International Journal of Korean Unification Studies
Vol. 22, No. 2, 2013, 63–90

Playing Blind-Man's Buff: Estimating North Korea's Cyber Capabilities

Tobias Feakin

This paper aims to create a clearer understanding of the size and scope of North Korean cyber capabilities. Due to the opaque and secretive nature of the North Korean regime, and the difficulties of attribution in cyberspace, it is problematic to present a complete picture of the North's malicious activities in cyberspace. This paper presents an open source literature based review of this issue. It begins by defining terminology used to describe cyber threats, and whilst seemingly these threats are new, cyberspace has merely facilitated a new method of achieving old ends. North Korean motivations for developing cyber capabilities are examined, followed by an examination of the historical context to their development of such efforts, and a breakdown of the various North Korean military departments involved cyber activities is presented. An analysis of the growing private sector-led evidential trail of North Korean cyber attacks is followed by an assessment of the impacts that these attacks have had on South Korean policymaking, and operational responses. Finally the author examines the potential impacts for national and regional destabilisation that unabated North Korean cyber attacks could have, concluding that severe damage to South Korea's economic, political and international reputation could be a distinctly negative consequence.

Key Words: cyber espionage, cyber attack, intelligence agencies, cyber policy, asymmetry

Introduction

Senator Steve Chabot in his opening remarks to the Subcommittee on Asia and the Pacific of the US House of Representatives' Committee on Foreign Affairs remarked:

> North Korea's growing cyber capabilities present the greatest likelihood of a cyber conflict in Asia. Earlier this year [2013] it demonstrated its capabilities in South Korea, where it crippled the operations of banks and news agencies by wiping the hard drives of thousands of computers. While McAfee's report on what is now called Operation Troy does not attribute these attacks to North Korea, it could not be clearer who was responsible. North Korea is not only a nuclear threat, but it a serious cyber threat as well.[1]

These stark words illustrate the increasing concern amongst government officials and commentators that North Korea has begun to rapidly accelerate its development of advanced offensive cyber capabilities. However, assessing a nation's ability to project power via cyber means is problematic, due in large part to the secrecy of those capabilities within government departments and the diffusion of responsibilities through those bureaucracies. To accurately understand the cyber capabilities of the USA is hard enough. However, when attempting to extract information from a nation as closed and secretive as North Korea, estimates on what capability is in existence are akin to playing Blind Man's Buff.[2] Despite the imperfect information in understanding North Korea's cyber capabilities, there is an increasing degree of open source information that when collated produces a best estimation of what capabilities it possesses. During 2013, this process was aided as more evidence and sources emerged detailing North Korea's prolonged targeting of its southern neighbours. This paper examines the motivations and attraction of cyber capabilities for North Korea and what drivers there might be for an offensive cyber

1. House of Representatives Subcommittee on Asia and the Pacific, "Committee on Foreign Affairs," *Asia the Cyber Security Battleground*, July 23, 2013, http://foreignaffairs.house.gov/hearing/subcommittee-hearing-asia-cyber-security-battleground.
2. Blindman's Buff, is a children's game played as early as 2,000 years ago in Greece. To play the standard game of blindman's buff, one player is blindfolded and then disoriented by being spun around several times. The other players, who are not blindfolded, amuse themselves by calling out to the "blind man" and dodging away from him. Encyclopaedia Britannica, http://www.britannica.com/EBchecked/topic/69380/blindmans-buff.

programme within that state. It then unpacks some of the historical context to cyber capability development in the North and examines how the state has begun to build educational programmes aimed at targeting the most gifted students to take into its military units. The paper gives a break down of the elements of the North Korean military which utilise cyber within their operations, and then dissects the growing evidence base of what North Korea is accused of doing in the South. Regardless of the success or not of the attacks, South Korea has been compelled to respond and develop its own cyber capabilities and has matured its relationship with its key ally, the US, on cyber issues. Finally the potential for regional destabilisation is examined through the unabated use of cyber capabilities in the region, and the dangers that offensive cyber usage can have in such a geopolitically sensitive part of the globe.

Defining Cyber Language

Whilst cyber threats are a relatively new concept, the desired ends that cyber means are used to reach are extremely old and well grappled with. But it is true that cyberspace has enabled a new method of achieving these old ends. An interconnected world enables new and increased access to information. This has become a significant problem for nation-states and their governments. As a tool for criminal purposes, to conduct espionage, to enhance war fighting capabilities or cause disruption via "hacktivism," cyberspace enables all these activities to take place on a larger scale than was previously possible. In practice these activities are not mutually exclusive and often by design intentionally overlap one another. In the context of this piece it is useful to define the various different malicious activities that take place online. This has the benefit of not only creating foundational clarity, but there is evidence to demonstrate that North Korean sources are exploiting all of these malicious avenues for their advantage.

Cybercrime

Cybercrime involves the use of computer systems to steal or compromise confidential information for criminal purposes, most frequently for financial gain. Such activities exploit vulnerabilities in the use of the internet and other electronic systems to illicitly access or attack information and services used by citizens, business and the Government. The total costs of this form of crime can have strategic effects over time, and the victims are most frequently individuals, businesses and other organisations.[3]

Cyber Espionage

Cyber espionage involves the use of computer systems to collect intelligence or enable certain covert operations, either in cyberspace or in the physical world. The motivations for such efforts include gaining classified, sensitive, personal or proprietary information to gain military, political, industrial or technological advantages.[4] Spying is nothing new, but conducting spying via electronic means enables a far larger data collection pool to be accessed at far less risk. Currently it is this area that will have the greatest impact on state-on-state relations unless considerable efforts are made to begin to stem the flow of information gathering from all governments.

