AIR WAR COLLEGE

AIR UNIVERSITY

WHEN NORMS FAIL:

NORTH KOREA AND CYBER AS AN ELEMENT OF STATECRAFT

by

Adam Albarado, CDR, USN

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Panayotis A Yannakogeorgos

06 April 2017

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

CDR Adam Albarado is assigned to the Air War College, Air University, Maxwell AFB, AL. He is a qualified Surface Warfare and Intelligence Officer in the United States Navy with operational tours aboard USS CUSHING (DD 985), USS PINCKNEY (DDG 91) and as a staff officer with Naval Construction Group TWO and Commander SEVENTH FLEET. He was awarded the Rear Admiral Edwin T. Layton award for outstanding mentorship and leadership in 2010 and has served ashore at Joint Intelligence Operations Command, Pacific, and as the Naval Science instructor at Tulane University NROTC. CDR Albarado has a Bachelor of Science in Business and Master of Arts in International Relations from Tulane University.

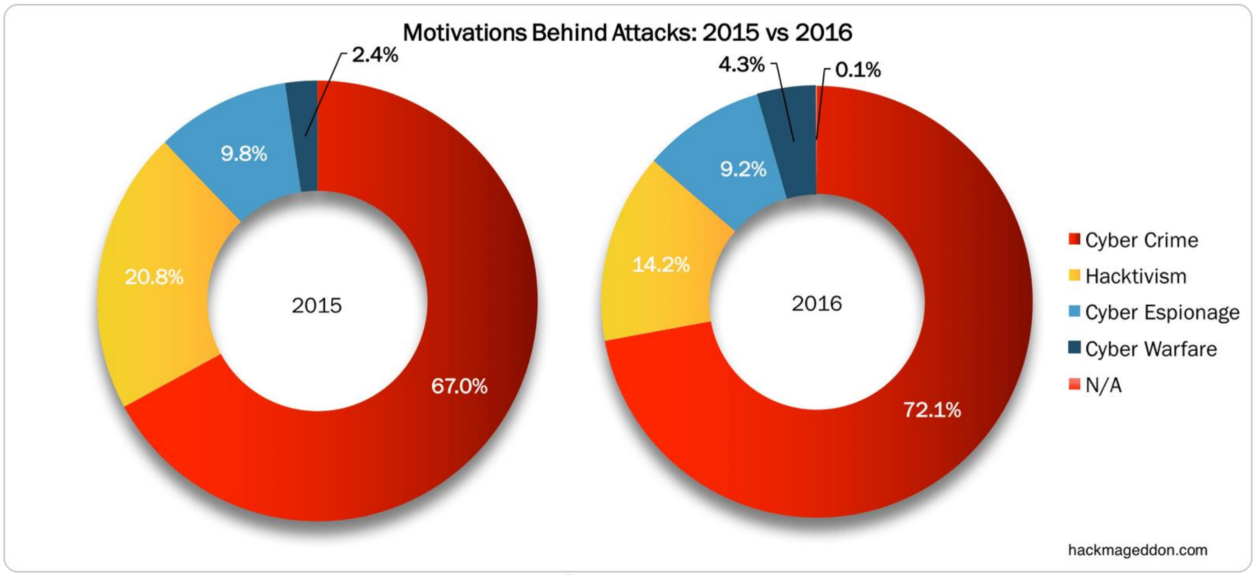
Abstract

With the increased reliance on information technology across society, nation states have begun to integrate cyber capabilities into their power projection strategies. While nation states use these increased cyber capabilities in attempts to wield greater influence in statecraft, cyber tools have not lived up to the hype of the great equalizer some claim it to be. To illustrate, this paper reviews select malicious cyber actions by North Korea in an effort to analyze the effectiveness of cyber as a form of statecraft for weaker states and potential deterrence responses by victims of such malign actions.

Introduction

Cyberspace has become the medium of choice for social and economic interaction around the world. Most elements of national power touch, or are influenced by, the cyber domain. A 2017 U.S. Defense Science Board report recognizes the significant economic, social, and military advantages the U.S. gains from cyberspace. The same report also points out that the "pursuit of these advantages has created extensive dependencies on highly vulnerable information technology and industrial control systems," putting U.S. security at risk.[1]

The U.S. Department of Homeland Security (DHS) estimates that 97 percent of Fortune 500 companies have been hacked.[2] The FBI suspects that only 15 percent of all cybercrime is reported by individuals and businesses and registered over $1B (USD) in losses from cyberattacks in 2015 (see Fig. 1).[3] In addition to cybercrime, cyberspace is increasingly being used by nation states for espionage and warfare. The Internet security statistics site, *Hackmageddon.com*, estimated that 9.2 percent of all cyberattacks in 2016 were attributable to cyber espionage and documented a two-fold rise in events it classified as cyberwarfare from 2015 to 2016.[4] While still a relatively small percentage of overall cyberattacks, states are becoming more active in cyberspace. The U.S. military is particularly vulnerable. It is estimated 98 percent of military communications runs over the civilian owned and operated Internet.[5] The U.S. Department of Defense observed in the *2015 DoD Cyber Strategy* that, "The increased use of cyberattacks as a political instrument reflects a dangerous trend in international relations" and that the U.S. is uniquely vulnerable to such attacks.[6]



(Fig. 1) 2015 vs. 2016 Cyber Attacks[7]

Developing nations, not nearly as reliant upon or connected to the internet, look to cyber to provide them a disproportionate level of influence in international affairs. The lack of established norms for state behavior in cyberspace and the ungoverned nature of the Internet provide states (both weak and strong) a temptation to use cyberspace aggressively, regardless of its potential effectiveness. Some states (e.g. North Korea, Russia) have also shown a willingness to ignore accepted norms if they feel it is in their interests to do so, which casts further doubt on the effectiveness of norms in cyberspace.

Powerful states already use cyber in attempts to coerce and deter actions by other states. Russia is perhaps the most active in this respect. Moscow's actions against Estonia in 2007 and Georgia in 2008 were obvious efforts at coercion and deterrence.[8] In the Georgia case, cyber efforts were accompanied by military force, while Russia paired its cyberattacks with economic actions against Estonia.[9] Both were of limited success in helping Moscow achieve its objectives but support Martin Libicki's finding that cyber is most effective as a support function for other elements of warfare, or state power.[10] More recently, Russia has been suspected of using cyberspace to interfere with the democratic process of U.S. and European elections in violation of sovereignty norms.[11]

While much has been written regarding great nation use of cyber for statecraft, less has been written about the use of cyber by weak and developing nations.[12] This paper will examine notable cyber actions by North Korea to influence international actors and achieve national objectives. North Korean actions will further be compared against models of deterrence and coercion to determine the level of success achieved and concludes with suggestions for U.S. cyber policy as it relates to cyber deterrence. I will demonstrate that cyber can be an effective tool of statecraft for a nation if it can maintain escalation dominance.

When Norms Fail: North Korea and Cyber as an Element of Statecraft

Much like air power at the start of the 20th century, nations are rushing to capitalize on the perceived advantages cyber may offer as an element of national power in today's technologically evolving world. Unlike air power, cyber is, at least theoretically, more readily available to any country, regardless of its overall economic standing. A Center for Strategic and International Studies report showed that, by 2012, 114 of 193 United Nation Member States – almost 60 percent – had national cybersecurity programs, with 47 of those states giving some cyber role to their militaries.[13] Hyeong-Wook Boo and Kang-Kyu Lee suggest, "[Cyber] enables poor countries with the chance to harm the wealthy nation's ICT [Information and Communication Technology] assets at low costs."[14] While it is debatable how much capability "low cost" cyber will provide, such accessibility is assumed to provide weaker states a level of influence heretofore reserved for great powers.

