Defending Forward on the Korean Peninsula

Cyber Deterrence in the U.S.-ROK Alliance

Dr. James E. Platte

ABSTRACT

The United States has provided extended deterrence, backed by U.S. nuclear weapons, to South Korea since the end of the Korean War in 1953, and despite repeated low-level provocations by North Korea, the U.S.-ROK alliance has successfully deterred strategic attack on South Korea. The allies now face a growing asymmetric threat from North Korea in the cyber domain, and the alliance has yet to incorporate the cyber domain into the allied strategic deterrence posture. This paper examines cyber deterrence thinking and analyzes how to formulate a cyber deterrence posture as part of the overall strategic deterrence posture of the U.S.-ROK alliance. As with kinetic attacks, the alliance should focus on deterring cyber-attacks that produce cross-domain strategic effects and divide responsibilities to leverage each other's capabilities and interests. Even for cyber-attacks that do not reach the threshold of producing strategic effects, U.S. Defense Department cyber concepts like "defending forward" and "persistent engagement" can be operationalized to reduce the threat to South Korea posed by the range of North Korea's malicious cyber activity.

I. INTRODUCTION

The alliance between the United States and the Republic of Korea (ROK, otherwise referred to as South Korea) has evolved significantly since the two countries signed a mutual defense treaty in 1953. Geopolitical changes since 1953, particularly the collapse of the Soviet Union and the economic rise of East Asia, have driven many of the changes in the alliance, but technological changes also have significantly impacted the alliance. The digital revolution and the penetration of digital technologies throughout all facets of society has led to the U.S.-ROK alliance placing an increased emphasis on dealing with threats in the cyber domain. This paper will analyze how the two allies view cyber deterrence and how theories of deterrence can be applied to the cyber domain in the context of the U.S.-ROK alliance.

While the U.S.-ROK alliance has "has expanded into a deep, comprehensive global partnership," the core of the alliance remains defending South Korea from North Korean aggression.[1] The joint communique from the U.S.-ROK Security Consultative Meeting in October 2018 reaffirmed this point by stating the fundamental mission of the alliance is "to defend the ROK through a robust combined defense posture and to enhance the mutual security of both nations under the U.S.-ROK Mutual Defense Treaty.[2] This paper will focus on how the allies can approach deterring and defending cyber threats to South Korea, particularly threats originating from North Korea. There will be an implicit focus on the two militaries' roles in cyber deterrence, but with an acknowledgement that cyber deterrence, like other forms of deterrence, requires a whole-of-government approach.

From a theoretical perspective, much of the deterrence thinking will come from the nuclear era, even though the concept of deterrence is likely as old as international relations and has roots in criminology and other non-military fields. Yet, much of the contemporary thinking on deterrence, especially in the US, comes from the superpower showdown between the Soviet Union and the US during the Cold War. Scholars have described four waves of deterrence research in the nuclear era, and there has been much scholarly and policy work done on developing cyber deterrence theories in recent years.[3] But as Joseph Nye noted in 2017, "[t]heorizing about deterrence in the cyber era is emerging from only its first wave."[4] Thus, this paper also will explore how theories of deterrence from the nuclear era can apply in the cyber domain, with a focus on cyber deterrence in the U.S.-ROK alliance context.

The second section of this paper will give an overview of deterrence theory and general methods of deterrence. Next, section three will discuss who and what is to be deterred in the cyber domain by the United States and South Korea and how cyber deterrence compares to other deterrence domains in the U.S.-ROK alliance. The fourth section will examine what has been said, so far, regarding cyber deterrence by the US and South Korea. Then section five will analyze how different methods of deterrence could be applied to bolstering deterring cyber threats to South Korea. The paper will conclude with thoughts on deterrence theory in this alliance relationship and with policy recommendations for the U.S.-ROK alliance.

II. OVERVIEW OF DETERRENCE THEORY AND METHODS

Concepts of deterrence in international relations literature can be found at least as far back as the Peloponnesian War.[5] The most common conception of deterrence can be described as dissuading an adversary from taking an action by threatening unacceptable violence in retaliation. This definition of deterrence has been come to be known as deterrence by punishment or deterrence by retaliation and was the most dominant form of deterrence thinking during the Cold War, elucidated by such prominent scholars as Thomas Schelling and Herman Kahn.

The overwhelming destructive power of nuclear weapons led scholars and practitioners to focus on deterrence by punishment from the start of the nuclear age. The retaliatory power of nuclear weapons made war nearly unthinkable to many early deterrence scholars, and any instance of deterrence failure in the nuclear era was unacceptable. In 1946, Bernard Brodie famously summarized this sentiment, declaring "[t]hus far, the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them."[6] Other prominent deterrence scholars, including Schelling and Kahn, similarly espoused a strategy of deterrence based on the overwhelming power of nuclear weapons.