Cyber War

Cyber war refers to the use of cyberspace by the military to deny an adversary, whether a state or non-state actor, the effective use of information systems and weapons, or systems controlled by information technology, in order to achieve a political end.[5] But the term

3. Kristin M. Lord and Travis Sharp, *America's Cyber Future: Security & Prosperity in the Information Age*, Center for New American Security, 2011, http://www.cnas.org/cyber.
4. *Ibid.*
5. *Ibid.*

becomes problematic. Whilst cyber attacks can have kinetic effects, they have not yet caused the type of destruction or bloodshed traditionally associated with warfare. It is important to point out that sophisticated cyber attacks, resulting in kinetic effects, by state actors against other states are aggressive and entail extreme political risk and potential for rapid escalation. Therefore, cyber exchanges are unlikely to be used in isolation within a "cyber war" but rather, they are likely to be used in conjunction with, or in advance of, a traditional physical attack.

Hacktivism

Hacktivism is used to define those that use computers or computer systems to promote particular political ends, primarily free speech, human rights and information ethics. It is used as a form of direct action against those that the hacker perceives as a legitimate target to publically expose or embarrass a particular company or government entity. Hacktivism is often associated with groups such as "Anonymous" and "LulzSec."

Why is North Korea attracted to cyber capabilities?

Regardless of what we actually know for certain about what North Korea is or is not doing in cyberspace, it is not difficult to conclude that the country's leadership would find it hard to resist the temptation to develop and invest in offensive cyber capabilities.

Cyber power is attractive to an entire spectrum of actors, be they large nation states, or small non-state actors, primarily because of its low relative cost, high potential impact and the general lack of transparency that surrounds it. There is still a great deal of difficulty in identifying the perpetrator of a cyber attack, so therefore, it becomes easier to avoid retaliation and in North Korea's case, further sanctions from the international community. Powerful actors can combine cyber power with existing military capabilities, and economic assets. Less

powerful actors — states, organisations and individuals, can gain asymmetrically in cyberspace by inflicting extensive damage on vulnerable targets. For a relatively small investment, networks can be bought down and valuable information stolen and interfered with. Cyber attacks rely on malicious code and highly trained code writers which cost a great deal less to train and deploy than purchasing new conventional forces such as aircraft, ships and missiles. With the North's poor economic situation it cannot hope to compete with the South or the US in building conventional forces, therefore cyber capabilities provide it with a means of asymmetrically lowering the military capability divide. The North Korean military have focused on expanding their asymmetric forces, of which cyber capabilities are one of a number of means by which the North perceives it can overcome the technological superiority of the South. This is a point re-enforced by Kim (2011), who explored a hypothetical scenario of warfare between the North and South:

> It is expected that the North Korean regime will first conduct a simultaneous and multifarious cyber offensive on the Republic of Korea's society and basic infrastructure, government agencies, and major military command centers while at the same time suppressing the ROK government and its domestic allies and supporters with nuclear weapons. If the North succeeds in developing and deploying its EMP weapons, it will be able to paralyze electronic functions as well.[6]

Additionally, despite having extensive military strength in terms of soldiers, tanks and jet aircraft, it is extremely rare that North Korea would have the conditions upon which it could actively deploy them. However, this is not the case with the projection of cyber power, which if used skilfully can have multiple strategic benefits for a nation which is still technically at war with the South, not least of all trying to undermine the reputation of the South as one of the most technologically advanced economies in the world, and the reputation

6. Duk-Ki Kim, "The Republic of Korea's Counter-Asymmetric Strategy," *Naval War College Review*, Vol. 65, No. 1 (Winter 2012), pp. 55-74.

of its politicians to be able to respond effectively to such attacks. This could also weaken confidence in the nation by Alliance partners such as the US. A key motivational factor for North Korea to be developing its cyber capabilities is as an intelligence collection tool. The ability to remotely probe South Korean networks for information that provides insights into the government's thinking on military, security and broader strategic issues is invaluable to North Korean planning. Understanding where vulnerabilities exist in South Korean defences provides valuable intelligence on how the North prepares for potential conflict on the Peninsula.

The benefits of such a capability are magnified considerably when examining the degree to which North and South Korea are dependent upon information technology networks and systems which could be susceptible to attack. South Korea is one of the most connected nations in the world. Following the Asian financial crisis in the late 1990s, South Korea invested heavily in a national broadband infrastructure that provides its citizens with a nation-wide network that carries data at the highest average speeds in the world. Indeed it has led Seoul to be called "the bandwidth capital of the world." In 2010 more than 81 per cent of South Korean citizens had access to the internet and over 16 million of those were subscribed to a broadband service. Over three-quarters of South Koreans use the Internet more than once per day.[7] This unfettered access to a networked society is an enormous enabler for social mobility and economic growth on the one hand, but on the other hand offers malicious actors the ability to penetrate South Korea's networked infrastructure, something that has become increasingly exploited by the North Koreans.

North Korea is the polar opposite to its neighbour, as one of the most unconnected nations in the world, and it does not have access to the same degree of advanced technology as the South. It is unusual for a North Korean citizen to have access to the Internet, and in many respects is the preserve of the elite. It has only three Internet service

7. Robert Deibert, et al (Eds), *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (Massachusetts Institute of Technology, 2012).

providers and in terms of Internet access, it ranks as one of the lowest nations in the world. Compounding the issue further, North Korea has an electricity supply that is unreliable and susceptible to regular power cuts.[8] Therefore, whilst a lack of access to the Internet presents many challenges to social and economic development, the advantage of this situation for the North is that there are fewer vulnerabilities that can be exploited by a cyber attack. This means that cyber attacks can provide them with an asymmetric advantage in their confrontations with the South, an advantage that it seems they are increasingly willing to exploit, placing increased focus on developing their cyber capabilities.