Proponents of cyber as an effective tool of statecraft argue such attacks are ethical because cyber weapons are able to specifically target certain systems to produce desired effects.[15] Opponents of such claims argue that there are too many limitations to its usage for cyber to be truly effective.[16] The reality is that cyber is most effective as an element of statecraft when used in conjunction with a whole-of-government approach to coercion or deterrence where the state maintains escalation dominance. Such capability normally resides with the stronger state. Yet weak states continue using cyber as a tool of statecraft in attempts to coerce and deter adversaries. North Korea (DPRK) is an example of such a country.

In addition to its tepid economy, it is also weak in most other forms of traditional statecraft. I define traditional forms of statecraft as the elements of DIME, i.e. diplomatic, information, military, and economic. The outlier here is that, while most of North Korea's military equipment is outdated, it maintains one of the world’s largest militaries with over one million active duty and eight million reserve personnel.[17] Its artillery holds Seoul, South Korea’s capital, under constant threat of annihilation, making the North’s military a credible threat despite questionable capability in conventional force-on-force engagement. Thus, its military can be used in conjunction with cyber to assist with coercion efforts. While other weak states may not have such military capability, what matters is that there is another element of state power that can be brought to bear.

Another characteristic of North Korean statecraft is its willingness to eschew international norms. One example of this is Pyongyang’s continued nuclear testing in the face of international acceptance of the Nonproliferation Treaty (NPT) and despite multiple United Nations Security Council (UNSC) resolutions intended to punish the DPRK for its nuclear program.[18] Another example is North Korea’s persistent ballistic missile tests, which are also repeatedly condemned and sanctioned by the UNSC.[19] UNSC resolutions are binding to all UN member states, which includes North Korea. However, North Korea continues to ignore such objections to its behavior, weakening arguments that cyber norms can effectively deter state-sponsored cyberattacks and act as a stabilizing influence in cyberspace.[20]

Pyongyang has launched numerous cyberattacks since 2009, with some estimates claiming North Korea perpetrates as many as 250 million cyberattacks per day against South Korean online entities.[21] Given the lack of Internet access to the general population, this activity indicates Pyongyang understands the importance of cyber as an asymmetric alternative and has invested heavily in its cyber warfare proficiency. With an aging military infrastructure and limited sources of national power, the DPRK has used cyber in an effort to exert pressure on stronger, more capable adversaries and retain its global relevance.

North Korea, under the leadership of both Kim Jong-Il and his successor, Kim Jong-Un, has developed cyber capabilities since the 1990s in hopes of building cheaper asymmetric options to use against more powerful adversaries.[22] Before the advent of the Internet, North Korea was limited to conventional military options to support its campaigns of coercion and deterrence, aimed mostly at South Korea. According to the International Telecommunications Union, South Korea had the highest ICT development index (IDI) score, of all 167 countries measured in 2015. With such reliance and integration of all aspects of cyber into the national makeup, South Korea is one of the most vulnerable countries to cyber threats. The U.S. is not far behind at 15.[23]

North Korea stands at the other end of the ICT spectrum. Although sufficient data is not available to calculate a valid IDI score, it is estimated only a handful of elites out of the state's 25 million people have regular Internet access. Such limited connectivity provides North Korea with the advantage of limited cyberattack vulnerability when compared to more powerful nations whose economies and command and control systems are more dependent upon stable and reliable ICT systems.

Despite Seoul's vulnerability to cyberattack, Pyongyang has been unable to translate its cyber aggression against its neighbor into noticeable state benefit. While some DPRK cyber activities arguably fall within a deterrence framework, other actions are better characterized as geopolitical protests or proof-of-concept demonstrations to refine future cyber capabilities. Cyberattacks against South Korea's financial sector and government in 2009, 2011, and 2013 created significant inconvenience for South Korean citizens, erasing bank files for some, and contributing to overall public unease. Although these actions did not result in any obvious concessions to North Korea, they also did not result in effective actions in retaliation against Pyongyang.

Outside of the 2014 Sony Pictures Entertainment (SPE) hack, little has been written regarding possible motives or objectives for some of the more significant attacks over this period. While Pyongyang's persistent cyber aggression likely furthers overall goals associated with the technical state of war between the two neighboring states, cyberattacks offer the North a tool that can be used in peacetime and wartime with little risk of consequence. Since the elevation of Kim Jong-Un in December 2011, the young leader has embarked on a recurring cycle of aggression across various domains in order to stabilize his regime and obtain leverage over the South through coercion and intimidation. The cyberattacks of 2013 and 2014 provide context to draw conclusions regarding Kim Jong-Un's objectives during these events.

Deterrence and Coercion

A conceptual framework of deterrence must be understood in order to grasp the potential effectiveness – or lack thereof – of deterrence in cyberspace for weak states. Simplistically, deterrence, as explained by Robert Pape, aims to persuade an adversary *not* to take a certain action.[24] Such persuasion is accomplished by convincing the enemy that the cost of an action is greater than the cost of not taking the same action. The threat of retribution must be anticipated and avoided by accommodation. The power to punish and the ability to communicate this capability, according to Thomas Schelling make deterrence possible.[25] Liam Nevill and Zoe Hawkins expand upon this by pointing out that states must also establish credibility for deterrence by, "communicating it has the ability, resources, and intent to follow through on the punishment."[26] Without credibility deterrence becomes problematic.

Another example of state limitations on cyber deterrence comes from James Lewis who points out that while the, "United States is widely recognized to have pre-eminent offensive cyber capabilities…it obtains little deterrent effect from this."[27] To illustrate, statements from President Obama at the 2016 G20 Summit acknowledged Russia's continued hacking of the U.S. despite the U.S. "being the best" at offensive cyber.[28] This statement regarding America's pre-eminent cyber capabilities was intended to deter Russia and other state actors from furthering cyberattacks on the U.S. for fear of retribution. Despite this warning from President Obama, Russia continued to hack the U.S. as was evident in the FBI's finding that Russia cyber actor, GRIZZLY STEPPE, attempted to influence the 2016 elections via cyber means.[29] The president's statement also did not deter North Korea from attacking U.S. financial institutions as late as February 2017.[30]

The ability to demonstrate capacity to threaten an adversary's center of gravity or other assets, via cyberspace, that results in a recalculation of costs and benefits is vital to deterrence and difficult for most nations. While major powers like the U.S., Russia, and China are already credited with demonstrating such capacity, smaller, less capable nations risk forfeiting their limited capability through such demonstration. This is because, as pointed out by Yannakogeorgos and Lowther, once a capability is demonstrated against a vulnerability, that vulnerability can be patched and the exploit – or tool – will no longer work.[31] An attack on any system (i.e. any network, program, or ICS) will draw attention to that system where other exploits will be at risk of discovery. Unlike nuclear deterrence, where any warhead is just as effective against a multitude of targets, cyber weapons are usually only effective against a particular system or program. Even if such tools are effective against multiple systems, exposure of the tool could reveal how it can be defended against and is thus maximally effective the first time it is used - if at all.

Deterrence is related to coercion in that it also seeks to influence the decisions of an adversary. Both strategies involve a cost-benefit analysis on the part of the targeted actor. The difference between the two is that deterrence seeks only to prevent an action from being taken while coercion is used to either stop an action already being taken, or persuade an actor to take a course of action that benefits the coercer. Both are applicable to cyberspace.

The threat of punishment is just as much a part of coercion as it is in deterrence. According to Pape, coercion by denial targets the military strategy of the opponent and works by preventing the adversary from achieving its political goals.[32] A denial strategy of coercion is more difficult to pursue from a cyber perspective.

Denial is not to be confused with defense. Today, tech and cyber-related companies spend significant funds toward reducing system vulnerability. This expenditure is more closely related to general defense and security, which guards against a broad spectrum of possible threats that include criminal, accidental, and state-sponsored originations. Denial is targeted to a specific threat and, more importantly, the specific strategy of an adversary. Outside of wartime, such a strategy is usually more difficult to execute because of the multitude of potential threat sources. Denial strategies are generally employed by the targeted actor and is thus of lesser significance to the question here of whether cyber actions undertaken by weaker states can be an effective tool of statecraft.