However, deterrence can be applied more broadly than this punishment model. In addition to deterrence by punishment, Glenn Snyder proposed another concept termed deterrence by denial in the late 1950s. Snyder viewed deterrence strategies as manipulating an adversary's cost-benefit analysis, and deterrence "means discouraging the enemy from taking military action by posing for him a prospect of cost and risk outweighing prospective gain."[7] Whereas deterrence by punishment acts on an adversary's estimate of possible costs, deterrence by denial acts on an adversary's estimate of the probability of gaining benefits. Thus, as Jeffrey Knopf observed, "denial strategies aim to dissuade a potential attacker by convincing them that the effort will not succeed and they will be denied the benefits they hope to obtain." Combining these two concepts of deterrence into a more robust definition, Joseph Nye provided a broader definition of deterrence as "dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit."[9]

Inherent in both of these concepts of deterrence is that deterrence occurs in the mind of an adversary. Deterrence is a function of the defender's capability and will to punish or deny, and the defender can formulate and signal a strategy to deter an adversary. But more appropriately, deterrence occurs as a function of an adversary's belief in the defender's capability and will to punish or deny. Deterrence scholars emphasize that the credibility of the defender's deterrence posture and effectively signaling this posture to an adversary is essential for creating a deterrent effect in the mind of an adversary. Recognizing that deterrence is a psychological phenomenon, scholars such as Robert Jervis, Richard Neb Lebow, Janis Stein, and Jeffrey Berejikian analyzed the effect that bias, misperception, and other cognitive functions can have on the success or failure of deterrence.[10] Nye summed up their arguments by stating, "[d]eterrence is a psychological process that depends on the perceptions of both the actors and the targets, and the ability to communicate those views clearly."[11]

Nye also adds two methods of deterrence to this discussion: deterrence by entanglement and deterrence by norms. Nye defines entanglement as "the existence of various interdependences that make a successful attack simultaneously impose serious costs on the attacker as well as the victim."[12] These interdependences, either dyadic or systemic, can lead a state to perceive that there is more benefit to maintaining the status quo than to potentially upsetting the status quo through some form of attack, even if the attack is not defended against or there is no fear of retaliation.[13] Deterrence by norms works "by imposing reputational costs that can damage an actor's soft power beyond the value gained from a given attack. Like entanglement, norms can impose costs on an attacker even if the attack is not denied by defense and there is no retaliation."[14]

Just like the concept of deterrence itself, none of these four methods of deterrence are exclusive to the nuclear domain or are inherently tied to nuclear weapons. Deterrence and the different deterrence strategies can apply to all domains, but there are challenges to applying each of these four deterrence methods in the cyber domain. The optimal cyber deterrence strategy likely will require a combination of these methods, and creative deterrence thinking will be required to move deterrence theories beyond the nuclear domain.

III. WHO AND WHAT TO DETER IN THE CYBER DOMAIN

The first step to crafting a cyber deterrence strategy is to answer the following two questions. First, who is being deterred, and second, what action is being deterred? Since this paper focuses on the U.S.-ROK alliance, answering those two questions requires identifying who are the major actors that threaten South Korea in the cyber domain.

The 2018 U.S. Department of Defense (DoD) Cyber Strategy identifies four states that employ malicious cyber activities to threaten US interests: China, Russia, Iran, and North Korea.[15] While those four states and non-state actors could employ cyber threats against South Korea, the ROK Ministry of National Defense's (MND) 2016 Defense White Paper only calls out North Korea.[16] Cybersecurity scholar Donghui Park also wrote that South Korea's primary external cyber security challenge is cyber attacks from North Korea.[17] Thus, for this paper, the answer to who is to be deterred is North Korea.

Answering what is to be deterred is not quite as straightforward as just cyber-attacks against South Korea originating from North Korea. But before attempting to formulate a more nuanced answer as to what is to be deterred, an additional point on deterrence theory should be made here for the U.S.-ROK alliance. For South Korea, this discussion involves direct deterrence, which concerns actions against one's own state and its immediate interests. The US provides extended deterrence, which is "dissuasion of adversary actions against a third party or non-immediate interests," for South Korea.[18] This distinction is fairly clear in the nuclear domain, where the US extended deterrence guarantee is meant to deter nuclear attack on South Korean territory, and US direct deterrence is meant to deter nuclear attack on U.S. territory. The interconnected nature of the cyber domain does not make the distinction between direct deterrence and extended deterrence as clear. US and South Korean interests can easily overlap in the cyber domain, and attacks on networks or digital systems that are owned and controlled by South Korean entities can have significant impacts on US interests, too.

In addition to this blurring of direct deterrence and extended deterrence in the cyber domain, there also is a wide range of malicious cyber behaviors that are undesirable, and it is not realistic to expect that the U.S.-ROK alliance can and should aim to deter the entire spectrum of malicious cyber behavior that could be directed at South Korea. Comparing the U.S.-ROK alliance's deterrence posture in other domains, namely nuclear and conventional, could be a useful starting point for thinking of where cyber deterrence fits into the alliance's overall deterrence posture and what actions are to be deterred in the cyber domain.

The original mutual defense treaty between the United States and the Republic of Korea signed in 1953 only briefly mentions deterring "armed attack" but does not elaborate further on who and what is to be deterred by the alliance.[19] There is a wide range of acts that could be considered armed attack, but more recent statements by the allies provides some more clarity. The joint communique from the 2017 U.S.-ROK Security Consultative Mechanism (SCM), an annual meeting between the US Secretary of Defense and the ROK Minister of National Defense, proclaimed that the United States would provide extended deterrence "using the full range of military capabilities, including the US nuclear umbrella, conventional strike, and missile defense capabilities."[20] The allies also committed to strengthening their "deterrence measures and capabilities in response to the increasing North Korean nuclear, weapons of mass destruction (WMD), and ballistic missile threat." The joint communique from the 2018 SCM reiterated the U.S. extended deterrence commitment from the previous year and added that the U.S.-ROK Combined Forces Command "has played the central role in deterring war on the Korean Peninsula" since it was formed in 1978.[21]