These factors have been noted by senior military figures in the region, who have grown ever more concerned at the increasing level of malicious cyber activity emanating from North Korea. In 2012 Army General James Thurman, the commander of US Forces Korea, presenting to the US House Armed Services Committee's annual regional overview of the region, stated that:

> North Korea employs sophisticated computer hackers trained to launch cyber infiltration and cyber attacks…. Such attacks are ideal for North Korea [as they can be done anonymously] … and they have been increasingly employed against a variety of targets including military, governmental, educations and commercial institutions.[9]

Such a statement from a senior US military commander, with such a level of experience of strategic military issues on the Peninsula, provides us with a clear indicator that North Korea is progressing in its development of cyber capabilities, and is willing to use them.

---

8. James A Lewis, *Speak Loudly and Carry a Small Stick: The North Korean Cyber Menace*, 2010, http://38north.org/2010/09/speak-loudly-and-carry-a-small-stick-the-north-korean-cyber-menace/.
9. Tony Capaccio, *North Korea Improves Cyber Warfare Capacity, U.S Says*, Bloomberg Businessweek, 2012, http://www.businessweek.com/news/2012-10-22/north-korea-improves-cyber-warfare-capacity-u-dot-s-dot-says.

What is the Historical Context to North Korea's Development of Cyber Capabilities?

Since the 1970s, the North Korean Military has developed and maintained a degree of electronic warfare capability as part of an effort to improve its asymmetric capabilities against the South.[10] However, it is thought that this area of capability was rapidly expanded following strategic reviews that took place in the country following Operation Desert Storm in the early 1990s. Here the US demonstrated not only its vast military superiority to a largely Soviet-equipped military but also its capacity for a new, different kind of warfare. Computers and other high-end technology provided real-time intelligence and enabled its array of smart weaponry. North Korean assessments in this area were not dissimilar to close ally China who was also attempting to understand how to transform its military capabilities in order to counter such threats.[11] This led the North Korean military to establish an information warfare (IW) capability under the concept of "electronic intelligence warfare (EIW)." This included an introduction of more modern electronic intelligence gathering equipment, jammers and radars.[12]

However, North Korea's more modern approach to cyber operations began towards the end of the 1990s when *Unit 121* (which will be discussed below) was reportedly established within the Reconnaissance Bureau of the General Staff Department with the purview to undertake offensive cyber operations.

---

10. Kim, *Op. cit*., p. 57.
11. Tobias Feakin, *Enter the Cyber Dragon: Assessing Chinese Intelligence Agencies' Cyber Capabilities*, ASPI Special Report, June 2013, http://www.aspi.org.au/publications/publication_details.aspx?ContentID=361.
12. International Institute for Strategic Studies, "Chapter Six: Asia," *The Military Balance*, Vol. 113, No. 1 (2013), pp. 245-352.

A Focus on Education

Part of North Korea's focus in developing its cyber capabilities has been to concentrate heavily on the educational process of training its citizens from a young age. It has been reported, largely sourced from those that have defected from the North, that the regime begins looking for talented children whilst they are still in primary education. Since the mid-1990s there have been many elite middle schools established across the country in an attempt to find the most talented students from across the nation, spreading the net wider than just in Pyongyang. Talented students who graduate at the top of their classes at the age of twelve/thirteen and who demonstrate higher levels of ability in science and maths are selected and then enrolled in the elite First and Second Geumseong Senior-Middle Schools in Pyongyang.[13] These children are taken through a six-year program at the school, at which time the most talented are then placed into either Kim Il-sung University, Kim Chaek University of Technology or the Command Automation University (formerly known as Mirim University), all of which are based either in Pyongyang or Hamheung.[14] Training at these institutions which is thought to include lessons in programming, command automation, computerised calculation, technical reconnaissance and cyber warfare, lasts for up to five years. Top graduates are sent to join military units within the General Bureau of Reconnaissance or the General Staff of the Korean People's Army (KPA) or sent abroad for further training to gain increased levels of practical experience.[15]

13. Kim, *Op. cit*., p. 67.
14. Sangwon Yoon, "North Korea Recruits Hackers at School," *Al Jazeera*, 2011, http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html.
15. Kim, *Op. cit*., p. 67.

Playing the Numbers Game: Estimating the Size of North Korean Cyber Capabilities

It is difficult to place exact numbers on the number of personnel who are involved in North Korea's cyber activities. Reports vary widely from estimates of a couple of hundred to tens of thousands of personnel directly attached to military efforts to project North Korean cyber power.[16] It is understood that their efforts in this area are concentrated in three different groups. The Central Party Investigative Group is responsible for technical education and training and the 204th Unit of the Operations Department, Unification Bureau, owns cyber-based psychological operations. But the final and most prominent cyber organisation is the General Staff Reconnaissance Bureau, North Korea's key intelligence agency. Lying under its purview is the secretive 121st Unit. The 121st Unit was originally only a specialist unit within the wider Staff Reconnaissance Bureau, but in 2008 was elevated in status, becoming its own department within the Bureau. Known as *Unit 121*, the group has been increasingly named in media sources for its role in alleged attacks on South Korea. Its core missions are to infiltrate computer networks, hack classified information and place viruses into targeted networks.[17] The number of personnel within the organisation varies depending on the source. Kim (2011) estimates that the group has approximately 300 personnel;[18] in 2010 Won Sei-hoon, then chief of South Korea's National Intelligence Service, put the number of professional hackers in North Korea's cyber warfare unit at 1000.[19] However, others have suggested that this group has rapidly swollen in numbers to around 3000 people.[20]

---

16. Ward Carrol, "Inside DPRK's Unit 121," *Defensetech*, December 2007, http://defensetech.org/2007/12/24/inside-dprks-unit-121/.
17. Kim, *Op. cit*., pp. 67-68.
18. Kim, *Op. cit*., p. 68
19. Youkyung Lee, "North Korea Cyber Warfare: Hacking 'Warriors' Being Trained in Teams, Experts Say," *Huffington Post*, March 24, 2013, http://www.huffingtonpost.com/2013/03/24/north-korea-cyber-warfare-warriors-trained-teams_n_2943907.html.