Another issue with deterrence in cyberspace is attribution. In order for a cyber operation to achieve deterrence or coercion and be considered an effective part of statecraft the victim should know who committed the attack. While the relative anonymity of cyberattacks can act as protection for entities embarking on espionage and illegal activities, this falls outside what is being described here as cyber deterrence and coercion. In the two cases discussed, North Korea was discovered to be behind the attacks. However, it took nearly a month to conclude Pyongyang was the perpetrator and respond accordingly.[33] This lag time necessary to attribute an incident to provide politicians with the necessary information needed to decide an appropriate response can provide a weaker state the necessary time to apply additional leverage or plan a defense but otherwise limits the effectiveness of cyber coercion and deterrence.

Attribution is more important to deterrence methods by punishment than by denial. According to the Defense Science Board (DSB), deterrence by denial is more defense-oriented. As such, denial methods focus on defending systems, information, and networks from attacks. This can occur by making the targeted object resilient to attack or making the cost to whoever is attacking the system enough to make them reconsider the act. Deterrence by punishment (called "deterrence by cost imposition" by the DSB), "requires the ability to attribute with high confidence, the perpetrator(s) of an attack in order to credibly threaten" them or their center of gravity to force a reconsideration of the act.[34]

For weaker states, strategies of coercion and deterrence are desirable but difficult to accomplish. Both types enable the weaker nation to achieve effects by cheaper means than possible via military action. Conversely, coercion and deterrence in cyberspace present their own problems for the weaker state due to the perishable nature of cyber tools, attribution and credibility issues. These issues also exist for the powerful state responding to cyber coercion/deterrence strategies by weaker challengers.

Despite the aforementioned issues that weaken cyber deterrence and coercion strategies for less powerful states, such states also usually lack the full range of resources necessary to successfully execute such strategies. In response to cyber coercion and deterrence strategies from weak states, powerful nations can draw upon elements of national power (i.e. DIME) unavailable to weaker aggressors. The U.S. acknowledged such realities in its 2015 report on cyber deterrence policy that outlined a whole-of-government approach to cyber deterrence as necessary for success in such ventures.[35] The 2017 DSB, *Task Force on Cyber Deterrence* report, also echoes the whole-of-government approach.[36] An overview of the 2013 North Korean cyberattack against Seoul's financial, media, and government sectors and the 2014 SPE attack highlights this requirement. Despite using multiple DIME resources available to Pyongyang, Kim Jong-Un was unable to fully realize coercive and deterrent goals against the U.S. and South Korean governments.

Overview of Notable North Korea Cyberattacks

If press reports are accurate, South Korea is under daily attack from DPRK hacker units.[37] Although North Korea has one of the poorest economies in the world, the reclusive regime maintains 17 cyber warfare organizations comprised of approximately 5,100 personnel who carry out research and development in addition to cyber espionage and cyberattacks against various entities.[38] Since 2009, North Korean hackers have persistently targeted South Korean media, financial, and political institutions.[39]

Pyongyang continues aggressive actions in cyberspace despite being ostracized from the international community and deprived of the economic benefits of globalization. What makes North Korea difficult to defend against is its disregard for international law. This disdain for the international law makes North Korea unpredictable and weakens normal methods of deterrence and coercion. What follows are overviews of two of the more significant North Korean malicious cyber actions. An examination of these events and the responses by international actors lend insights into the effectiveness of cyber as an element of statecraft and potential deterrence responses by the victims.

20 March 2013 DarkSeoul Attack

On 20 March 2013, the networks of three of Seoul's main television broadcasters (KBS, MBC, and YTN), along with three South Korean banks (Shinhan, Nonghyup, and Jeju) were attacked by "DarkSeoul" malware suspected of being distributed by Bureau 121 hackers from North Korea.[40] The attacks resulted in the networks of the affected companies being frozen, with some customers of affected banks being unable to withdraw money from ATMs and news broadcasting crews unable to access computers. Unlike the distributed denial of service (DDoS) attacks South Korea experienced in the past, DarkSeoul malware was specifically designed to defeat popular Korean antivirus software and hit the targeted networks. Notably, all the victimized businesses had been previously cited as potential targets by Pyongyang. It is obvious Kim Jong-Un was trying to send a message. The *New York Times* suggested the North's leader was demonstrating that, "[North Korea] can reach into Seoul's economic heart without blowing up South Korean warships or shelling South Korean islands."[41]

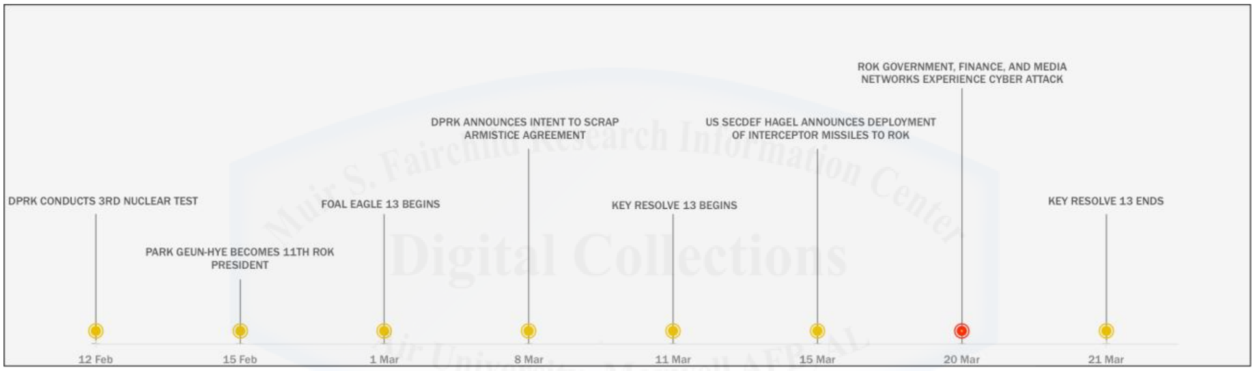
The outages in each affected network only lasted a few hours before bank and computer services were restored. None of the television broadcasters' programming was interrupted.[42] On 10 April 2013, the South Korean government announced North Korea was behind the attack and had evidence the attacks had been planned for at least eight months.[43] While it is ultimately unknown why the 20 March cyberattacks against South Korea occurred, awareness of some of the events surrounding the incident provide context within which to gauge possible DPRK objectives.

The year, 2013, was a low point in North-South relations on the Korean peninsula. In just his second year of power, Kim Jong-Un, was still consolidating his position as North Korea's Supreme Leader and possibly looking for opportunities to demonstrate strength to a domestic audience. On 12 February 2013, North Korea conducted its third nuclear test with the detonation of what it claims was a miniaturized device, giving fuel to fears it was closer to weaponizing a nuclear warhead with which to arm a ballistic missile.[44] The test violated the U.N. NPT, to which North Korea was a signatory member until formally withdrawing in 2003, and blatantly disregarded international norms on nuclear testing.[45] The nuclear test also occurred on the same day President Obama delivered his State of the Union address for 2013 and coincided with threats several days earlier from DPRK news outlets to retaliate against the U.S. and South Korea for cyberattacks it claims to have suffered.[46]

In addition to the nuclear test, the South inaugurated its first female president, Park Geun-hye on 15 February, roughly one month prior to the 20 March attacks. The inauguration occurred approximately two weeks prior to the 01 March commencement of the annual FOAL EAGLE combined field training exercise involving over 210,000 U.S. and Korean military forces. The multi-week FOAL EAGLE exercise, conducted by the Combined Forces Command, has been a source of friction between the North and South for years. The North routinely proclaims the exercise to be a provocation to war. On 08 March, in the aftermath of fresh sanctions against Pyongyang for its nuclear test and in the run-up to FOAL EAGLE, North Korean news agencies announced the nation had "scrapped" the 1953 armistice. It also threatened military retaliation against Seoul and the U.S., and cut off a Red Cross Hotline between the two governments on 11

March, the same day the annual U.S., ROK computer-assisted command post exercise, KEY RESOLVE, began.[47]