The allies have increasingly focused on the threat from North Korea's nuclear, WMD, and ballistic missile programs in recent years, most notably establishing a joint Tailored Deterrence Strategy Against North Korean Nuclear and other WMD Threats in 2013. This strategy created a framework for "tailoring deterrence against key North Korean nuclear threat scenarios across armistice and wartime."[22] Joint communiques from subsequent SCMs all have mentioned implementing the Tailored Deterrence Strategy, making it a major pillar of the U.S.-ROK alliance. At the press conference announcing the signing of the Tailored Deterrence Strategy, then-ROK Minister of National Defense Kim Kwan-jin added that the U.S.-ROK alliance "has efficiently deterred North Korean provocations, as well as maintained peace and stability on the Korean peninsula."[23]

It also is worth considering what providing extended deterrence means for the United States. Extended deterrence may be most commonly thought of as using U.S. nuclear weapons to deter nuclear attack on U.S. allies, but the 2018 Nuclear Posture Review (NPR) made clear that the United States does not reserve using its nuclear weapons only for deterring other nuclear weapons. The NPR stated that the United States "would only consider the employment of nuclear weapons in extreme circumstances. Extreme circumstances could include significant non-nuclear strategic attacks. Significant non-nuclear strategic attacks include, but are not limited to, attacks on the U.S., allied, or partner civilian population or infrastructure, and attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities." [24] Thus, U.S. nuclear weapons are used for deterring all strategic attacks, both nuclear and non-nuclear, and the 2018 NPR also commits the United States to deterring strategic attacks on its allies.

Taken together, the recent SCM joint communiques, the Tailored Deterrence Strategy, and the 2018 NPR imply that the US extended deterrent commitment to South Korea is intended to deter strategic attacks on South Korea. Strategic attacks could include North Korean use of nuclear, biological, or chemical weapons or a large-scale, conventional attack on South Korea. Attacks or provocations that fall below the strategic level may be included more in the U.S.-ROK alliance's defense posture, or the South Korean military may take primary responsibility for deterring and defending against non-strategic attacks and provocations.

The history of the U.S.-ROK alliance also suggests that this division of responsibilities between the allies is the case. North Korea has conducted repeated attacks and provocations against South Korea, occasionally resulting in South Korean casualties or destruction of property, but the US preference after such provocations has been to deescalate and restore deterrence before escalating to a larger conflict. No North Korean provocation since the invasion that started the Korean War on 25 June 1950 has risen to the level of strategic attack. Despite numerous North Korean provocations, this is why the allies can credit the U.S.-ROK alliance with preserving peace on the Korean Peninsula since hostilities in the Korean War ceased in July 1953. This also is an implicit acknowledgement of the difficulty of deterring lower-level provocations, especially against a determined adversary like North Korea.

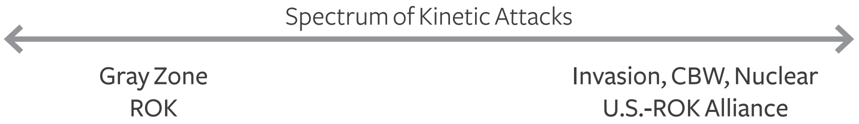

Figure 1. Division of responsibility for deterring North Korean kinetic attacks on South Korea

Figure 1 graphically summarizes this deterrence posture of the U.S.-ROK alliance. On the full spectrum of kinetic attacks that North Korea could launch against South Korea, the U.S.-ROK alliance takes more responsibility at the upper end, and South Korea takes more responsibility at the lower end, represented by so-called gray zone attacks. The U.S.-ROK alliance certainly could have a deterrent effect on lower-level attacks, but the alliance is postured more toward deterring strategic attacks.

One could reasonably project that the U.S.-ROK alliance would posture similarly in the cyber domain. Namely, South Korea would take more responsibility for deterring lower-level North Korean cyber provocations, and the U.S.-ROK alliance would take more responsibility for deterring strategic cyber-attacks. This is depicted in Figure 2.

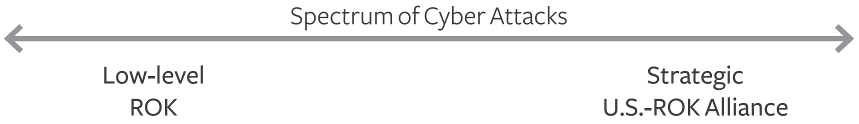

Figure 2. Division of responsibility for deterring North Korean cyber attacks on South Korea

The bigger challenge then is determining what constitutes a cyber-attack with strategic effect or what types of cyber-attacks the U.S.-ROK should posture to deter. The following list provides examples of North Korean cyber-attacks on South Korean entities.[25] This list is not comprehensive but gives some of the more impactful North Korean cyber-attacks. North Korea's cyber-attack on Sony Pictures in 2014 is not included because that attack targeted U.S. entities.

- July 2009: Distributed denial of service (DDoS) attack on US and ROK websites, including Blue House and White House, destroyed nearly 1,500 computers
- April 2011: Attack on Nonghyup Bank that deleted financial data from 273 servers that disrupted financial networks for 20 days
- March/June 2013: DarkSeoul attacks on ROK media, financial firms, and Blue House servers that destroyed some 48,000 computers and servers at 68 institutions
- December 2014: Hack of Korea Hydro and Nuclear Power released nuclear reactor data, including a power plant blueprint
- September 2016: Attack on ROK MND vaccine server and theft of U.S.-ROK planning documents[26]

For the U.S.-ROK alliance, the first question to ask when looking this history of North Korean cyber-attacks on South Korea is whether any of them are the type of attack against which the alliance needs to posture to deter. It is arguable that none of these attacks had strategic effects on South Korea, but the diversity of targets and increasing scale of damage is concerning. It also is less clear in the cyber realm what type of attack would produce strategic effects, especially since cyber attacks could be used as a precursor to or force multiplier for larger-scale kinetic attacks.

