK and U.S. forces than any politically motivated strategic cyberattack ever could. The DPRK military's materiel is considered technologically obsolete at the tactical level. However, evidence suggests the Korean People's Army (KPA) will conduct cyber operations as an asymmetric means to disrupt enemy command and control and to offset its technological disadvantages during combat operations; therefore, U.S. and partner forces should prepare for this threat.[3]

North Korean Military Strategy

To understand how the DPRK would be likely to conduct tactical cyber operations in support of combat units during war, it is helpful to consider the historical aims and presumed military theory of the increasingly isolated and technologically declining nation. After failing to unify the peninsula from 1950 to 1953, *kukka mokp'yo*—communization of the ROK, through military force if necessary—became and has remained a primary objective of the DPRK, according to Korea expert James M. Minnich.[4] As a 2012 report to Congress pointed out, however, the real purpose of the DPRK's military policy and political aggressiveness has become to control and subdue its own population and retain power rather than to unify the Korean Peninsula.[5] Nonetheless, events such as the shelling of Yeonpyeong Island in 2010 and the exchange of artillery fire in Yeoncheon in 2015 have shown that minor provocations have the potential to erupt into open combat. Moreover, combat could become full-scale war. Whether through accidental escalation of force or a premeditated surprise invasion, the DPRK may be fully willing to go to war.[6]

Following its failure in the Korean War, the DPRK expanded and reorganized its military using features of the Soviet and Chinese militaries. Subsequently, it has continued to draw influence, equipment, and doctrine from Russia and China, according to Minnich.[7] To avoid the same fate as the drawn-out invasion of the ROK, the DPRK military appears to have developed a strategy known as *kisub chollyak*, which calls for a quick, decisive war conducted with mixed tactics against ROK and U.S. military forces on the peninsula.[8] This approach has become more intransigent over time due to the DPRK's increasing economic inability to sustain a protracted war. Therefore, to achieve its tactical objectives as rapidly as possible, the DPRK has organized its military to initiate combat with "massive conventional and chemical cannon and missile bombardments while simultaneously employing special operations forces teams," according to Minnich.[9] Estimates of the number of DPRK special operations forces vary between eighty thousand and one hundred eighty thousand soldiers who could conduct asymmetric attacks in the south, intended to enable the large-scale light infantry forces that would follow.[10]

Initially, the DPRK likely considered bombardment and special operations followed by a large-scale invasion force sufficient to quickly disrupt, confuse, outmaneuver, and overwhelm peninsula-based ROK and U.S. military

forces before U.S. reinforcements could arrive. However, the strategy faced a shock in the early 1990s after the fall of the Soviet Union and withdrawal of materiel support that came from it. This shock no doubt was amplified in 1991 by the unexpectedly fast and easy defeat by the United States of Saddam Hussein's Iraqi army, which attempted to employ similar tactics and weaponry against the United States as the DPRK had long planned to use against the ROK.[11] The fall of Hussein's numerically superior army to the U.S. military surely came as a wake-up call to China and the DPRK, which were relying on technologically inferior but numerically superior forces to overwhelm their enemies quickly. Technology was proven superior to overwhelming numbers in force-on-force combat. Concurrently, the likelihood that DPRK forces would be easily overmatched by U.S. technological advantages was accompanied by a rapid decline of the DPRK economic and agricultural sectors, which further diminished its ability to project and sustain military forces.[12]

The DPRK's response to these events included building its nuclear program.[13] While U.S. success in Operation Desert Storm implied that the DPRK military could be quickly and decisively defeated by the United States in conventional war, albeit at a potentially high cost of life of Korean civilians, the DPRK's nuclear program introduced a high risk of mass destruction of ROK and U.S. targets, should the United States or the ROK provoke war.

Notwithstanding, while the development of a nuclear deterrence option supported defensive political goals for the DPRK, it did little to advance the prospect of kukka mokp'yo. For that, the DPRK seems to have emulated China's apparent doctrinal changes made in the wake of Desert Storm.