Regardless of the size of the organisations involved, there is clear intent from the North Korean leadership to exploit this capability increasingly over the coming years. Lieutenant General Bae Deukshin, chief of the Defence Security Command in the South Korea Army, was quoted publicly stating:

> North Korea is strategically nurturing its cyber warfare unit…. This unit has shown the potential for attacks that are larger in scale and more intelligent by pinpointing a specific target…. In the future, North Korea will try to cause social confusion and inflict significant national damage through an intensive cyber attack.[21]

So whilst it is difficult to put exact figures on the number of people involved in North Korea's cyber activities, there is sufficient evidence to illustrate that they possess growing capability, both in terms of size and sophistication. The level of sophistication involved has increasingly been revealed through private sector-led forensic reports released during the course of 2013.

The Growing Evidence of North Korean Attacks on the South

One of the features of any cyber attack is that attributing who was specifically to blame with any certainty can be a challenging process, especially when the ramifications of any public blame can have serious geopolitical impact. However, over the past year we have seen an increasing number of incidences where nations have decided to "call out" those they feel are responsible, most notably at the beginning of the year when senior US politicians publically announced their requests for China to reign in its cyber espionage activities.[22]

---

20. Vantage Point, "Developments in North Korea," *Vantage Point*, Vol. 34, No. 8 (August 2011), p. 5
21. *Ibid*.
22. Tobias Feakin, "Cyber Goes Strategic," *The Strategist*, March 19, 2013, http://www.aspistrategist.org.au/cyber-goes-strategic/.

In regards to North Korean attacks in cyberspace, as James Lewis of the Center for Strategic and International Studies stated in testimony given to the US House of Representative Committee on Foreign Relations, North Korea is a source of turbulence and an irritant to both the US and China. Although confirmable intelligence is sparse, so far most North Korean activity seems to have been directed against South Korea.[23]

Supporting this view is a number of detailed investigations that have emerged in the past year from the private sector. These reports have begun to provide a higher granularity of evidence that North Korea is the source of recent attacks on South Korea, which in the past did not exist. The following section examines some of these key attacks that have taken place and explores the evidence that is being provided by companies such as Symantec, Kaspersky Labs and MacAfee. The analysis that they have provided does not give irrefutable evidence that that North Korea is the main source of the attacks, yet they leave little doubt that it is the main culprit, and that its capabilities are being developed rapidly. Perhaps the most interesting aspect of this reporting is the linkage made between North Korea and a barrage of increasingly aggressive attacks on South Korea, carried out over a four-year period, which will now be examined.[24]

Operation Troy - A Four-Year Cyber Espionage Campaign?

South Korea has suffered from a number of high-profile cyber attacks over the past four years that have increased in both frequency and sophistication. At first these were considered separate attacks, emanating from two groups who appeared to have no previous connection, the *New Romantic Cyber Army Team* and the *Who is Hacking Team*.

---

23. House of Representatives Subcommittee on Asia and the Pacific, *Op. cit*.
24. Mark Clayton, "In Cyberarms Race, North Korea Emerging as a Power, Not a Pushover," *The Christian Science Monitor*, October 19, 2013, http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover.

However, evidence prepared by Symantec and McAfee began linking the various attacks, and suggested that they were part of a sustained cyber espionage campaign by North Korea. McAfee dubbed the attacks "Operation Troy."[25] [26]

Recent analysis pinpoints the starting point of the campaign at around 2009 when a series of coordinated Distributed Denial of Service (DDoS) attacks were carried out against South Korean and US targets. These attacks clogged up the websites of White House, the Pentagon, the Blue House, the Korean Ministry of Defense, the Ministry of Public Administration and Security, the National Intelligence Service and the National Assembly over a period of six days. Further attacks targeted major South Korean banks, such as the Shinhan bank, Korea Exchange bank plus the New York Stock Exchange and the top internet portal in South Korea, Naver.[27]

Attacks continued through the course of 2010, including attacks routed through Chinese-based servers against South Korean government websites,[28] and these were quickly blamed on North Korea by the South Korean government. In March 2011 a larger-scale DDoS attack began which targeted 40 South Korean websites affiliated with the government, military and critical infrastructures as well as the network of US Forces Korea and the US Air Force Base in Kunsan,

---

25. Ryan Sherstobitoff, Itai Liba & James Walter, *Dissecting Operation Troy: Cyberespionage in South Korea*, McAfee White Paper, 2013, http://blogs.mcafee.com/mcafee-labs/dissecting-operation-troy-cyberespionage-in-south-korea.
26. The name "Troy" actually comes from repeated citations of the ancient city found in the compile path strings of the malware. The primary suspect group in these attacks is the New Romanic Cyber Army Team that makes significant use of Roman terms in their code. The McAfee Labs investigation into the Dark Seoul incident uncovered a long term domestic spying operation operating against South Korean targets all based on the same code base.
27. Matthew Weaver, "Cyber attackers target South Korea and US," *The Guardian*, July 8, 2009, http://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack.
28. Agence France-Presse, "South Korean Government Website Hit by Cyber Attacks," *AFP*, June 9, 2010, http://www.google.com/hostednews/afp/article/ALeqM5j-cLHwEp033Jo3lRnOJSFM9L3z6Q.