In the cyber domain, South Korean scholars write that North Korea's primary aim is "to attack the intelligence network when there is a total war to delay the intervention of U.S. troops." [27] This cyber operation would then be followed by attacking South Korea's C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) system to neutralize ROK weapon systems and munitions support, which would leave South Korean troops vulnerable to massive kinetic attacks. Another South Korean scholar speculated that North Korea could "first conduct a simultaneous and multifarious cyber offensive on...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."[28] While the cyber-attacks listed above are concerning and require some sort of response, the potential for combining cyber-attacks with conventional or nuclear weapons is more troubling for the U.S.-ROK alliance.

Along the lines of the hybrid attack scenarios described by scholars, South Korea's 2016 Defense White Paper also suggested what should be the focus of an alliance cyber deterrence posture. "To prepare for potential cyber-attacks from North Korea, a framework for protecting critical national infrastructures and military-operated systems is currently under development."[29] Cyber attacks on South Korean critical infrastructure or military networks have the most potential to produce strategic effects, either on their own or when combined with conventional or nuclear weapons, and North Korea could use various cyber tools to attack ROK critical infrastructure or military networks.

Thus, the U.S.-ROK alliance should focus on deterring North Korean cyber attacks that have strategic effects or could enable strategic attacks, not particular types of cyber weapons or attacks. This cyber deterrence posture should include ROK critical infrastructure, military C4ISR and warning systems, and systems critical for network-centric warfare. The December 2014 hack of South Korean's nuclear plant operator and September 2016 hack of ROK MND servers could be examples of attacks that the alliance should posture to deter in the future, although neither of those attacks on their own produced strategic effects. The lack of clarity on the effects of cyber attacks is a significant issue that the alliance will have to grapple with when making a cyber deterrence strategy. South Korea should take whole-of-government approach to deter, defend, and respond to lower level attacks, such as those on ROK government websites, South Korean financial and media companies, and DPRK information operations.

This is not to say that the alliance should not be concerned with malicious North Korean cyber activity that falls below the threshold of producing strategic effects. As with kinetic attacks, lower level cyber attacks are disruptive and damaging to South Korean society, threaten US personnel and interests in South Korea, and can damage the credibility of the US security commitment in the minds of South Koreans. This is where the United States can operationalize its "defending forward" and "persistent engagement" concepts to help South Korea address lower level North Korean cyber attacks.

As the vision statement for U.S. Cyber Command (USCYBERCOM) declares, "Through persistent action and competing more effectively below the level of armed conflict, we can influence the calculations of our adversaries, deter aggression, and clarify the distinction between acceptable and unacceptable behavior in cyberspace."[30] In this way, the U.S.-ROK alliance can act against sub-strategic threshold North Korean attacks to both counter those attacks and possibly produce a deterrent effect against similar attacks in the future. North Korea is notorious for not accepting or upholding norms of behavior, but persistent engagement could compel North Korea to at least respect U.S.-ROK norms in the cyber domain.

Defending forward and persistent engagement are also similar to the concept of cumulative deterrence, which Israel has developed to address threats from non-state actors. Cumulative deterrence simultaneously uses "threats and force (mostly military) over the course of an extended conflict."[31] By employing force and achieving a series of victories accumulated over extended periods, the defender moderates the behavior of the adversary, which leads to the adversary reducing the scope, scale, or frequency of attacks.[32] Reducing the scope, scale, and frequency of lower level North Korean cyber attacks through active defense and deterrence also should be an objective of the U.S.-ROK alliance.

Ideally, the U.S.-ROK alliance or South Korea on its own could formulate a cyber deterrence posture that would prevent all such attacks in the future, but as with kinetic attacks, not all cyber attacks can be deterred. North Korea also seems to have embraced the cyber domain and sees cyber operations as being able to achieve tactical, operational, and strategic objectives during peacetime and in war.[33] North Korea is a very determined cyber actor, and it may be difficult to deter lower-level attacks, just like it has been difficult to deter lower-level conventional attacks by North Korea. South Korea can focus on defending, responding to, and recovering from lower-level attacks, and the U.S.-ROK alliance can focus on deterring strategic or potentially strategic attacks from North Korea.

IV. U.S.-ROK VIEWS ON CYBER DETERRENCE

In order to posture to deter cyber-attacks that could have strategic effects, the allies need to express their ability and willingness to deter such attacks, but there has been no comprehensive U.S.-ROK cyber deterrence statement or document released. The allies have made several joint statements on cooperation in the cyber domain, and both the United States and South Korea have made their own statements related to cyber deterrence. This section will examine some of the major statements regarding the cyber domain to see where the U.S.-ROK alliance stands in crafting a cyber deterrence posture.

This section will focus on statements since the start of the Trump administration in 2017 (current ROK President Moon Jae-in also assumed office in 2017), but setting a baseline for those statements is a 2015 joint statement on the U.S.-ROK alliance made by the previous US and South Korean presidents. That 2015 statement gave four areas of emphasis for U.S.-ROK alliance cooperation in cyberspace:

1) enhancing information sharing on cyber threats, particularly to critical infrastructure,

2) strengthening collaboration on investigation on cyber incidents,

3) deepening military-to-military cyber cooperation, and

4) encouraging collaboration on cybersecurity research and development, education and workforce development, and cooperation on technology between cybersecurity industries.[34]

The US and South Korea also pledged to strengthen bilateral cooperation mechanisms, including the U.S.-ROK Cyber Policy Consultations and the mil-to-mil Cyber Cooperation Working Group, and they established a White House-Blue House cyber coordination channel.