After the United States defeated the Iraqi army—the fifth largest in the world in 1990—in just five weeks, the Chinese military apparently reevaluated its warfighting strategy and tactics.[14] In the 1990s, China developed a strategy of hybrid warfare that relied on relatively cheap technological methods for negating the United States' qualitative military superiority through indirect attacks. In 1999, evidence of the Chinese military's new approach appeared in *Unrestricted Warfare: China's Master Plan to Destroy America* (an English summary translation based on a 1999 publication by two Chinese army colonels), which described using several asymmetric measures to defeat the United States, including conducting information warfare aimed at negating the U.S. military's visibility of the battlefield through all means necessary.[15] National security scholars Richard A. Clarke and Robert Knake assert that this strategy has resulted in China's adoption of large-scale cyberwarfare, which would include the stealing of technological information and the tactical targeting of intelligence, reconnaissance, and surveillance assets to equalize the battlefield in any force-on-force action.[16]

Believing its nuclear program would deter attacks on its homeland, and having survived the economic and agricultural crisis of the 1990s, the DPRK faced a dilemma in the early 2000s similar to what China faced in the wake of the Gulf War, when it became apparent that China would be vulnerable to defeat by advanced U.S. weapons technology. The DPRK's general response to this dilemma was threefold: increasing the number of special operations forces to conduct unconventional warfare, expanding its electronic warfare and signals intelligence assets to conduct jamming operations, and, most important, creating tactical and strategic cyber operations under what are known as Bureau 121, No. 91 Office, and Lab 110.[17] As with any aspect of the DPRK, it is difficult to verify information about these secretive organizations.

North Korean Cyber Organization

It is reported that Bureau 121, No. 91 Office, and Lab 110 are components of six bureaus under the Reconnaissance General Bureau (RGB) that specializes in intelligence gathering under the administration of the General Staff Department (GSD). While the GSD is responsible for the command and control of the KPA, it falls under the Ministry of People's Armed Forces (MPAF), according to Andrew Scobell and John M. Sanford.[18] This arrangement would give the RGB direct operational control from the top of the chain of command and ensure the cyber component could conduct operations independently and in support of the KPA based on operational need.

1st Lt. Scott J. Tosi, U.S. Army, is the executive officer for A Company, 310th Military Intelligence Battalion, 902nd Military Intelligence Group. He previously served as the executive officer for Headquarters and Headquarters Company, 501st Military Intelligence Brigade out of Yongsan, Korea. He holds a BS in history and social sciences education from Illinois State University, and he taught high school history and civics in Bloomington, Illinois.

Bureau 121 reportedly comprises an intelligence-gathering component and an attack component. The unit is thought to operate primarily out of Pyongyang as well as the Chilbosan Hotel in Shenyang, China.[19] No. 91 Office is believed to operate out of Pyongyang to conduct hacking operations for the RGB.[20] Lab 110 is believed to conduct technical reconnaissance, infiltration of computer networks, intelligence gathering through hacking, and planting viruses on enemy networks.[21]

While there appear to be numerous other cyber organizations in the DPRK, those outside the RGB primarily pertain to internal political control or spreading political propaganda to foreign nations. Therefore, their work relates little to tactical or operational cyber support for combat operations.

Estimates of the size of the DPRK's cyber force have ranged from as few as 1,800 hackers and computer experts to nearly six thousand, which would make it the third largest cyber agency behind the United States and Russia.[22] The higher estimate reportedly came from ROK intelligence early in 2015, but the number cannot be verified. Moreover, it was unclear whether No. 91 Office and Lab 110 were included in the calculation, but given the ROK's desire to influence the United States to consider DPRK cyber threats a priority, it is likely their strength was included (some consider the ROK estimates inaccurate due to bias). Furthermore, the ROK's estimate represents 2013 data and, like much intelligence on North Korea, is already out of date.

North Korean army hackers are widely reported to work in the Chilbosan Hotel (photographed here 17 April 2005), partly owned by the North Korean government, in Shenyang, China. Such reports are plausible due in part to the apparent advantages of working from China, such as the ready availability of multiple lines of communication, not to mention modern equipment, training, logistical support, and a reliable source of power. (See, for example, James Cook, "PHOTOS: Inside The Luxury Chinese Hotel Where North Korea Keeps Its Army of Hackers," Business Insider website, 2 December 2014, accessed 12 June 2017, http://www.businessinsider.com/photos-chinese-hotel-where-north-korea-keeps-hackers-2014-12). (Photo by tack well, Flickr)