In response, U.S. Secretary of Defense, Chuck Hagel, announced the U.S. would add 14 additional ground based interceptor (GBI) missiles to Alaska as a deterrent to North Korean threats. The U.S. also deployed four additional guided missile destroyers (DDGs), stationed B-52 bombers in Guam, and brought F-22 Raptors to participate in the final part of the exercises. Finally, the North continued provocations by staging an unusually aggressive military exercise of their own, within their own borders.[48]


DPRK CONDUCTS 3RD NUCLEAR TEST
PARK GEUN-HYE BECOMES 11TH ROK PRESIDENT
FOAL EAGLE 13 BEGINS
DPRK ANNOUNCES INTENT TO SCRAP ARMISTICE AGREEMENT
KEY RESOLVE 13 BEGINS
US SECDEF HAGEL ANNOUNCES DEPLOYMENT OF INTERCEPTOR MISSILES TO ROK
ROK GOVERNMENT, FINANCE, AND MEDIA NETWORKS EXPERIENCE CYBER ATTACK
KEY RESOLVE 13 ENDS
12 Feb
15 Feb
1 Mar
8 Mar
11 Mar
15 Mar
20 Mar
21 Mar

(Fig. 2) 20 March 2013 Hacking Timeline

2013 North Korean Objectives and Results

Under the rule of Kim Jong-Un’s father, Kim Jong-Il, North Korea routinely conducted a predictable cycle of brinksmanship that usually resulted in concessions from the United Nations or South Korea in exchange for a cessation of the North’s provocative behavior. In exchange for halting activity at its Yongbyon Nuclear Scientific Research Center, or other incendiary behavior, the North received economic aid or other forms of dispensation, strengthening the Kim family hold on power.[49] After the death of Kim Jong-Il in December of 2011, Kim Jong-Un attempted similar behavior by launching a long-range ballistic missile in December of 2012.

While the launch served a military research and development purpose, it is likely the younger Kim anticipated similar concessions, which he could use for domestic consumption and subsequently consolidate his hold on power.

North Korea is also known to posture before each KEY RESOLVE / FOAL EAGLE (KR/FE) set of exercises in an attempt to coerce the U.S. and South Korea into canceling the exercise. As stated, the North equates the annual exercise to war preparations by its adversaries. In the past Pyongyang has offered to suspend nuclear tests and return to Six Party Talks on denuclearization in exchange for a halt to joint U.S., Korean exercises.[50]

Early 2013 provided an optimum time for Kim Jong-Un to attempt to coerce concessions from South Korea's new president given her recent inauguration; fresh U.N. sanctions as a result of the North's December 2012 ballistic missile launch; threats of new sanctions as a result of a third nuclear test in February; and the upcoming KR/FE combined exercise. Each of these events can be viewed as attempted coercion by deterrence and coercion by compellence. On the one hand, through its actions the DPRK was attempting to deter the South from conducting KR/FE. On the other, Kim was likely also attempting to coerce concessions (e.g. increased humanitarian aid and possibly increased dialogue with the international community) to solidify his domestic position and increase his legitimacy. The computer attacks on South Korea's financial and media networks were intended to signal an escalation in coercion attempts. North Korea likely chose computer attacks because it was one of its only options left for escalation.

While North and South Korea have been at a stalemate since the official end of hostilities in 1953, both enjoy what academics term the stability-instability paradox. Such a situation is said to exist when there is enough overall deterrence for either side to engage in all-out warfare, but not enough deterrence to prevent minor provocations. Stephen Haggard and Jon R. Lindsay cite the Cold War as such an example. During the Cold War, the risk of nuclear warfare and mutually assured destruction deterred nuclear and large-scale conventional war between the U.S. and the Soviet Union. However, this threat did not deter proxy wars between the two nations, or minor conventional conflicts. Haggard and Lindsay conclude their analogy by saying, “The use of threats to attenuate the risks of general war…can incentivize lower-level aggression.”[51] In the case of North and South Korea, this situation exists because, while U.S. and South Korean forces enjoy overwhelming conventional advantages, South Korea’s major economic and population centers are well within range of the North’s excessive conventional capability. While South Korea might win any prolonged military engagement with the DPRK, the possibility of such conflict turning into a regional war and the devastating damage it would cause prevent such conflict, but is not enough to prevent lesser forms of aggression, such as the March 2013 cyberattacks.

Ultimately, Kim’s efforts in 2013 failed to produce coercion by compellance or deterrence and his added use of cyber aggression can be viewed as an attempt at escalation in order to achieve his strategic objectives. However, Kim was not able to duplicate the cycle of brinksmanship used by his father, which had periodically resulted in successful coercion. Nor did Kim have other viable options at escalation short of provoking an unacceptable response.

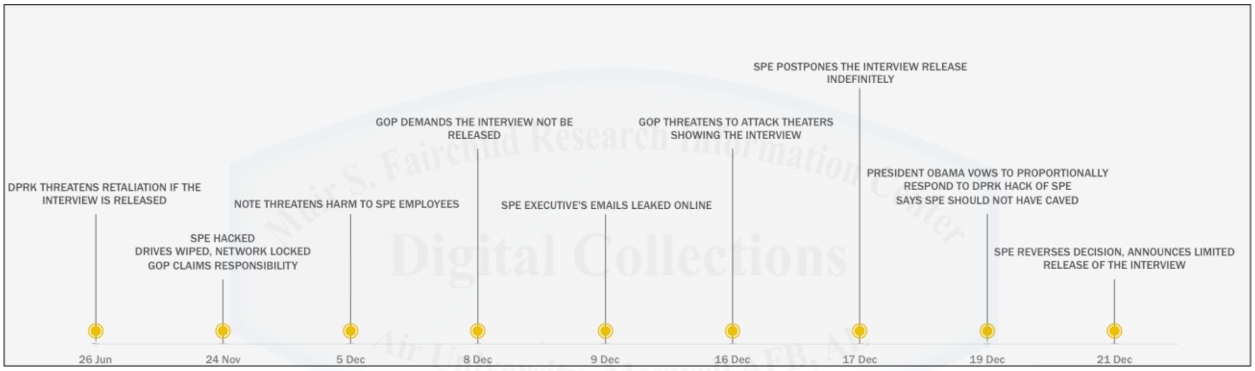
North Korea’s actions did not result in any humanitarian, financial, or other concessions to the regime, nor was KR/FE cancelled. Three important points can be drawn from this analysis. First, internationally accepted norms deterring nuclear testing and proliferation as well as emerging norms prohibiting cyber interference in a state’s financial systems did little to deter state-sponsored cyberattacks or strengthen the coercive effects of such an attack. Second, cyber, while an available form of statecraft to be used in attempts at coercion, was not used in isolation, but as part of a broader escalatory effort. Finally, in this case, the cyberattacks were the last available form of escalation short of provoking a response that would result in either diminished domestic prestige for Kim or a larger conflict that would almost certainly result in defeat. In other words, Pyongyang did not maintain escalation dominance.