This statement does not mention deterrence specifically and lacks much detail, but there is a focus on protecting critical infrastructure and military networks. Importantly for deterrence, there also is a focus on identifying threats and the source of an attack. The attribution problem is widely recognized in the cyber domain, and a deterrent threat cannot be carried out if the attacker is not identified in a timely manner.

On the military side, the SCM joint communiques provide even less detail on how the U.S.-ROK alliance views cyber deterrence. The 2017 SCM joint communique "recognized cyber capacity as a core security issue and decided to expand bilateral defense cooperation in cyber-related areas. Through regular bilateral engagements and the ROK-U.S. Cyber Cooperation Working Group (CCWG), both sides plan to continue to explore new opportunities to enhance cooperation."[35] The 2018 SCM joint communique struck a similar tone, with the allies committing to "strengthen Alliance cyber capabilities in light of the increasing scope of cyber security threats…share information regarding the reorganization of their respective cyber commands in order to promote cyber security cooperation in the future."

These statements show that the US and South Korea both recognize that the cyber domain is increasingly important to the alliance, but there is little detail on how the U.S.-ROK alliance plans to develop a joint cyber deterrence posture. The last sentence quoted above from the 2018 SCM joint communique shows a problem that the alliance faces in crafting a joint cyber deterrence strategy. Both countries are still developing their own strategies, policies, and organizations to address the cyber domain, which complicates developing joint cyber strategies, policies, and operations necessary to create an effective joint cyber deterrence posture.

The U.S. Department of State released major cyber policy documents in 2016 and 2018. The Department of State International Cyberspace Policy Strategy released in March 2016 described a whole-of-government approach to cyber deterrence, using all tools of national power. It stated that the United States would pursue deterrence by denial and deterrence by "cost imposition" (punishment), using diplomatic tools, law enforcement tools, economic tools, military capabilities, and intelligence capabilities.[37] In May 2018, the State Department released "Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats," and it defined a desired end state for U.S. cyber deterrence strategy. This end state would see an "absence of cyber-attacks that constitute a use of force against the United States…and allies" and a "significant, long-lasting reduction in destructive, disruptive, or otherwise malicious cyber activities directed against U.S. interests that fell below the threshold of the use of force."[38] This document also declared that the United States would use both deterrence by denial and deterrence by imposing consequences (punishment) against cyber adversaries.

These end states acknowledge that not all malicious cyber acts can be deterred, particularly lower consequence cyber-attacks, but they are not a clear parallel to the kinetic realm. As has been seen on the Korean Peninsula since 1953, not all lower-level kinetic attacks can be deterred, and the U.S.-ROK alliance focuses on deterring strategic attacks while defending against lower-level attacks. While it is yet unclear what type of cyber-attack would constitute a use of force, deterring all uses of force could be a difficult goal to achieve.

The DoD released its Cyber Strategy in 2018, with "defend forward" as a key tenet. Defined as disrupting or halting malicious cyber activity at its source, a strategy based on defending forward makes alliances vital, and the U.S.-ROK alliance is on the front line against North Korean cyber threats. Regarding deterrence, this document said the Defense Department would "use all instruments of national power to deter adversaries from conducting malicious cyberspace activity that would threaten US national interests, our allies...prioritize securing sensitive DoD information and deterring malicious cyber activities that constitute a use of force against the United States, our allies, or our partners...Should deterrence fail, the Joint Force stands ready to employ the full range of military capabilities in response."[39] This is similar to the State Department's statements on deterrence but does add an extra priority on deterring cyber-attacks that would threaten DoD information security.

South Korea's Ministry of National Defense publishes a Defense White Paper every two years, and cybersecurity has received increasing attention this decade in the white papers. However, the white papers have not clearly discussed cyber deterrence, and have instead focused on defense, organizational policy, human resources, technology acquisition, and international cooperation. Previously quoted in this paper was the 2016 Defense White Paper's statement on guarding against North Korean cyber-attacks on critical infrastructure and military networks. The 2018 Defense White Paper acknowledged that North Korea continues to develop its cyber capability and personnel but refrained from specifically calling North Korea a cyber threat.[40]

In April 2019, South Korea's Blue House published the country's National Cybersecurity Strategy, which mentioned deterrence but did not specify any particular malicious cyber actors. One of the three goals of the strategy is to respond to cyber-attacks, including strengthening "security capabilities to deter cyber threats."[41] To ensure cyber-attack deterrence, the strategy listed taking the following measures:

1) actively respond to all cyber-attacks that infringe upon national security and national interests by concentrating national capabilities,

2) strengthen preventive capacity by building a system that efficiently collects, manages, and eliminates vulnerabilities in cyberspace, and

3) acquire practical capabilities to analyze causes of cyber attacks and identify the culprits.[42]

The cyber deterrence thinking described here sounds more like deterrence by denial, and unlike recent US cybersecurity strategy documents, there is no explicit mention of using all tools of national power to establish a deterrence by punishment posture. Similar to South Korea's Defense White Papers, protection of critical infrastructure and national networks receives top priority in the National Cybersecurity Strategy.

V. APPLYING CYBER DETERRENCE METHODS IN THE U.S.-ROK ALLIANCE

The cyber policy documents released over the last few years by the US and South Korean governments show that they are interested in establishing a cyber deterrence posture, and the U.S.-ROK alliance recognizes the need to deepen their cyber cooperation. Washington and

Seoul also seem to generally agree that deterring cyber-attacks on critical infrastructure and military networks are top priorities, but the allies may have some differences on what methods to use to enforce a cyber deterrence posture. This section will consider the four deterrence methods introduced in section 2 (punishment, denial, entanglement, and norms) and how those methods could be applied to deterring strategic-level North Korean cyber-attacks by the U.S.-ROK alliance, such as on critical infrastructure or military networks or as a force enabler for larger kinetic attacks.