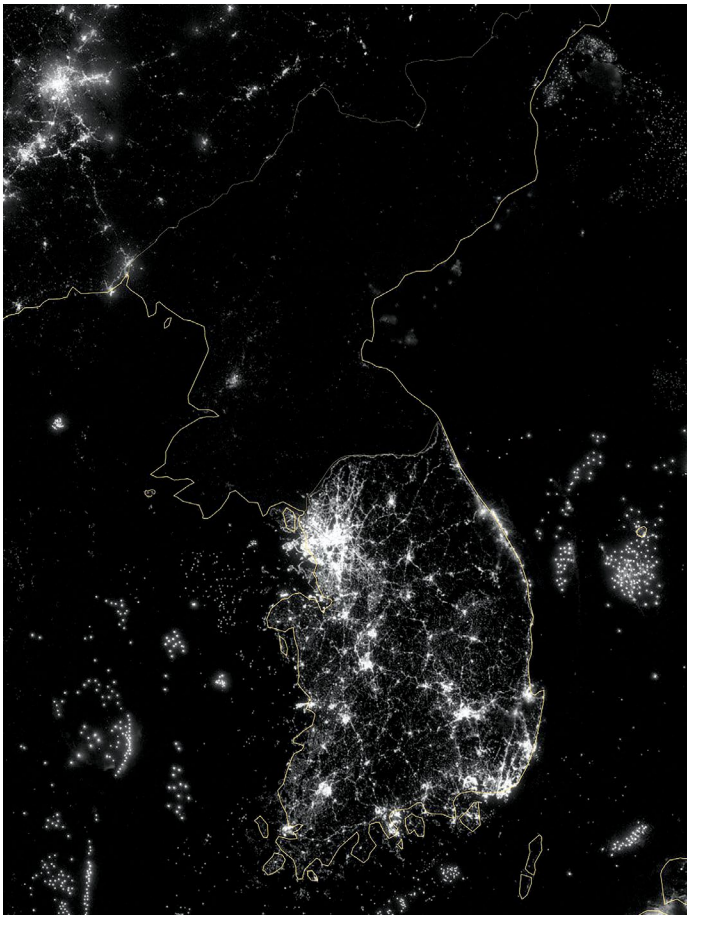
Irrespective, the shortage of concrete knowledge of DPRK cyber organizations is compounded by the nature of DPRK's Internet access. The DPRK has divided its networks into two components. Only government and military agencies can access the outward-facing network routed through China, which hackers use for conducting cyberattacks. The other component is the *kwangmyong*, a monitored intranet of government-selected content.[23] As of January 2013, one "Internet café" was reported

in the DPRK, in Pyongyang, where citizens reportedly can access only the kwangmyong.[24] The use of Chinese networks to access the global Internet provides a buffer for DPRK hackers to deny responsibility for their intrusions and attacks. Moreover, they can safely conduct outbound attacks while avoiding inbound attacks from the ROK or the United States.[25]

However, use of third parties for outward Internet access also makes DPRK cyber operations reliant on continued cooperation from China and other partners. Despite waning support for the isolated state in recent years, China's support seems assured during peacetime. However, it is not guaranteed if war breaks out.

Since the low level of connectivity functions as protection from outside attacks, the DPRK can focus on developing offensive cyber capabilities. Few DPRK systems or networks if compromised would reduce warfighting capabilities.[26] The high-profile cyberattacks attributed to DPRK hackers have served largely strategic and political purposes. However, cyber support to combat units in the event of full-scale war likely remains a key component of a DPRK strategy.

Cyberwarfare is unique in that once a new methodology or technique has been used in an attack, the victim can create countermeasures relatively quickly to prevent future attacks. Probably for this reason the DPRK has not, and most likely would not, conduct large-scale tactical or operational cyberattacks on the ROK or the United States unless at war. Rather, the DPRK would conduct only small-scale reconnaissance and testing of methodologies on enemy networks. This approach would mitigate the risk of enemies developing countermeasures that would compromise advantages the DPRK wants to maintain for full-scale war.