South Korea. This attack closely resembled the DDoS attacks of 2009. Analysis conducted by McAfee on the attacks, which became known as "Ten Days of Rain," led them to determine that there was "strong evidence to conclude that both attacks had originated from the same adversary."[29] Their analysis of the malware showed a level of sophistication that they felt was not usually a feature of these types of attack, should it have been written by a criminal group, and lent itself more to an effort of espionage. The malware had clearly defined targets and a ten-day limitation on its operational lifespan. Once this deadline had passed, it wiped the hard drives of the host computer it was resting on, complicating forensic analysis, ensuring the discovery of the attackers would be problematic. The report's conclusions for the potential motivation of the attackers bore a stark warning:

> This may have been a test of South Korea's preparedness to mitigate cyber attacks, possibly by North Korea or their sympathizers. While the code and botnet architecture were advanced, the attack itself was very limited and may have been utilized to test and observe how quickly the attack would be discovered, reverse engineered, and mitigated. Armed with this knowledge, the aggressor could launch cyber attacks, possibly in conjunction with kinetic attacks, with a great understanding of South Korea's incident response capabilities. As such, the attacks could better understand their own requirements for a successful campaign.[30]

Throughout 2012, the attacks continued. The conservative paper *Joong Ang Ilbo* and its sister paper were targeted, their photo and article databases were destroyed, and their websites temporarily shut down. This come only a week after North Korea had threatened the paper and other media outlets in the South over their reporting of the North.[31]

---

29. McAfee, *Ten Days of Rain: Expert Analysis of Distributed Denial-of-Service Attacks Targeting South Korea*, 2011, http://blogs.mcafee.com/mcafee-labs/10-days-of-rain-in-korea.
30. *Ibid*.
31. "South Korean Paper Hit by Major Cyber Attack," *The Sydney Morning Herald*,

This year a cyber attack took place on 20th March known as "Dark Seoul." It targeted South Korean banks and three TV stations and caused significant damage as it deleted tens of thousands of computers' Master Boot Record (MBR), leaving the computers disabled.[32] The evidence from this incident led McAfee to conclude that a majority of the attacks from 2009 shared a similar motivation, state-led espionage from the North.[33] Symantec had concluded that these attacks had required "intelligence and coordination" and that they expected the attacks to continue "regardless of whether the gang is working on behalf of North Korea or not, the attacks are both politically motivated and have the necessary financial support to continue acts of cyber sabotage on organizations in South Korea."[34]

It now appeared from the evidence base that a single group was responsible for the attacks from 2009 onwards, not multiple groups as was claimed in the press. This group had "designed a sophisticated encrypted network designed to gather intelligence on military networks."[35]

"Kimsuky" Campaign

In September 2013, the Kaspersky Lab published findings from a six-month investigation they had been conducting into an extensive cyber espionage campaign against 11 South Korean, and two Chinese organisations. Named the "Kimsuky" Campaign after the drop box mail accounts registered in the name of "*kimsukyang*" and "*Kim asdfa*"

June 12, 2012, http://www.smh.com.au/it-pro/security-it/south-korean-paper-hit-by-major-cyber-attack-20120611-206pf.html.

32. The MBR is necessary for a computer to start up or 'boot' up.
33. Ryan Sherstobitoff, Itai Liba & James Walter, *Op. cit*.
34. Symantec, *Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War*, June 26, 2013, http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war.
35. Ryan Sherstobitoff, Itai Liba & James Walter, *Op. cit*.

used in the attacks, Kaspersky Lab researchers discovered an unsophisticated but extensive and highly targeted campaign against predominantly South Korean military think tank targets. There were a number of malicious programs involved in the campaign, and there were modules for performing keystroke logging, directory listing collection, document theft, remote control download and remote control access.[36]

The report's writer states that it's difficult to identify with one hundred per cent certainty that the attacks originated in North Korea, but there were a number of indicators that led the researchers to conclude that it was the most likely suspect. Firstly were the targets themselves, which included the Korea Institute for Defense Analyses (KIDA) who research various defence related issues, the Sejong Institute which researches national security strategy as well as other regional security matters, and the Ministry of Unification which is a government department responsible for pursuing inter-Korean cooperation and dialogue.[37] All of these targets would be of direct interest to the North Korean government, as the work they conduct gives a good insight into the direction of South Korean strategic thinking. The second piece of evidence were the IP addresses used for the attacks, all of which rested in the range of the Jilin Province Network and Liaoning Province Network in China, both of which are adjacent to North Korea on the border. As Tarakanov states:

> … the ISPs providing Internet access in these provinces are also believed to maintain lines into North Korea. Finally, this geo-location supports the likely theory that the attackers behind Kimsuky are based in North Korea.[38]

---

36. Dimitry Tarakanov, *The 'Kimsuky' Operation: A North Korean APT?*, Securelist, September 11, 2013, http://www.securelist.com/en/analysis/204792305/The_Kimsuky_Operation_A_North_Korean_APT.
37. *Ibid*.
38. *Ibid*.

What are the Results of these Attacks?

In a speech in the South Korean Parliament in October 2013, Member of Parliament Chung Hee-soo attempted to put a financial cost on this period of attacks on the South. He stated that the financial cost of the 2013 attacks, which he accused North Korea of conducting, had caused 800 billion won (US$750 million) of economic damage. To rectify the damage of the 2009 DDoS attacks had cost 50 billion won (US$47 million) and the 2011 attacks had cost another 10 billion won (US$9.5 million) to clean up.[39] Clearly the economic costs of these attacks are severe, and a continual stream of high-level attacks will lead to these costs increasing, but perhaps of more importance for business and government is the reputational damage that they cause. This is especially the case if it is perceived that they are not doing enough to mitigate against such threats. Regardless of whether North Korea has been directly responsible for the attacks on the South, the high-profile nature of the attacks has forced the South Korean government to take action to reassure the public, its trading partners and allies that they are not a "soft" target.

South Korean Government's Cyber Security Response

All governments experience difficulty in creating comprehensive responses to cyber attacks and creating cyber resilience across all sectors within its borders. Arguably no one country has achieved complete success in this area. However, the most effective responses and policies will harness the capabilities across government, incorporate the private sector address public concerns about privacy and civil liberties, and coordinate them in a way that enables effective response to high-tempo cyber emergencies.