The first method is deterrence by punishment, which US government agencies also have termed deterrence by cost or consequence imposition. This subtle semantic difference may be useful in thinking of all the ways to punish an adversary and get past the association with kinetic attacks, particularly nuclear attacks. All the tools of national power, including diplomatic, information, and economic tools, could be used to punish North Korea. Punishment methods also should include both in-domain punishments and cross-domain (non-cyber domain) punishments.

Table 1. Cyber deterrence by punishment

Options	Pros and Cons
In-domain - Disruption of civilian or military networks - Sabotage of digital military assets - Information operations aimed at sowing social unrest	**Pros** - Places cyber deterrence well within overall U.S.-ROK deterrence posture - Strong deterrent signal against high-impact cyber attacks
Cross-domain - Legal action against cyber corps operating outside of DPRK - Diplomatic sanctions - Targeted economic sanctions - Kinetic strikes on cyber corps or civilian/military infrastructure	**Cons** - Timely, convincing attribution - Appropriate targets and proportionality[43] - Credibility of threat can be doubted

Table 1 summarizes punishment options and the pros and cons of such a posture. The biggest challenge to this method is finding punishments that the United States and South Korea would be able and willing to enforce, that produce a deterrent effect on North Korea, and can be credibly signaled to North Korea. If the allies cannot find punishments that meet those conditions, then they may be forced to pursue one of the other methods.

Table 2. Cyber deterrence by denial

Options	Pros and Cons
- Increase resiliency and ability to recover - Increase redundancy in critical networks and systems - Improve supply chain and personnel security	**Pros** - Increases time and effort for DPRK to achieve goal[40] - Increases failure rate for DPRK - Best practices applicable to cyber defense in other sectors **Cons** - Cannot prevent all attacks - Must stay ahead of adversary's techniques

Table 2 summarizes options and pros and cons for deterrence by denial. Given the challenges with punishments in the cyber domain, this is probably the default cyber deterrence posture. It mostly requires bolstering cyber defenses and credibly signaling to North Korea that cyber attacks will not achieve their desired goal because of those defenses. A significant challenge would be trying to maintain such a posture in the face of a determined, persistent adversary like North Korea, who likely will defeat defenses at some point.[45]

Tables 3 and 4 summarize options and pros and cons for entanglements and norms, the two other cyber deterrence methods introduced by Nye. These two methods would likely work best if combined with either punishment or denial. Lacking a deterrence by punishment or denial posture, deterrence failure with these two methods would leave the U.S.-ROK alliance vulnerable with insufficient defenses or counterattack capability. However, using deterrence by entanglement or norms could open new ways to use non-military tools of power to enforce cyber deterrence, such as by tying the current diplomatic processes on the Korean Peninsula or external economic engagement projects with malicious North Korean cyber behavior. But such options also would require convincing North Korean leadership that these things are in their interest or agreeing to uphold norms, and North Korean history does not suggest that this would be easy or likely to happen.

Table 3. Cyber deterrence by entanglement

Options	Pros and Cons
- Increase DPRK economic and social interdependence on the Internet - Tie current U.S.-DPRK and ROK-DPRK diplomatic processes to malicious DPRK cyber behavior	**Pros** - Can lead to self-deterrence by DPRK and preference for stability - Avoids escalation ladders and cyber arms races **Cons** - DPRK has low degree of interdependence with international economic system - DPRK leadership may resist further interdependence - DPRK leadership views cyber as critical asymmetric tool and integral to war planning

Table 4. Cyber deterrence by norms

Options	Pros and Cons
- Engage DPRK on agreeing to norms in cyberspace - No targeting of civilians in peacetime - Apply laws of armed conflict in cyberspace - Propose cyber confidence building measures to work to agreement on norms[46]	**Pros** - Similar to entanglements **Cons** - Attribution is necessary[47] - DPRK has not adhered to many international norms

VI. CONCLUSION AND RECOMMENDATIONS

Scholars and practitioners are still in early stages of applying deterrence theory to the cyber domain, but it is critical that the US and South Korea more deliberately and explicitly formulate a cyber deterrence posture for their alliance. The existing deterrence posture in the U.S.-ROK alliance is built from the US extended deterrence guarantee, which is backed by US nuclear weapons. Credibility of the extended deterrence guarantee is further bolstered by the US military presence in South Korea. This application of nuclear deterrence theory based on punishment may not directly apply to cyberspace, but broader deterrence theory can be applicable, using other deterrence methods, such as denial, entanglement, and norms.

Yet, like nuclear deterrence, any cyber deterrence strategy must be credible and effectively signaled to be successful. The U.S.-ROK alliance should move beyond stated commitments to increase cyber cooperation to integrating cyber deterrence into the alliance's overall deterrence posture. While integrating cyber deterrence into the U.S.-ROK deterrence posture, the allies also should recognize that cyber deterrence methods contribute to overall cyber strategy and should not be expected to deter all cyber-attacks. Just as cyber deterrence is a component of overall deterrence strategy, cyber deterrence is one component of an overall allied cybersecurity strategy.

With these thoughts in mind, this paper concludes with the following recommendations for cyber deterrence in the U.S.-ROK alliance.