A satellite image of North Korea compared to South Korea at night. Technological backwardness reportedly compels North Korean army hackers to seek locations outside of North Korea, such as the Chilbosan Hotel in China, where access to technology and communications lines is readily available to conduct cyberattacks. (Image courtesy of NASA)

Although U.S. and partner forces know relatively little about the DPRK's cyber capabilities, China and Russia can be studied as models. China, as North Korea's closest (and perhaps only) ally, provides not only outward-facing networks for North Korean cyber units but also bases of operations, such as the Chilbosan Hotel, and training. Known Chinese cyber actions have primarily focused on technological espionage, something the DPRK probably has little interest in as it lacks the infrastructure to build or maintain technologically advanced weaponry as China does. In contrast, Russia's cyber activities during its 2008 invasion of Georgia and 2014 military action in Ukraine suggest the DPRK's likely tactical cyber actions in the event of war on the Korean Peninsula.

North Korean Tactical Cyber Support to Warfighting

While a land, air, and sea war on the Korean Peninsula would commence, or escalate, at a specific date and time, the cyber war would begin long before any shots were fired.[27] While, arguably, the cyber war with the DPRK is already ongoing, it would need to increase the frequency and intensity of cyber reconnaissance and attacks before a general war in order to

successfully support conventional combat units. In the lead-up to war and early stages of war, North Korean asymmetric cyber units would target civilian communications through simple denial of service.

In 2008, Russia preceded its attack on Georgia with distributed denial of service (DDOS) attacks for weeks before Russian soldiers crossed the border to test their capabilities and conduct reconnaissance on Georgian networks, planning to attack them again later. Russia attacked Georgian communications, crippling the government's ability to communicate and coordinate against Russian forces.[28] The Russian cyberattacks combined simplicity with sophistication in execution; they allowed Russia to cheaply take down Georgian command and communications. What would have taken days, if not weeks, of bombing and coordination between intelligence and air power took minutes from the safety of Russian computers but achieved the same result. U.S. and partner forces can reasonably expect that as a technologically inferior nation with an obsolete air force and navy, the DPRK would conduct similar attacks.

Furthermore, the DPRK appears to have demonstrated such capability. From 2014 to 2016, the DPRK reportedly hacked "more than 140,000 computers" in the ROK belonging to government and businesses, and it tried to attack the ROK transportation system's control network.[29] The attacks, likely carried out by Bureau 121, enabled the DPRK to gain access to and monitor ROK government and business communications.

If this had occurred during an invasion, the DPRK might have turned off all 140,000 computers, rendering these organizations' communications defunct. It might have been able to shut down or desynchronize the ROK transportation network.

If increased in scope and aggressiveness, such attacks could cut the ROK's communication and information-sharing capabilities with the military. Conducted in conjunction with special operations forces destroying physical communications systems in the ROK, the DPRK might disable ROK and U.S. communications, leaving units on the battlefield blind. Cutting communications in the early stages of the war would cripple the ROK and U.S. ability to coordinate artillery and aerial assets, giving DPRK forces time and space to overwhelm ROK and U.S. forces in the demilitarized zone.

While targeting of communications and critical networks in the ROK would hamper ROK and U.S. efforts, alternative means of communication might still enable the two nations to counter the DPRK's aggression. However, vital secondary means of communication could be neutralized by targeting the ROK power grid, potentially negating the ROK and U.S. advantages over DPRK forces by slowing a timely coordinated response to aggression. Several years ago, such an attack would have been deemed impossible for a nation as technologically backward as the DPRK. Today, such an attack by the DPRK in the event of war is almost certain.

For example, in December 2015, Russian hackers caused a power outage in Ukraine via cyberattack. They installed malware on Ukraine's power plant network and remotely switched breakers to cut power to over 225,000 people.[30] Russia then swamped Ukrainian utility customer service with fake phone calls to prevent the company from receiving customer calls.[31] Given the level of sophistication that DPRK cyber units seem to have reached and the relationship the DPRK maintains with Russia, it is likely that the DPRK has received support from Russia for potentially conducting similar attacks against ROK power plants.

Cyberattacks, in essence, would be an asymmetric approach to compensate for the DPRK's almost nonexistent air force. They could inflict tactical and operational damage on the ROK to enhance the "shock-and-awe" bombardments that likely would precede military intervention. By knocking out critical communications, transportation, and support infrastructure, the DPRK would cause confusion and disorder that would facilitate its conventional infantry forces' overwhelming ROK and U.S. forces.