November 2014 Sony Pictures Entertainment (SPE) Hack

The November 2014 cyberattack on SPE is another example of the DPRK's use of cyber as an element of statecraft. In this case, North Korea attempted to deter a private U.S. company from showing a film, *The Interview*, depicting the murder of its leader, Kim Jong-Un. While Pyongyang did not directly threaten the U.S. government, it likely knew the U.S. would respond to any coercive attempts against SPE over U.S. networks. This may have been the impetus on 25 June 2014 when the North Korean Ministry of Foreign Affairs appealed to the Obama administration not to support release of the film, before any cyberattack took place.[52]

As the Christmas release date for the film approached, and it became apparent SPE would release the film, entities attributed to North Korea hacked into the Sony network and began stealing sensitive data to include emails, movie scripts and other sensitive information before launching a "wiper" attack on 24 November.[53] SPE employees were made aware of the attack through messages displayed on screens of Sony terminals proclaiming the Guardians of Peace (GOP) carried out the attack. Over the next several days the personal data of SPE employees, along with embarrassing emails from SPE executives, and scripts to several movies still in development were leaked online. The Guardians of Peace escalated its rhetoric on 16 December, posting an online threat to carry out 9/11-type attacks on theaters showing *The Interview*.[54]

In response to the threat of terrorism, SPE indefinitely postponed the release of *The Interview* on 17 December, the same day U.S. officials blamed North Korea for the attacks. The GOP cyberattacks appeared to end the next day, 18 December. The FBI confirmed the GOP's link to Pyongyang on 19 December, the same day President Obama, during his year-end address said SPE made a mistake cancelling the release and announced the U.S. would respond proportionally. The president's announcement was also the first time the U.S. named a foreign government responsible for a cyberattack and promised to punish it. Two days later, SPE representatives reversed course and announced *The Interview* would be released.[55]



(Fig. 3) 2014 Sony Pictures Entertainment (SPE) Hack Timeline

2014 North Korean Objectives and Results

Unlike the innuendo during increasingly tense relations on the peninsula amidst the 2013 financial and entertainment network cyberattacks, North Korea was specific and vocal regarding its intent in 2014. It made this apparent through GOP statements and DPRK official channels. The objective of the 2014 SPE attack was to deter Sony from releasing *The Interview* and, barring that, deter theaters from showing the film. While Pyongyang initially succeeded in coercing SPE to cancel the release, its triumph turned into failure once the U.S. government stepped in.

Despite its eventual failure and relative ineffectiveness, the 2014 SPE attack demonstrates the potential value of cyber as a coercive tool when dealing with entities below the state level. SPE executives were quick to cave to hackers' demands just three weeks after the initial breaches of the company's networks and one day after being threatened with 9/11-style attacks on theaters showing the film. As mentioned, the attacks by the GOP appear to have ended after Sony's announcement of postponement. This can be viewed as successful use of cyber means for deterrence.

Two additional characteristics of the 2014 SPE hack are worth noting. First, the pairing of other forms of statecraft with the SPE cyberattack is present. The SPE cyberattacks contained elements of diplomacy (e.g. statements by the Ministry of Foreign Affairs), information (e.g. statements through official DPRK media), and economic (e.g. the publishing of unreleased movie scripts online in attempts to affect SPE income). Each would have been more effective if carried out with the initial knowledge the acts were supported and perpetuated by the North Korean government. For example, by confusing attribution at the outset, North Korea limited potential use of military or economic provocations to threaten escalation and elicit potential concessions from SPE or other involved governments. Obscuring attribution also arguably limited any future attempts to halt the film's release through diplomacy, though the June 2014 attempts had already failed. Instead of blunting retaliation by the victim, attribution issues limited the options of the attacking government.

Second, the 2014 SPE cyberattack represented another example of North Korea ignoring norms of international behavior. In this instance, Pyongyang violated U.S. law as well as U.S. territorial sovereignty by conducting a cyberattack that resulted in theft and damage to a computer network resident within the U.S. These violations fall into what have been deemed "internationally wrongful acts," as decided by the UN Group of Governmental Experts recommendations.[56]

Finally, while the GOP attacks appear to have ceased after SPE announced the postponement of *The Interview's* release, the exact cause for this termination is debatable. The cessation of North Korean cyber hostilities can just as easily be linked to President Obama's escalation through his 19 December announcement naming North Korea as responsible for the attacks and promising a U.S. response. The fact that there was no reported retaliation by Pyongyang after the 21 December announcement by SPE that *The Interview* would indeed be released, supports the argument that cyber is not as effective a tool of coercion if the attacker does not maintain escalation dominance. The declaration by the president represented an escalation in the conflict; and the U.S. maintains escalation dominance over North Korea in all elements of statecraft. North Korea, having been blamed by the U.S. for the SPE attack risked further escalation were it to have continued cyberattacks.

Escalation Dominance

Both case studies illustrate the limitations on the use of cyber as a coercive tool for weak states that do not maintain escalation dominance. If a state attacks another state via cyberspace, the attacked state has the option of responding with means other than cyberspace. The hacks by Russia during the 2016 U.S. presidential election illustrate this point. The FBI and DHS attributed cyberattacks during the 2016 presidential campaign to Russian intelligence services in a 29 December Joint Analysis Report (JAR). President Obama responded with sanctions against Russia's leading intelligence agencies, expelled 35 Russian diplomats, and closed two U.S.

properties used by Russia. In addition, the U.S. administration alluded to possible covert cyber responses.[57]

The U.S. retaliation is one example of escalation. Given the lack of established cyber deterrent capability in a state, any response to a cyberattack is likely to include escalation beyond cyberspace because of the relatively invisible and stealthy nature of cyberattacks themselves. This is especially true for democracies where governments are held accountable to the people they are supposed to protect. If the public perceives the government will not, or cannot respond to attacks against it, the public may remove those leaders from office. In the case of most Western countries, constituent populations likely need to see more tangible actions (e.g. economic sanctions, diplomatic expulsions, military response) in response to cyberattacks to be reassured and limit domestic disruptions. The use of cyber is also risky for the weak state because of the possibility of unintended effects, which could result in unwanted escalation. For weaker states without the considerable strategic depth of Russia, escalation could prove fatal.

A weak state, such as North Korea, may be able to match some South Korean escalation in response to cyber aggression through limited military and economic means. Such response proves to be an unrealistic option when dealing with powerful states not geographically connected. Escalation dominance is necessary for the optimum effectiveness of cyber statecraft and compliments deterrence in cyberspace. The DoD supported this point of view in a January 2013 report conducted by the Defense Science Board that suggested the U.S. maintain the ability to escalate beyond cyberspace and retaliate with all elements of statecraft in order to maintain a credible deterrence in cyberspace.[58] P.W. Singer and Allan Friedman reinforce this by stating that escalation dominance is the true advantage strong states maintain in cyber conflicts. While weak states can inflict some damage on powerful states via the cyber domain, strong states can always choose to escalate the matter outside the cyber realm if things go poorly. As Singer and Friedman say, “Being powerful means you have the choice [to escalate]. Being weak means you don’t.”[59]

Conclusion

North Korea provides U.S. policy makers useful insight on how to deal with weaker nations for whom norms and international law mean little. As a weak nation, North Korea has been mostly unsuccessful when using cyber for deterrence and coercion primarily because it does not maintain escalation dominance against the state actors it is targeting. In instances where it did maintain escalation dominance (e.g. in the SPE hack, before U.S. government intervention) it achieved some success. Other weak states are likely to find similar results when using cyber as a form of statecraft. While reinforcing state action in cyberspace with other forms of statecraft may enhance a deterrence campaign's effectiveness, the use of cyber will remain limited as a form of statecraft as cyber tools mature. Issues with attribution and credibility also weaken the effectiveness of cyber as a form of statecraft.

The establishment of international cyber norms may help limit escalation among near peer competitors, but will not have a similar effect on weaker states looking for an advantage in the international community. While outside the scope of this paper, the pursuit by revanchist powers like China and Russia to create a parallel international system through the establishment of such institutions like the Asian Investment Bank and organizations based non-Western principles also limit the effectiveness and establishment of such norms. The Joint Chiefs of Staff reinforce this in *Joint Operations Environment (JOE) 2035*. *JOE 2035* highlights the evolution of parallel international institutions that might legitimize state actions the current Western-led international order view as illegitimate.[60] At best, cyber norms may prevent a state from taking actions that could result in sanctions or damage to its reputation. At worst, states may not care about norms if they feel their sovereignty is threatened or if they seek to challenge the western-led international order.

Although, this paper has shown limits to cyber deterrence and coercion, this is not to say states should not pursue these as options in statecraft. While deterrence and coercion may be relatively ineffective for weak states, strong states may be able to use such options more effectively. However, escalation dominance should be viewed as a prerequisite for the effectiveness of any cyber deterrence or coercion campaign.