- **The U.S.-ROK alliance should formulate a joint cyber deterrence strategy.** The strategy should be part of overall alliance deterrence strategy. The strategy could be integrated into the Tailored Deterrence Strategy, considering the Tailored Deterrence Strategy addresses North Korea's strategic and asymmetric capabilities. The cyber deterrence strategy must first define what is to be deterred and what methods will be used to deter, and it should clarify roles for the US and South Korea. While deterring cyber-attacks that produce strategic effects should be the focus, employing persistent engagement to address lower level attacks could reduce the scope, scale, and frequency of such attacks. Finally, the strategy should address an issue not explored in this paper, which is pursuing partnerships in the region, namely China. Beijing's relationship with Pyongyang and the presence of North Korean cyber agents in China mean the U.S.-ROK alliance should seek ways to engage China on North Korea's cyber activities.[48]
- **Build on existing cooperative mechanisms to form a combined cybersecurity unit under the Combined Forces Command**. The US and South Korean militaries have a Cyber Cooperation Working Group, and DoD established a cyber operations-integrated planning element within U.S. Forces Korea last year.[49] A combined cybersecurity unit would strengthen these efforts and signal to North Korea that the alliance is serious about deterring cyber threats. A combined unit also could make it easier to integrate efforts, share intelligence and practices, and dynamically deter, defend, and respond to North Korean cyber-attacks.

- **Improve understanding of North Korean cyber strategy.** A cyber deterrence strategy or combined unit will only succeed if the allies better understand the adversary. What are North Korea's tactical, operational, and strategic goals in the cyber domain, and what cyber capabilities could they use to achieve these objectives? Why has there not been a North Korean cyber-attack that produced strategic effects yet? Can North Korean cyber behavior be predicted and preempted, and is the cyber activity a precursor of kinetic or other asymmetric attacks?[50] How can North Korea be engaged on cyber norms and interdependence? Better understanding these types of questions is necessary for tailoring a cyber deterrence strategy against North Korea, and the U.S.-ROK alliance needs to work together and with external analysts to better understand a hard intelligence target like North Korea.

- **For South Korea, leverage the U.S.-ROK alliance as an asymmetric advantage**. South Korea has economic and technological advantages over North Korea, but the U.S.-ROK alliance is Seoul's "core asymmetric factor."[51] The United States has successfully provided extended deterrence against strategic threats to South Korea for over 60 years, and it would be prudent for Seoul to apply this advantage now to the cyber domain. In particular, the US can improve options for deterrence by punishment, while South Korea focuses on denial and entanglement. For example, Washington has more power to employ economic sanctions and may be more willing and able to use powerful cyber tools against North Korea. South Korea can continue to improve its domestic cyber defenses and resiliency, which contributes to deterrence by denial. Relying on the US for punishment also could leave Seoul more space to continue diplomatic and economic engagement, with a goal of deterrence by entanglement and norms. However, South Korea should not become overly reliant on Washington or stretch the US extended deterrence guarantee too far.

- **For the United States, embrace South Korea as a partner in defend forward.** Malicious North Korean cyber activity is a threat to the US, but South Korea is the primary target of North Korean cyber-attacks. Working with the South Korean military, civilian government agencies, and private industry will improve US understanding of North Korean cyber capabilities, intentions, and operations. Deterring cyber-attacks on a critical ally is clearly in US national interests, but a partnership with South Korea will also help prevent North Korean cyber-attacks from reaching US targets.

DISCLAIMER

This paper may not be cited or redistributed without the permission of the author. Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Air University, the United States Air Force, the Department of Defense, or any other U.S. Government agency.

Author Bio

Dr. James E. Platte

Dr. James E. Platte is an Assistant Professor with the U.S. Air Force Center for Strategic Deterrence Studies (CSDS). His teaching and research focus on nuclear deterrence and counterproliferation, with a regional focus on East Asia. Prior to joining CSDS in 2017, Dr. Platte was an intelligence research specialist with the U.S. Department of Energy, and he also has worked on nuclear counterproliferation with the Defense Intelligence Agency and the National Nuclear Security Administration. He received his PhD in International Relations from The Fletcher School of Law and Diplomacy at Tufts University and has held research fellowships with the National Bureau of Asian Research, East-West Center, Pacific Forum, the Council on Foreign Relations, and the Harvard Kennedy School.