Nevertheless, while these methods could be effective, it is unlikely Bureau 121 would be able to fully take the ROK network offline, although a fractional network disruption could severely hinder ROK and U.S. actions on the battlefield. To fully negate ROK and U.S. technological superiority, the DPRK would need to employ more sophisticated cyberattacks against GPS, radar, logistics support systems, and weapons targeting systems. Exactly how the DPRK would conduct such attacks is outside the scope of this discussion. The threat should be taken seriously, however, as the Defense Science Board warns, "should the United States find itself in a full-scale conflict with a peer adversary, … U.S. guns, missiles, and bombs may not fire, or may be directed against our own troops. Resupply, including food, water, ammunition, and fuel may not arrive when or where needed."[32]

Students work at computers 13 April 2013 at Mangyongdae Revolutionary School in Pyongyang, North Korea. The school is run by the military, and school administrators say it was originally set up in 1947 for children who had lost their parents during Korea's fight for liberation from its Japanese occupiers. (Photo by the Associated Press)

Hacking or taking radar and GPS offline, if even for several days before ROK and U.S. forces could recover, could ground air power, offering DPRK units freedom of maneuver on the battlefield. Moreover, the disruption of GPS would not only negate the use of GPS-guided weapons systems, but, more dangerously, it could also cause weapons to fire at incorrect coordinates. The hacking of U.S. satellites, which China reportedly has already shown it can accomplish, could blind ROK and U.S. intelligence to DPRK movements on the ground.[33]

If the DPRK hacked automated logistical networks that supported ROK and U.S. forces on the peninsula, those forces would have difficulty sustaining warfighting capabilities. Tracking, requisitioning, and delivering essential war supplies could be disrupted by a simple DDOS attack that would shut down systems or corrupt data, causing logistical supplies to be sent incorrectly. ROK and U.S. soldiers could quickly find themselves without the resources necessary to fight.

Therefore, the DPRK could use cyberattacks to ensure its numerical superiority and overwhelming volume of firepower could triumph despite inferior materiel. When combined with electronic warfare and special operations forces acting behind the battle lines, this would, consistent with the ideals in *Unrestricted Warfare*, cause ROK and U.S. forces to lose momentum and maintain a defensive and reactionary posture.

Unrestricted Warfare describes the "golden ratio" and the "side-principal" rule. The idea is that the golden ratio, 0.618 or roughly two-thirds, which is usually applied to art, architecture, and mathematics, can be applied to warfare. The authors point out that once the Iraqi army was reduced by the U.S. Air Force to 0.618 of its original strength, it collapsed and the war ended.[34] The side-principal rule, in essence, is the idea that war can be won through nonwar actions. When taking these two theories together, it becomes apparent that while the Chinese may

believe they could not defeat the United States in war through conventional combat, they probably believe they could defeat the United States if nonwar actions were used to diminish the U.S. military's strength to around two-thirds of its combat power.

For China, the options for achieving this are numerous, as China has increasing resources it can draw upon to carry out nonwar actions for extended periods, be they cyber, financial, or political. For the DPRK, with its goal of kukka mokp'yo and its extremely limited resources, the options are fewer. The DPRK likely would translate the golden ratio and side-principal rule into diminishing ROK and U.S. forces through cyberattacks, combined with numerous other asymmetric means, by one-third. With their systems taken offline or corrupted, U.S. and ROK warfighting capabilities would be diminished or disrupted to a point where, theoretically, the DPRK army could launch a massive ground invasion. Cyberattack, therefore, is a means by which the DPRK likely would strike at enemy warfighting support systems, thereby giving its numerically superior military the space, time, and freedom of maneuver to sustain a fight on the peninsula.

A cyberattack could include a nuclear-detonated electromagnetic pulse that would disable electronic devices within a 450-mile radius.[35] The DPRK could, theoretically, achieve this by detonating a nuclear device in the atmosphere at an altitude of thirty miles. This attack could negate technological advantages of friendly forces on the peninsula, rendering equipment with an electronic component useless. However, given the threat of nuclear retaliation as well as the increased likelihood of U.S. support of a prolonged war, which would most likely result in the DPRK's defeat, this option probably would remain a last resort short of a tactical nuclear strike.

Solutions to Counter North Korean Cyber Capabilities

North Korean leadership likely believes the DPRK could revert the tactical balance of power to that of the 1950s, using its cyber capabilities to gain an advantage. In June 1950, U.S. tactical ground forces were embarrassingly defeated by a numerically superior enemy that was less trained, less equipped, and thought to be less prepared for war. As the United States continues to withdraw permanent combat units from the ROK and revert to a support role, leaving its forces on the peninsula unprepared to mount a major defense, the United States should take action to avoid finding itself in a situation similar to 1950.