The 2017 DSB, *Task Force on Cyber Deterrence*, make several specific policy recommendations to address the challenges of deterrence in cyberspace and how the U.S. can better prepare its cyber deterrence capability. The report addresses deterrence approaches to both weak and powerful nations. The U.S. government should adopt these recommendations. The recommendations below echo similar recommendations found in the 2017 DSB, *Task Force on Cyber Deterrence* and the *DoD Cyber Strategy*.[61] In priority, the U.S. should:

1. Develop a Credible Cyber Second-Strike Capability.

The DoD, Department of Energy, and DHS should create a working group to identify U.S. strike systems (e.g. strategic nuclear forces, F-16s, aircraft carriers), their supporting systems (e.g. C3ISR, C2), and related critical infrastructure (e.g. electrical grid, alternate power generation), to be made resilient to cyber attack. Such forces represent a second-strike capability in case of cyber attack and serve as a deterrent to such an attack. It is currently cost-prohibitive and unrealistic to apply this to all U.S. strike systems. Not all strike systems need be resilient to serve as a deterrent. This recommendation is similar to the DSB's, "Thin Line" force but includes the DoD and DHS because of the likelihood elements of supporting infrastructure for strike systems (e.g. power generation) fall outside the DoD.[62] Ensuring a second-strike capability in the aftermath of a significant cyber attack enables the U.S. to maintain escalation dominance and supports deterrence by denial and by punishment. Without a second-strike capability, U.S. deterrence potential is significantly weakened.

2. Develop Cyber Playbook of Response Options

USCYBERCOM in conjunction with the Under Secretary of Defense for Policy develop a "whole-of-government adversary-specific "playbook" of response options to cyber attacks."[63] The playbook is meant as a reference guide and point of departure from which leadership can modify based on the unique context of a given cyber event. The playbook should include responses to a range of cyberattacks, focusing on the impacts of such responses and potential follow-on physical and economic affects.[64] The "whole-of-government" approach capitalizes off U.S. escalation dominance and gives decision-makers flexible, scalable options from which to implement a response.

3. Create and Publish a U.S. Policy on the Use of Offensive Cyber Capabilities

The Departments of State and Defense, in conjunction with the National Security Council, should develop a U.S. policy on the use of offensive cyber capabilities. This policy should identify U.S cyber redlines and clarify norms the U.S. recognizes in cyberspace. The U.S. is already establishing its own normative behavior through its response to attacks and intrusions by Russia, China, and North Korea. The norms addressed here should address responses to only the most egregious cyberattacks that involve the loss of life or ones that physically or operationally damage recognized critical infrastructure. A public declaration of these norms and when the U.S. deems using offensive cyber capabilities as appropriate "provide[s] the basis for international legitimacy for imposing sustained costs on violators."[65]

The U.S. must maintain escalation dominance across the range of DIME and show a willingness to exercise such escalation in order to deter coercive efforts via cyberspace. To achieve this, an inclusive, “whole-of-government” approach needs to be used in formulating the policies to address cyber deterrence. As cyber tools become more effective for deterrence and coercion it is important that the U.S. is consistent and proportional in its response. Cyber capabilities may also eventually develop to a point when they can achieve the equalizing effect weaker states seek. The U.S. must maintain its cyber dominance, much as it has with nuclear and precision-guided weapons intended by the first and second offset strategies, in case this happens. Elements of the third offset strategy apply but U.S. policy must maintain swift and expansive options in response to cyberattacks that cross America’s redlines when norms fail.[66]

Bibliography

Beeker, Kevin R. “Strategic Deterrence in Cyberspace: Practical Application.” Graduate Research Project, Air Force Institute of Technology. June 2009.

Boo, Hyeong-Wook and Kang-Kyu Lee. “Cyber War and Policy Suggestions for South Korean Planners.” *International Journal of Korean Unification Studies*, 21, no. 2 (2012): 85-106.

Crosston, M. “World Gone Cyber MAD: How “Mutually Assured Debilitation” is the Best Hope for Cyber Deterrence.” *Strategic Studies Quarterly*, (Spring 2011): 100-116.

Daugirdas, Kristina and J.D. Mortenson, ed. “Contemporary Practice of the United States Relating to International Law.” *American Journal of International Law* 109, no.2. 2015: 407-32.

Department of Defense, *Task Force on Cyber Deterrence*, Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington D.C., February 2017, 1. http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28- 17_Final.pdf.

Fan Zheng Jiang and Ma Bao An. *The Theory of Military Strategy*. National Defense University Publishing House, 2007.

Finnemore, Martha, and Kathryn Sikkink. “International Norm Dynamics and Political Change.” *International Organization* 52.4. 1998: 894-905.

Haggard, Stephan and Jon R. Lindsay. “North Korea and the Sony Hack: Exporting Instability Through Cyberspace.” *Asia Pacific Issues*. East West Center, Honolulu, HI, no. 117. May 2015.

Healy, Jason (ed). *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*. (Washington, DC: Cyber Studies Association, 2013).

Herzinger, Lt Blake D. “Cyber Secrecy Undermines Deterrence.” *Proceedings Magazine*, vol. 142/9/1363 (September 2016): 44-46.

Iasiello, Emilio. “Is Cyber Deterrence an Illusory Course of Action?” *Journal of Strategic Security* 7, no. 1 (2014): 54-67.

Measuring the Information Society Report 2015, International Telecommunications Union, 2015, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf.

Jun, Jenny, Scott Lafoy, and Ethan Sohn. 2016. *North Korea's Cyber Operations : Strategy and Responses*. n.p.: Rowman & Littlefield Pub Inc, 2016.

Kane, Angela. 2014. "The Rocky Road to Consensus: The Work of UN Groups of Governmental Experts in the Field of ICTs and in the Context of International Security, 1998–2013." *American Foreign Policy Interests* 36, no. 5: 314-321.

Kirk, Donald. "What's behind cyber attacks on South Korea, US?." *Christian Science Monitor*, July 08, 2009., 9, Academic Search Premier, EBSCOhost (accessed October 19, 2016).

Kondoch, Boris. 2013. "Jus ad Bellum and Cyber Warfare in Northeast Asia." *Journal Of East Asia & International Law* 6, no. 2: 459-478.

Lemos, Robert. 2014. "FBI Investigation Confirms North Korea Behind Sony Network Breach." *Eweek* 1.

Lewis, James A. “The “Korean” Cyber Attacks and Their Implications for Cyber Conflict.” Center for Strategic and

International Studies. October 2009.

--. “The Cyber War Has Not Begun.” Center for Strategic and International Studies. March 2010.

Limbago, Andrea L. “One Size Does Not Fit All: The Multifaceted Nature of Cyber Statecraft.” *Joint Forces Quarterly*, no. 78 (3rd Quarter 2015): 84-90.

Libicki, Martin C. 2009. “Cyberdeterrence and Cyberwar.” Santa Monica, CA. RAND.

Lupovici, Amir. 2016. "The "Attribution Problem" and the Social Construction of "Violence": Taking Cyber Deterrence Literature a Step Forward." *International Studies Perspectives* 17, no. 3: 322-342.

McKay, Angela, Jan Neutze, Paul Nicholas, and Kevin Sullivan. *International Security Norms: Reducing Conflict in an Internet-Dependent World*. Microsoft, December 2014.

Maness, Ryan C., and Brandon Valeriano. 2016. "The Impact of Cyber Conflict on International Interactions." *Armed Forces & Society (0095327X)* 42, no. 2: 301-323.

Maurer, Tim. “Cyber Norm Emergence at the United *Nations* – An Analysis of the UN‘s Activities Regarding Cyber-security” Discussion Paper 2011. Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School. September 2011.

Nye, Joseph S. Jr. *The Regime Complex for Global Cyber Actitivies*. Global Commission on Internet Governance, no. 1. Chatham House, London. May 2014.

Office of the Secretary of Defense. *Military and Security Developments Involving People’s Republic of Korea*. Washington D.C.: Government Printing Office. 2013.

Pawlak, Patryk. *Cyber Diplomacy: Confidence-building Measures*. European Parliamentary Research Service. October 2015.