---

39. Alex Hern, "North Korean 'Cyberwarfare' Said to have Cost South Korea £500 Million," *The Guardian*, October 16, 2013, http://www.theguardian.com/world/2013/oct/16/north-korean-cyber-warfare-south-korea.

South Korea's mechanisms for responding to cyber incidents have developed a great deal over the past 15 years. In 2000, triggered by a large scale DDoS attack and the global media attention it received, the Cyber Terror Response Center (CTRC) of Korea National Police Agency was established. In the national defense sector, a Cyberspace Command was established in January 2010 to carry out planning, implementation, training, and research and development for its cyberspace operations and it currently serves under the direct control of the Ministry of National Defense.[40]

Following the spate of DDoS attacks in 2011, and in an effort to further coordinate across government efforts, the Korea Communications Commission (KCC) announced in 2011 a national cyber security master plan established with the joint effort of fifteen government agencies. According to KCC, cyberspace will be considered another operational domain like the nation's territories on land, air and sea that needs a state-level defence system.

Under the master plan, the National Cyber Security Centre (NCSC), run by the National Intelligence Service (NIS), the country's intelligence agency, serves as the control tower to coordinate efforts against cyber attacks among government agencies.[41] The NCSC is the centre point of government for identifying, preventing and responding to cyber threats, and looks to coordinate with the private sector in responding to security incidents and protecting critical national infrastructure. Under the Director of the National Intelligence Service, the National Cyber Security Strategy Council oversees the establishment and improvement of the national cyber security infrastructure, the coordination of policy and roles among government, military and private institutions and deliberating measures and policies related to presidential orders.[42] The efforts of the South Korean government to join

40. Japanese Ministry of Defense, *Defense of Japan 2012 White Paper*, http://www.mod.go.jp/e/publ/w_paper/2012.html.
41. Adrienne Valdez, "South Korea Outlines Cyber Security Strategy," *Asia Pacific Future Gov*, August 13, 2011, http://www.futuregov.asia/articles/2011/aug/13/south-korea-outlines-cyber-security-strategy/.
42. Japanese Ministry of Defense, *Op. cit*.

up its various programmes of work have clearly been substantial, especially over the past four years. However, the test of the new cyber master plan will be how it enables true cooperation across government and the private sector and how it enables links with international partners.

There is already evidence that cyber issues are becoming an increasingly important element of South Korea's discussions with its key strategic ally, the US. Indeed at the 43rd Republic of Korea-United States Security Consultative Meeting (SCM) in 2011, the respective Defence Ministers announced in the official communique:

> The Minister and the Secretary affirmed the need to strengthen cooperation with respect to protection of, and access to, the space and cyberspace domains, and to promote the resilience of critical infrastructure, including the security of information and space systems. The Minister and the Secretary committed themselves to discuss new ways for the ROK and the United States to confront the challenges posed by increasing threats in cyberspace and welcomed the establishment of a bilateral strategic policy dialogue on cyber-security issues. They also acknowledged that effective bilateral cooperation on cyber-security would require a "whole-of-government" approach and coordination with the private sector.[43]

This was further reinforced at the following meeting in Washington DC in 2012 where increasing cooperation on cyber issues was high on the agenda, and it was announced that a number of joint cyber policy consultations between the two nations would take place which would have a whole of government approach, incorporating a wider range of bodies, including the private sector. There is no doubt that South Korea views this increase in cooperation as a response to the threat from North Korea. As was noted by the then Korean Foreign Minister Kim in 2012 at a meeting with his US counterpart: "We also agreed to promote bilateral cooperation regarding North Korea, just as Secretary

43. United States Forces Korea, *Joint Communique of the 43rd US-ROK Security Consultative Meeting*, 2011, http://www.usfk.mil/usfk/%28S%28c320cgglsyvgh4twc4estb3v%29%29/article.aspx?id=920.

Clinton mentioned, against cyber security threats, and will in this regard launch a whole-of-government consultative body."[44]

Clearly South Korea has prioritised the international dimensions of cyberspace as a national priority as was demonstrated by the hosting of the third international conference on cyberspace in October 2013. The process was initiated in 2011 by the UK Government to begin a dialogue on internationally shared principles in cyberspace and outline an agenda for a secure, resilient and trusted global digital environment. This major conference process attempts to bring together stakeholders from across the public, private and civil-society to discuss how to create "rules of the road" for the future of cyberspace. President Park Geun-hye gave the opening address of the conference and stated that:

> As the Internet environment develops, threats to cyberspace security such as leakage of personal information, spam and malicious codes are growing…. We need to build together international regulations and principles to prevent such risk while guaranteeing the open nature of cyberspace.[45]

This top-level endorsement and commitment from the South Korean leadership assisted in the formation of a framework document with a set of six agreed outcomes in the areas of economic growth and development, social and cultural benefits, cyber security, international security, cybercrime, and capacity building.[46] This was no easy task due to the difficulties in resolving the polarised opinions between the

---

44. Hillary Rodham Clinton, Leon Panetta, Kim Sung-Hwan and Kim Kwan-Jin, *Remarks with Secretary of Defense Leon Panetta, Korean Foreign Minister Kim Sung-Hwan and Korean Defense Minister Kim Kwan-Jin After Their Meeting*, June 2012, http://www.state.gov/secretary/rm/2012/06/192400.htm.
45. Seo-Ji-Eun, "Park Speaks at Seoul Cyberspace Conference," *Korea Joongang Daily*, October 18, 2013, http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2979058&cloc=joongangdaily|home|newslist1.
46. *Seoul Conference on Cyberspace 2013*, "Seoul Framework for and Commitment to Open and Secure Cyberspace," http://www.seoulcyber2013.kr/en/references/references_2013.do.

key nations involved in this debate, and demonstrates that South Korea has a role to play in the international aspects of cyber security. However, it is closer to home within its immediate geographical region where South Korea faces the greatest risks should a cyber attack lead to misinterpretation or miscalculation.