DPRK cyber capabilities are not without their vulnerabilities. In 2014, in retaliation for the Sony hacks, the United States conducted a DDOS attack on the DPRK that took the kwangmyong offline.[36] This attack, however, did not retaliate against the cyber units, mostly operating out of China, but instead took the intranet offline. This event highlights a major vulnerability of the DPRK in a time of full-scale war. DPRK cyber operability likely would be at the mercy of the Chinese government. Should the Chinese government decide the continued support of the DPRK was politically unsustainable, the DPRK's cyber capability could become marginalized.

To mitigate the risk of DPRK cyber threats, Army assets must actively partner with ROK forces and reassess the way they view cyber operations. As a preventive measure, Army cyber assets must monitor U.S. networks within the ROK and networks of units scheduled to deploy to the ROK, as these units are the most likely to be targeted by DPRK assets. Rather than actively neutralize identified DPRK cyber threats, Army leaders must assess the intelligence benefits gained by allowing adversaries limited freedom of action in order to study their tactics, techniques, and procedures in the cyber domain.

Army leaders should begin studying cyber operations as a force multiplier from both an offensive and defensive vantage, and not as a discipline outside the tactical or operational domain. Additionally, Army forces stationed in the ROK should develop contingency plans with ROK forces anticipating DPRK cyberattacks similar to those outlined in this article, and they should train in environments shaped by cyberwarfare. In this way, U.S. and South Korean forces could mitigate the significant threat posed by North Korean cyber forces. ■

Notes

1. Jason Andress and Steve Winterfield, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners,* 2nd ed. (Waltham, MA: Syngress, 2013), 73. Andress and Winterfield cite Jung Kwon Ho, "Mecca for North Korean Hackers," Daily NK online, 13 July 2009.

2. Clyde Stanhope, "How Bad is the North Korean Cyber Threat," Hackread website, 20 July 2016, accessed 2 May 2017, https://www.hackread.com/how-bad-is-the-north-korean-cyber-threat/; Office of the Secretary of Defense (OSD), "Military and Security Developments Involving the Democratic People's Republic of Korea: 2015," A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2012, accessed 4 May 2017, https://www.defense.gov/Portals/1/Documents/pubs/Military_and_Security_Developments_Involving_the_Democratic_Peoples_Republic_of_Korea_2015.PDF.

3. James M. Minnich, *The North Korean People's Army: Origins and Current Tactics* (Annapolis, MD: Naval Institute Press, 2005), 68.

4. Ibid.

5. OSD, "Military and Security Developments Involving the Democratic People's Republic of Korea: 2012," A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2012, 15 February 2013, accessed 6 May 2017, http://archive.defense.gov/pubs/Report_to_Congress_on_Military_and_Security_Developments_Involving_the_DPRK.pdf.

6. Daniel Wagner and Michael Doyle, "Scenarios for Conflict Between the Koreas," Huffington Post, 25 February 2012, accessed 2 May 2017, http://www.huffingtonpost.com/daniel-wagner/scenarios-for-conflict-be_b_1169871.html.

7. Minnich, *The North Korean People's Army*, 53–54.

8. Ibid., 73.

9. Ibid., 73–74.

10. Ibid.; Blaine Harden, "North Korea Massively Increases Its Special Forces," *Washington Post* website, 9 October 2009, accessed 3 May 2017, http://www.washingtonpost.com/wp-dyn/content/article/2009/10/08/AR2009100804018.html; OSD, "Military and Security Developments Involving the Democratic People's Republic of Korea: 2015."

11. Joseph Bermudez, *North Korea's Development of a Nuclear Weapons Strategy* (Washington, DC: US-Korea Institute at SAIS [Johns Hopkins School of Advanced International Studies], August 2015), accessed 4 May 2017, http://uskoreainstitute.org/wp-content/uploads/2016/02/NKNF_Nuclear-Weapons-Strategy_Bermudez.pdf.

12. Ibid.

13. Ibid.

14. James M. Broder and Douglas Jehl, "Iraqi Army: World's 5th Largest but Full of Vital Weaknesses," *Los Angeles Times* online, 13 August 1990, accessed 8 May 2017, http://articles.latimes.com/1990-08-13/news/mn-465_1_iraqi-army.

15. Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), 28–29; Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America*, summary translation (Panama City, Panama: Pan American Publishing, 2002).

16. Clarke and Knake, *Cyber War*, 30–32.

17. Harden, "North Korea Massively Increases Its Special Forces"; Stanhope, "How Bad is the North Korean Cyber Threat."

18. Andrew Scobell and John M. Sanford, *North Korea's Military Threat: Pyongyang's Conventional Forces, Weapons of Mass Destruction, and Ballistic Missiles* (Carlisle, PA: Strategic Studies Institute, 2007), 14–16; Hewlett-Packard [HP] Enterprise SR [Security Research]-FI_Team, "Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape," HP Security Briefing, Episode 16, August 2014, HP Enterprise Community website, accessed 6 May 2017, http://community.hpe.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf.

19. SR_FI Team, "Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape."

20. Pierluigi Paganini, "Concerns Mount over North Korean Cyber Warfare Capabilities," Infosec Island website, 11 June 2012, accessed 14 February 2017, http://www.infosecisland.com/blogview/21577-Concerns-Mount-over-North-Korean-Cyber-Warfare-Capabilities.html.

21. "North Korea Launched Cyber Attacks, Says South," *The Guardian* website, 11 July 2009, accessed 4 May 2017, https://www.theguardian.com/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks.

22. Ju-min Park and James Pearson, "In North Korea, Hackers are a Handpicked, Pampered Elite," Reuters website, 5 December 2014, accessed 6 May 2017, http://www.reuters.com/article/us-sony-cybersecurity-northkorea-idUSKCN0JJ08B20141205; Darren Pauli, "NORKS Hacker Corps Reaches 5,900 Sworn Cyber Soldiers—Report," The Register website, 7 July 2014, accessed 6 May 2017, http://www.theregister.co.uk/2014/07/07/north_korea_employs_6000_leet_hackers_source_claims/.

23. Ashley Moreno, "Social Media in North Korea: The AP Bureau Chief from Pyongyang on Cell Service, Instagram, Etc.," *Austin Chronicle* website, 11 March 2013, accessed 4 May 2017, http://www.austinchronicle.com/daily/sxsw/2013-03-11/social-media-in-north-korea/.

24. Olga Khazan, "North Koreans Shouldn't Count on Using the New Google Maps," *Washington Post* website, 29 January 2013, accessed 3 May 2017, https://www.washingtonpost.com/news/worldviews/wp/2013/01/29/north-koreans-shouldnt-count-on-using-the-new-google-maps/.

25. OSD, "Military and Security Developments Involving the Democratic People's Republic of Korea: 2015."

26. Duk-Ki Kim, "The Republic of Korea's Counter-Asymmetric Strategy," *Naval War College Review* 65, no. 1 (Winter 2012): 68, accessed 8 May 2017, https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strateg.aspx.

27. For another perspective on North Korean cyber war, see Kim, "The Republic of Korea's Counter-Asymmetric Strategy," 58.

28. John Markoff, "Before the Gunfire, Cyberattacks," *New York Times* website, 12 August 2008, accessed 3 May 2017, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

29. Jack Kim, "North Korea Mounts Long-Running Hack of South Korea Computers, Says Seoul," Reuters website, 13 June 2016, accessed 14 February 2017, http://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE.

30. Dustin Volz, "U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage," Reuters website, 25 February 2016, accessed 14 February 2017, http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K.

31. Ibid.

32. Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, January 2013), 5, accessed 3 May 2017, http://www.dtic.mil/docs/citations/ADA569975.

33. Mary Pat Flaherty, Jason Samenow, and Lisa Rein, "Chinese Hack U.S. Weather Systems, Satellite Network," *Washington Post* website, 12 November 2014, accessed 3 May 2017, https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html.

34. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America*, 153–69.

35. Andress and Winterfield, *Cyber Warfare*, 147.

36. Cecilia Kang, "North Korean Web Goes Dark Days after Obama Pledges Response to Sony Hack," *Washington Post* website, 22 December 2014, accessed 3 May 2017, https://www.washingtonpost.com/business/economy/north-korean-web-goes-dark-days-after-obama-pledges-response-to-sony-hack/2014/12/22/b76fa0a0-8a1d-11e4-9e8d-0c687bc18da4_story.html.