Potter, Evan H. 2002. *Cyber-Diplomacy : Managing Foreign Policy in the Twenty-First Century*. n.p.: McGill-Queen's University Press, 2002.

"Talking Foreign Policy: A Discussion On Cyber Warfare." *Case Western Reserve Journal Of International Law* 47, no. 3 (Spring2015 2015): 319-342. Academic Search Premier, EBSCOhost (accessed October 19, 2016).

Timothy L. Thomas, *Chinas Cyber Incursions: A Theoretical Look At What They See And Why They Do It Based On A Different Strategic Method Of Thought.* May 2013.

United Nations, General Assembly. 2015. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174, available from www.un.org/ga/search/view_doc.asp?symbol=A/71/172

Whyte, Christopher. 2016. "Ending Cyber Coercion: Computer Network Attack, Exploitation and the Case of North Korea." *Comparative Strategy* 35, no. 2: 93-102.

Youd, Nathaniel. 2015. "Cyber Deterrence: Is a Deterrence Model Practical in Cyberspace?." *Space & Defense* 8, no. 1: 47-58.

Notes

[1] Department of Defense, *Task Force on Cyber Deterrence*, Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington D.C., February 2017, 1. http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

[2] *All Fortune 500 Companies Have Been Hacked: 97% Know It, the Other 3% Don't*, Homeland Security News Wire, (08 January 2014), http://www.homelandsecuritynewswire.com/srcybersecurity20140108-all-fortune-500-companies-have-been-hacked-97-know-it-the-other-3-don-t.

[3] *2015 Internet Crime Report*, Federal Bureau of Investigations, U.S. Department of Justice, 2015, 5, https://pdf.ic3.gov/2015_IC3Report.pdf.

[4] Hackmageddon 2016 Cyber Attack Statistics. Accessed at: http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/.

[5] "Talking Foreign Policy: A Discussion On Cyber Warfare," *Case Western Reserve Journal Of International Law* 47, no. 3 (Spring2015 2015): 319-342.

[6] *The DoD Cyber Strategy*, U.S. Department of Defense, April 2015, 1-2, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[7] Hackmageddon 2016 Cyber Attack Statistics. Accessed at: http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/.

[8] Ryan C. Maness and Brandon Valeriano, "The Impact of Cyber Conflict on International Interactions," *Armed Forces & Society* 42, no. 2 (2016): 317; Tim Maurer, "Cyber Norm Emergence at the United Nations - An Analysis of the UN's Activities Regarding Cyber Security," (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011): 17.

[9] Andreas Schmidt, "The Estonian Cyber Attacks," *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, (Washington DC: Cyber Conflict Studies Association, 2013), 186-188; Andreas Hagen, "The Russo-Georgian War 2008," *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, (Washington DC: Cyber Conflict Studies Association, 2013), 194-204.

[10] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, RAND Report FA7014-06-C-0001 (Santa Monica, CA: RAND, 2009), xv

[11] Saim Saeed, "U.S. Intelligence Chief: Russia Interfering in French, German Elections," *Politico Europe*, 30 March 2017, http://www.politico.eu/article/us-intelligence-chief-russia-interfering-in-french-german-elections/.

[12] Works such as Jason Healy's, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Panayotis Yannakogeorgos and Adam Lowther's, *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, and P.W. Singer and Allan Friedman's, *Cybersecurity and Cyberwar What Everyone Needs to Know*, are just a few of the multiple books to explore some of the more popular cyber actions by Russia, China, and significant non-state actors like Anonymous. The literature on cyber actions assumed to be perpetrated by weaker nations (e.g. North Korea and Iran) are limited to press reports and smaller examinations done by think tanks and special interest groups. This may change as additional information becomes available regarding the Nov 2014 North Korea hack of Sony Pictures Entertainment, and the presumed Iranian hack of the Saudi energy sector with the Shamoon malware.

[13] Center for Strategic and International Studies, *The Cyber Index: International Security Trends and Realities*, United Nations Institute for Disarmament Research, Geneva, Switzerland (2013), 1.

[14] Hyeong-Wook Boo and Kang-Kyu Lee, "Cyber War and Policy Suggestions for South Korean Planners," *International Journal of Korean Unification Studies*, 21, no. 2 (2012): 97.

[15] "Talking Foreign Policy" 325.

[16] Boo and Lee, “Cyber War and Policy,” 89-90.

[17] James Hackett, ed. *The Military Balance 2010*, International Institute for Strategic Studies, (London, Routledge, 2010).

[18] *Treaty on the Non-Proliferation of Nuclear Weapons*, United Nations Office for Disarmament Affairs, United Nations, 01 July 1968, https://www.un.org/disarmament/wmd/nuclear/npt/text; Anna Fifield, “Punishing North Korea: A Rundown on Current Sanctions,” *Washington Post*, 22 February, 2016, https://www.washingtonpost.com/news/worldviews/wp/2016/02/22/punishing-north-korea-a-run-down-on-current-sanctions/?utm_term=.8db1b327826f.

[19] Edith M. Lederer and Eric Talmadge, “UN Security Council Strongly Condemns North Korea Missile Test,” *Chicago Tribune Online*, 13 February 2017, http://www.chicagotribune.com/news/nationworld/ct-north-korea-missile-test-20170213-story.html; Taehoon Lee and Ben Westscott, “Failed North Korean Missile Exploded ‘Within Seconds,’ US Says,” *CNN World Online*, 22 March 2017, http://www.cnn.com/2017/03/21/asia/north-korea-missile-test/.

[20] Private and public entities, such as Microsoft Corporation, the United Nations and the European Union have claimed that internationally accepted cyber norms and confidence-building measures will deter state-sponsored malicious actions in cyberspace and serve to decrease the risk of conflict and misunderstanding. See NATO Cooperative Cyber Defense Center of Excellence, “OSCE Confidence-Building Measures for Cyberspace,” 20 December 2013, https://ccdcoe.org/osce-confidence-building-measures-cyberspace.html; Angela McKay, Jan Neutze, Paul Nicholas, and Kevin Sullivan, *International Security Norms: Reducing Conflict in an Internet-Dependent World*, Microsoft, December 2014 and Patryk Pawlak, *Cyber Diplomacy: Confidence-building Measures*, European Parliamentary Research Service, October 2015.

[21] Chico Harlan and Ellen Nakashima, “Suspected North Korean Cyber Attack on a Bank Raises Fears for S. Korea, Allies,” *The Washington Post*, 29 August 2011, https://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.html?utm_term=.c5b3ed73fc08; “N. Korea Steps Up Hacker Attacks on S. Korean Firms,” *Chosun Ilbo*, 30 August 2011, https://www.english.chosun.com/site/data/html_dir/2011/08/30/2011083004444.html

[22] “N.Korea’s Highly Trained Hacker Brigades Rival CIA,” *Chosun Ilbo Online*, 05 May 2011, http://english.chosun.com/site/data/html_dir/2011/05/05/2011050500392.html.

[23] *Measuring the Information Society Report 2015*, International Telecommunications Union, 2015, 60. The IDI takes into account several measures of ICT penetration into a society (e.g. internet usage, broadband subscriptions, data availability, households with a computer, etc.).

[24] Robert Pape, *Bombing to Win: Air Power and Coercion in War*, (Ithica, NY: Cornell University Press, 1996), 12.

[25] Thomas C. Schelling, *Arms and Influence*, (New Haven, CT: Yale University Press).

[26] Liam Nevill and Zoe Hawkins, *Deterrence in Cyberspace: Different Domain, Different Rules*, (Barton, Australia: Australian Strategic Policy Institute, 2016), 6.

[27] James A. Lewis, “The “Korean” Cyber Attacks and Their Implications for Cyber Conflict,” *Center for Strategic and International Studies*, October 2009, 4.

[28] Kevin Liptak, “Obama Has ‘Blunt’ Meeting with Putin but ‘Gaps of Trust’ on Syria Remain,” *CNN Politics Online*, 5 September 2016, http://www.cnn.com/2016/09/05/politics/barack-obama-g20-summit-asia/.