Potential for National and Regional Destabilisation

At present the primary concern for South Korea is not so much the kinetic damage that cyber attacks could directly inflict on the Peninsula, the disruption to services and financial cost of such attacks create reputational damage, but they are not catastrophic. The more pressing concern is that these persistent attacks will act as a further destabilising factor in an already precarious situation, one where nuclear weapons are a factor to consider. This final section will examine the implications of persistent cyber attacks on South Korea, both at the national level and within the region it sits.

South Korea is in a strong economic situation, boasting one of the world's most technologically advanced economies, with a well-developed broadband infrastructure and a strong digital economy across the public and private sectors. However, as discussed in this paper, this highly networked economy brings increased vulnerabilities that are being exploited in cyber attacks. There are various consequences for South Korea. The most important of which is the reputational damage economically, politically and internationally that accompanies appearing vulnerable to cyber attacks. As outlined in the previous section there was a significant cost to the South Korean people suffered by the cyber attacks in 2013, absorbing these kinds of costs on a regular basis is not catastrophic, but the damage it does to potential economic investor perceptions is grave. Given the choice it could mean that investors decide to take their money elsewhere, leading to longer-term damage to the South Korean economy, a trend clearly advantageous to the North. Politically South Korea has responded by having set up extensive policy and operational responses to the

attacks. However, this does not mean that the government will be entirely buffered from political damage from malicious cyber activity and the North will continue to probe South Korea's networks and attempt to embarrass and undermine the government. This situation is not assisted by the current scandal encompassing members of South Korea's Cyberwarfare Command, where four officials were accused of posting political messages online during 2012's general election in support of the now President Park Geun-hye.[47] The mixed public and media perceptions of the agency and its activities could provide an opportunity for the North to exploit the situation and conduct further malicious cyber activity to undermine the credibility of the government.

A final area of reputational damage is in South Korea's international security relationships, especially with larger allies, particularly the US. Persistent cyber attacks on South Korean government networks, especially those which contain intelligence data important to military and security operations, could lead to allies who are unwilling to share sensitive intelligence data with them. If the risk of that data being compromised is perceived to be too high, then allies could be increasingly hesitant to facilitate such arrangements. However, through increased capability support and dialogues with allied partners, these fears can be mitigated. Certainly the North Korean regime's willingness to carry out attacks on the US military systems of the Peninsula and beyond does not assist in undermining intelligence sharing; it acts to strengthen cooperative resolve to counter the threat.

Conclusion

When dealing with a leadership as predictably aggressive as North Korea, there is a concern that Pyongyang does not have the ability to accurately calculate the risk that a cyber attack entails, leading to

47. Choe Sang-Hun, "Investigators Raid Agency of Military in South Korea," *The New York Times*, October 22, 2013, http://www.nytimes.com/2013/10/23/world/asia/south-korean-military-agencys-headquarters-raided-in-growing-scandal.html?_r=0.

undesired or unexpected escalatory reactions from the South.[48] Its willingness to perpetrate acts of aggression without regard for the consequence has been demonstrated many times. Whether it be the sinking of a South Korean Naval vessel, Cheonan, killing 46 sailors in 2010[49] or the intentional GPS jamming of hundreds of civilian aircraft flights, and navigation systems on South Korean coast guard craft, fishing boats and passenger vessels during 2012.[50] Therefore, if the North can "get away" with other potentially more serious actions they may believe a cyber attack wouldn't warrant much consideration or consequence.

Added to the unpredictability of the North Korean mindset is the unpredictability of actors in cyberspace. Cyberspace allows a great deal of deniability, with absolute proof on who perpetrated acts often difficult to ascertain, this additional layer of complexity is not helpful in easing tensions between two confrontational nation states. With such a politically charged situation existing on the Peninsula, it is of no comfort that so called hacktivists group, *Anonymous* attempted to become embroiled in the situation by trying to hack into North Korean systems in 2013.[51] The effort reportedly failed, but when added to the internal hacktivist activity in South Korea directed both at North and South Korean government websites, it is clearly an unwelcome additional factor to have to manage, and has the potential to initiate an escalation from either side if the attacks are perceived to have originated from respective government sources.[52]

---

48. James A. Lewis, "Testimony to the Subcommittee on Asia and the Pacific House Foreign Affairs Committee," *Asia: The Cybersecurity Battleground*, July 23, 2013, http://csis.org/testimony/asia-cybersecurity-battleground.
49. *BBC News*, "North Korea Torpedo' Sank South's Navy Ship," May 20, 2010, http://www.bbc.co.uk/news/10129703.
50. Bruce E. Bechtol, "Developments in the North Korean Asymmetric Threat: Missiles and Electronic Warfare," *International Journal of Korean Studies*, Vol. XVI, No. 2, 2012.
51. Max Fisher, "Hacker Group Anonymous no match for North Korea," *The Washington Post*, June 27, 2013, http://www.washingtonpost.com/blogs/worldviews/wp/2013/06/27/hacker-group-anonymous-is-no-match-for-north-korea/.

Nigel Inkster (2013) has suggested that the actions that North Korea took in its recent nuclear testing activity could have prompted the prospect of China being drawn into direct conflict with the United States as a result of North Korea's "provocative and irresponsible" behaviour. He suggests that this behaviour could equally manifest itself in cyberspace:

> … It is not hard to imagine circumstances in which a South Korean cyber attack or activity by an entity like Anonymous — which North Korea might interpret as ventriloquised by the US government — elicits a response which escalates into a North Korean cyber attack, seemingly emanating from China, against US critical infrastructure. Such escalation would appear to cross a US "red line" — with unpredictable consequences.[53]

This concept of the cascading effects of actions taken by a power such as North Korea, which cares little about the ultimate impact of what it does, demonstrates how seriously the international community should take North Korea's activity in cyberspace. Unchallenged and unmanaged continued malicious activity by North Korea in cyberspace has the very real potential to exacerbate the situation on the Peninsula and lead to kinetic conflict.