NOTES

1. "U.S. Relations With the Republic of Korea," U.S. Department of State, 17 July 2018, https://www.state.gov/u-s-relations-with-the-republic-of-korea/.
2. "Joint communique of 50th U.S.-ROK Security Consultative Meeting," United States Forces Korea, 31 October 2018, http://www.usfk.mil/Media/News/Article/1679753/joint-communique-of-50th-us-rok-security-consultative-meeting/.
3. Jeffrey Knopf, "The Fourth Wave in Deterrence Research," *Contemporary Security Policy* 31, no. 1 (April 2010), 1-2.
4. Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/17), 46.
5. Aaron F. Brantly, "The Cyber Deterrence Problem," Proceedings of the 10th International Conference on Cyber Conflict, NATO Cooperative Cyber Defence Centre of Excellence, 2018, 32.
6. Lawrence Freedman, *Deterrence* (Malden, MA: Polity Press, 2004), 10-11.
7. Glenn Snyder, *Deterrence and Defense: Toward a Theory of National Security*, Princeton, NJ: Princeton University Press, 1961.
8. Knopf, "The Fourth Wave in Deterrence Research," 10.
9. Nye, "Deterrence and Dissuasion in Cyberspace," 45.
10. Brantly, "The Cyber Deterrence Problem," 33-34.
11. Nye, "Deterrence and Dissuasion in Cyberspace," 53.
12. Nye, "Deterrence and Dissuasion in Cyberspace," 58.
13. Nye, "Deterrence and Dissuasion in Cyberspace," 58-61.
14. Nye, "Deterrence and Dissuasion in Cyberspace," 60.
15. "Summary of Department of Defense Cyber Strategy," U.S. Department of Defense, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, 1.
16. Republic of Korea Ministry of National Defense, *2016 Defense White Paper*, Seoul: Ministry of National Defense, 2017, 77-79.
17. Donghui Park, "Cybersecurity Spotlight: South Korea," University of Washington Henry M. Jackson School of International Studies, January 12, 2016, https://jsis.washington.edu/news/cybersecurity-spotlight-south-korea/.
18. Brantly, "The Cyber Deterrence Problem," 34.
19. "Mutual Defense Treaty Between the United States and the Republic of Korea," Yale Law School Lillian Goldman Law Library, 1 October 1953, https://avalon.law.yale.edu/20th_century/kor001.asp.
20. "Joint Communiqué of the 49th ROK-U.S. Security Consultative Meeting," U.S. Department of Defense, October 28, 2017, https://dod.defense.gov/Portals/1/Documents/pubs/20171028-Joint-Communique-OSD-MND-October-17-Final-version.pdf.
21. "Joint communique of 50th U.S.-ROK Security Consultative Meeting."
22. "Joint Communique of the 45th ROK-U.S. Security Consultative Meeting," U.S. Department of Defense, October 2, 2013, https://dod.defense.gov/Portals/1/Documents/pubs/Joint%20Communique_%2045th%20ROK-U.S.%20Security%20Consultative%20Meeting.pdf.
23. "Joint Press Conference with Secretary Hagel and Minister Kim Kwan-jin in the Republic of Korea," U.S. Department of Defense, October 2, 2013, https://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5316.
24. "Nuclear Posture Review," U.S. Department of Defense, 2018, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF, 21.
25. Young-joon Lee, Hyuk-jin Kwon, Jae-il Lee, and Dong-kyoo Shin, "The Countermeasure Strategy Based on Big Data against North Korea Cyber-attacks," *The Korean Journal of Defense Analysis* 30, no. 3 (September 2018), 441.
26. Christine Kim, "North Korea hackers stole South Korea-U.S. military plans to wipe out North Korea leadership: lawmaker," Reuters, 10 October 2017, https://www.reuters.com/article/us-northkorea-cybercrime-southkorea/north-korea-hackers-stole-south-korea-u-s-military-plans-to-wipe-out-north-korea-leadership-lawmaker-idU.S.KBN1CF-1WT.
27. Lee et al., "The Countermeasure Strategy Based on Big Data against North Korea Cyber-attacks," 438.
28. Duk-Ki Kim, "The Republic of Korea's Counter-asymmetric Strategy," *Naval War College Review* 65, no. 1 (Winter 2012), 4.
29. ROK MND, *2016 Defense White Paper*, 78.

NOTES

30. “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command,” U.S. Cyber Command, April 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010, 6.
31. Uri Tor, “’Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence,” *The Journal of Strategic Studies* 40, no. 1-2 (2017), 102.
32. Tor, “’Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence,” 106-107.
33. Donghui Park, “Cybersecurity Strategy Advice for the Trump Administration: U.S.-South Korea Relations,” University of Washington Henry M. Jackson School of International Studies, February 7, 2017, https://jsis.washington.edu/news/cybersecurity-strategy-advice-trump-administration-us-south-korea-relations/.
34. “Joint Fact Sheet: The United States-Republic of Korea Alliance: Shared Values, New Frontiers,” The White House, October 16, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/10/16/joint-fact-sheet-united-states-republic-korea-alliance-shared-values-new.
35. “Joint Communiqué of the 49th ROK-U.S. Security Consultative Meeting.”
36. “Joint communique of 50th U.S.-ROK Security Consultative Meeting.”
37. “Department of State International Cyberspace Policy Strategy,” U.S. Department of State, March 2016, https://2009-2017.state.gov/documents/organization/255732.pdf, 20-23.
38. “Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats,” U.S. Department of State, May 31, 2018, https://www.state.gov/recommendations-to-the-president-on-deterring-adversaries-and-better-protecting-the-american-people-from-cyber-threats/.
39. “Summary of Department of Defense Cyber Strategy,” 4-5.
40. “2018 년 국방백서(2018 Defense White Paper),” Republic of Korea Ministry of National Defense, December 2018, http://www.mnd.go.kr/user/mnd/upload/pblictn/PBLICTNEBOOK_201901160236460390.pdf, 18-22.
41. “National Cybersecurity Strategy,” Cheong Wa Dae National Security Office, April 2019, https://www.krcert.or.kr/filedownload.do?attach_file_seq=2162&attach_file_id=EpF2162.pdf.
42. “National Cybersecurity Strategy.”
43. Brantly, “The Cyber Deterrence Problem,” 45.
44. Nye, “Deterrence and Dissuasion in Cyberspace,” 56.
45. Nye, “Deterrence and Dissuasion in Cyberspace,” 57.
46. Nye, “Deterrence and Dissuasion in Cyberspace,” 61.
47. Nye, “Deterrence and Dissuasion in Cyberspace,” 60.
48. Park, “Cybersecurity Strategy Advice for the Trump Administration: U.S.-South Korea Relations.”
49. Mark Pomerleau, “Why DoD is starting a new cyber cell on the Korean Peninsula,” *Fifth Domain*, 20 April 2018, https://www.fifthdomain.com/dod/cybercom/2018/04/20/why-dod-is-starting-a-new-cyber-cell-on-the-korean-peninsula/.
50. Lee et al., “The Countermeasure Strategy Based on Big Data against North Korea Cyber-attacks,” 451.
51. Kim, “The Republic of Korea’s Counter-asymmetric Strategy,” 17.