[29] Joint Analysis Report, “GRIZZLY STEPPE - Russian Malicious Cyber Activity,” *National Cybersecurity and Communications Integration Center*, Ref. JAR-16-20296, 29 December 2016, https://assets.documentcloud.org/documents/3248231/Report-on-Russian-Hacking.pdf. ; David E. Sanger, “Obama Strikes Back at Russia for Election Hacking,” *The New York Times*, 29 December 2016, http://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html.

[30] “Global Run of Cyberattacks Linked to North Korea,” PYMNTS, 13 February 2017, http://www.pymnts.com/news/security-and-risk/2017/global-run-of-cyberattacks-connected-to-the-north-koreans-who-hacked-sony/.

[31] Panayotis A. Yannakogeorgos and Adam Lowther, “The Prospects for Cyber Deterrence: American Sponsorship of Global Norms,” *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, (Boca Raton, FL: Taylor and Francis Group, 2014), 51.

[32] Pape, *Bombing to Win*, 13

[33] Clinton M. Woods, *Implementing Cyber Coercion*, Calhoun Institutional Archive of the Naval Postgraduate School, Monterrey, CA, 2015, 17.

[34] Department of Defense, *Task Force on Cyber Deterrence*, Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington D.C., February 2017, 3. http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

[35] Scott Maucione, “White House Finally Acquiesces to Congress on Cyber Deterrence Policy,” 13-15.

[36] Department of Defense, *Task Force on Cyber Deterrence*, Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington D.C., February 2017, 9, 13-14. http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

[37] “N. Korea Steps Up Hacker Attacks,” *Chosun Ilbo*

[38] Son To’k-ho, “Pyongyang Hacking Support Personnel Increased by 900,” *Chosun Ilbo*, 29 April 2015, accessed online at Open Source Center, https://www.opensource.gov/portal/server.pt/gateway/PTARGS_0_0_ 200_0_0_43/content/Display/ KPR2015050125607748?returnFrame=true

[39] David Lee, “Bureau 121: How Good Are Kim Jong-Un’s Elite Hackers?” *BBC Online*, 29 May 2015, http://www.bbc.com/news/technology-32925503.

[40] “Broadcasters, Banks Recover Networks After Suspected Cyber Attacks,” *Yonhap*, 21 March 2013, http://english.yonhapnews.co.kr/news/2013/03/21/55/0200000000AEN20130321003500315F.HTML; Graham Cluley, “DarkSeoul: SophosLabs Identifies Malware Used in South Korean Internet Attack,” *Naked Security by Sophos*, 20 March 2013, https://nakedsecurity.sophos.com/2013/03/20/south-korea-cyber-attack/.

[41] Choe Sang-hun, “Computer Networks in South Korea Are Paralyzed in Cyberattacks,” *New York Times*, 20 March 2013, http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html.

[42] Ibid.

[43] “South Korea Blames North for Bank and TV Cyber-Attacks,” *BBC Online*, 10 April 2013, http://www.bbc.com/news/technology-22092051.

[44] David Chance and Jack Kim, “North Korea Nuclear Test Draws Anger, Including from China,” *Reuters*, 12 February 2013, http://www.reuters.com/article/us-korea-north-idUSBRE91B04820130212.

[45] Kelsey Davenport, “Chronology of U.S.-North Korea Nuclear and Missile Diplomacy,” *Arms Control Association*, October 2016, https://www.armscontrol.org/factsheets/dprkchron.

[46] Choe, “Computer Networks in South Korea are Paralyzed.”

[47] Choe Sang-hun, “North Korea Declares 1953 War Truce Nullified,” *New York Times*, 11 Mar 2013, http://www.nytimes.com/2013/03/12/world/asia/north-korea-says-it-has-nullified-1953-korean-war-armistice.html.

[48] Thom Shanker, David E. Sanger, and Martin Fackler, “U.S. is Bolstering Missile Defense to Deter North Korea,” *The New York Times*, 15 March 2013, http://www.nytimes.com/2013/03/16/world/asia/us-to-bolster-missile-defense-against-north-korea.html.

[49] Ibid.

[50] “Change in N. Korea Does Not Mean Regime Change: Senior U.S. Diplomat,” *The Korea Times*, 05 February 2015, http://www.koreatimes.co.kr/www/news/nation/2015/02/485_173053.html.

[51] Stephan Haggard and Jon R. Lindsay, “North Korea and the Sony Hack: Exporting Instability Through Cyberspace,” *Asia Pacific Issues*, no. 117, May 2015, 3-4.

[52] Choe Sang-Hun, “North Korea Warns U.S. Over Film Mocking Its Leader,” *The New York Times*, 25 June 2014, https://www.nytimes.com/2014/06/26/world/asia/north-korea-warns-us-over-film-parody.html?_r=0.

[53] Ellen Nakashima, “Why the Sony Hack Drew an Unprecedented U.S. Response Against North Korea,” *The Washington Post*, 15 January 2015, https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html.

[54] Lori Grisham, “Timeline: North Korea and the Sony Pictures Hack,” *USA Today*, http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/; Ellen Nakashima, “Why the Sony Hack Drew an Unprecedented U.S. Response Against North Korea,” *The Washington Post*, 15 January 2015, https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html.

[55]Ellen Nakashima, “Why the Sony Hack Drew an Unprecedented U.S. Response Against North Korea,” *The Washington Post*, 15 January 2015, https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html; Haggard and Lindsay, “North Korea and the Sony Hack”; Lori Grisham, “Timeline: North Korea and the Sony Pictures Hack,” *USA Today*, http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/.

[56] United Nations, General Assembly. 2015. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174, 2/17 available from www.un.org/ga/search/view_doc.asp?symbol=A/71/172.

[57] Joint Analysis Report, “GRIZZLY STEPPE - Russian Malicious Cyber Activity,” *National Cybersecurity and Communications Integration Center*, Ref. JAR-16-20296, 29 December 2016, https://assets.documentcloud.org/documents/3248231/Report-on-Russian-Hacking.pdf. ; David E. Sanger, “Obama Strikes Back at Russia for Election Hacking,” *The New York Times*, 29 December 2016, http://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html.

[58] Quoted in Nathaniel Youd, "Cyber Deterrence: Is a Deterrence Model Practical in Cyberspace?" *Space & Defense* 8, no. 1, 2015: 47-58.

[59] P.W. Singer and Alan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, New York, 2014.

[60] *Joint Operating Environment (JOE) 2035: The Joint Force in a Contested and Disordered World*, 14 July 2016, 7-8.

[61] Department of Defense, *Task Force on Cyber Deterrence*, Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington D.C., February 2017. http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf; *The DoD Cyber Strategy*, U.S. Department of Defense, April 2015, 1-2, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[62] Department of Defense, *Task Force on Cyber Deterrence*, Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington D.C., February 2017, 18-20. http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

[63] Department of Defense, *Task Force on Cyber Deterrence*, Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington D.C., February 2017, 13. http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

[64] *The DoD Cyber Strategy*, U.S. Department of Defense, April 2015, 14, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. The DoD Cyber Strategy lists, “Build and Maintain Viable Cyber Options” as its fourth strategic goal.

[65] Department of Defense, *Task Force on Cyber Deterrence*, Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington D.C., February 2017, 11. http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf. This recommendation is similar to the DSB's recommendation for a policy framework for cyber deterrence, which includes the declaratory policy. Unlike the DSB's recommendation, I include elements outside the DoD. Overall, my recommendations take a more whole-of-government approach to cyber policy actions.

[66] Robert Martinage, "Toward a New Offset Strategy: Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection Capability," Center for Strategic and Budgetary Assessments, Washington D.C. 2014, v-vi, http://www.csbaonline.org/publications/2014/toward-a-new-offset-strategy-exploiting-u-s-long-term-advantages-to-restore-u-s-global-power-projection-capability/.