Regardless of what we know precisely in terms of the size of North Korean cyber capabilities, recent evidence explored in this paper illustrates a growing North Korean cyber capability, and a willingness to use it alongside its other traditional sabre-rattling tactics of low-level military attacks and strong rhetoric. The ability of South Korea to respond to these incidents as they arise without escalation taking place will be yet another challenge for strategic planners to consider on the Peninsula. The onus is on the South to develop an ever more sophisticated and mature cyber policy architecture and cyber resilience

---

52. Soo-Kyung Koo, "Cyber Security in South Korea: The Threat Within," *The Diplomat*, August 19, 2013, http://thediplomat.com/2013/08/19/cyber-security-in-south-korea-the-threat-within/.
53. Nigel Inkster, "Conflict Foretold: America and China," *Survival*, Vol. 55, No. 5, October-November 2013, pp. 7-28.

framework in order that in the face of extreme cyber provocation they can remain resilient in absorbing such attacks and, most difficult of all, remain clearheaded in their responses so it does not become a precursor to large-scale military action.

■ **Article Received: 11/5** ■ **Reviewed: 11/8** ■ **Revised: 12/11** ■ **Accepted: 12/13**

Bibliography

BBC. North Korea torpedo sand South's navy ship. *BBC News*. May 20, 2010.

Bechtol, B. E. Developments in the North Korean Asymmetric Threat: Missiles and Electronic Warfare. *International Journal of Korean Studies*, Vol. XVI, No. 2, 2012.

Capaccio, T. *North Korea Improves Cyber Warfare Capacity, US Says*. Bloomberg Businessweek, 2012.

Carrol, W. Inside DPRK's Unit 121. *Defensetech*, December 2007.

Clayton, M. In Cyberarms Race, North Korea Emerging as a Power, Not a Pushover. *The Christian Science Monitor*, October 19, 2013.

Defense, J. M. *Defense of Japan 2012 White Paper*. Japanese Ministry of Defense, 2012.

Deibert, R. P. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. Massachisetts Institute of Technology, 2012.

Feakin, T. Cyber Goes Strategic. *The Strategist*, March 19, 2013.

Feakin, T. *Enter the Cyber Dragon: Assessing Chinese Intelligence Agencies' Cyber Capabilities*. Australian Strategic Policy Institute, 2013.

Fisher, M. Hacker Group Anonymous no match for North Korea. *The Washington Post*, June 27, 2013.

France-Presse, A. South Korean government website hit by cyber attack. *AFP*, June 9, 2010.

Herald, T. S. South Korean Paper Hit by Major Cyber Attack. *SMH*, June 12, 2012.

Hern, A. North Korean 'Cyberwarfare' Said to have Cost South Korea 500 million. *The Guardian*, October 16, 2013.

Hillary Rodham Clinton, L. P.-H.-J. *Remarks with Secretary of Defense Leon Panetta, Korean Foreign Minister Kim Sung-Hwan and Korean Defense Minister Kim Kwan-Jin After Their Meeting*. US State Department, 2012.

House of Representatives Subcommittee on Asia and the Pacific, C. o. *Aisa the Cyber Security Battleground*. Washington DC: US Government, 2012.

Inkster, N. Conflict Foretold: America and China. *Survival*, Vol. 55, No. 5 (October-November, 2013), pp. 7-28.

Kim, D.-K. The Republic of Korea's Counter-Asymmetric Strategy. *Naval War College Review*, Vol. 65, No. 1 (2012), pp. 55-74.

Koo, S.-K. Cyber Security in South Korea: The Threat Within. *The Diplomat*, August 19, 2013.

Korea, G. o. Seoul Framework for and Commitment to Open and Secure Cyberspace. *Seoul Conference on Cyberspace 2013*.

Korea, U. S. *Joint Communique of the 43rd US-ROK Security Consultative Meeting*. US Government, 2011.

Lee, Y. North Korea Cyber Warfare: Hacking 'Warriors' Being Trained in Teams. *Huffington Post*, March 24, 2013.

Lewis, J. A. *Speak Loudly and Carry a Small Stick: The North Korean Cyber Menace*, 2010.

Lewis, J. A. *Testimony to the Subcommittee on Asia and the Pacific House Foreign Affairs Committee*. US Government, 2013.

McAfee. *Ten Days of Rain: Expert analysis of distributed denial-of-service attacks targeting South Korea*. McAfee, 2011.

Point, V. Developments in North Korea. *Vantage Point*, Vol. 34, No. 8 (2011).

Ryan Sherstobitoff, I. L. *Dissecting Operation Troy: Cyberespionage in South Korea*. McAfee White Paper, 2013.

Sang-Hun, C. Investigator Raid Agency of Military in South Korea. *The New York Times*, October 22, 2013.

Seo-Ji-Eun. Park Speaks at Seoul Cyberspace Conference. *Korea Joongang Daily*, October 18, 2013.

Sharp, K. M. *America's Cyber Future: Security and Prosperity in the Information Age*. Washington DC: Center for New American Security, 2011.

Studies, I. I. *The Military Balance*. London: IISS 2013.

Symantec. *Four Years of Dark Seoul Cyberattacks Against South Korea Continue on Anniversary of Korean War*. Symantec, 2013.

Tarakanov, D. *The 'Kimsuky' Operation: A North Korean APT?* Securelist, 2013.

Valdez, A. South Korea Outlines Cyber Security Strategy. *Asia Pacific Future Gov*, 2011.

Weaver, M. Cyber Attackers Target South Korea and US. *The Guardian*, July 8, 2009.

Yoon, S. North Korea Recruits Hackers at School. *Al Jazeera*, 2011.