Space and Defense

Volume 11
Number 0 *Volume 11 Issue 1 (Spring 2019)*

Article 5

March 2019

Communicating Cyber Consequences

Timothy Goines
United States Air Force Academy, timothy.goines@edu.edu

Recommended Citation
Goines, Timothy (2019) "Communicating Cyber Consequences," *Space and Defense*: Vol. 11: No. 0, Article 5.
DOI: 10.32873/uno.dc.sd.11.01.1093
Available at: https://digitalcommons.unomaha.edu/spaceanddefense/vol11/iss0/5

Communicating Cyber Consequences

Timothy Goines

More consideration ought to be accorded "loud" cyber weapons for signaling resolve in 21st century deterrence contests.

"Deterrence is at times a necessary or useful instrument of foreign policy, but the correct and prudent use of deterrence strategy is by no means self-evident or easily determined in all circumstances."[1]

In their seminal text, Alexander L. George and Richard Smoke thoroughly examined the topic of deterrence, tracing its historical roots and conducting case studies on its use.[2] The product of this intense study was a formula that encapsulates the essence of deterrence theory. "In its simplest form, deterrence is merely a contingent threat: 'If you do x, I shall do y to you.' If the opponent expects the costs of y to be greater than the benefits of x, he will refrain from doing [x]; he is deterred."[3] Since its pronouncement, this formula has been codified in Department of Defense (DoD) doctrine, most recently in the DoD's "Deterrence Ops Joint Operating Concept" and it's "Cyber Strategy."[4]

Unfortunately, in this simple form, the formula is misleading. It tends to convince the reader that deterrence is a simple balancing act and all a deterring state must do is increase the costs to outweigh the benefits. This omits a fundamental aspect of deterrence, the actor's *perception* of the anticipated costs and benefits. In other words, it is not the *actual* costs and benefits that the actor weighs within this formula, but the *anticipated* costs and benefits. Therefore, if an actor perceives the costs to be higher than the actual costs, the deterring party benefits from this miscalculation. Conversely, if an actor perceives the costs to be lower than the actual costs, it is to the deterring party's detriment, regardless of the actual costs.

A more accurate formulation is as follows: if the *anticipated* costs of a proposed action exceed the *anticipated* benefits of that action, the actor is less likely to engage in the action and is deterred. This revised formulation flows naturally from the original. As George and Smoke note, it is a contingent threat, and if the opponent *expects* the costs to be greater, then he is deterred.[5] Additionally, this formulation, revised from DoD orthodoxy, makes sense: the actor in practice is unable to know precisely the costs and benefits prior to his action; those occur after and in response to the act.

Consequently, formulation of an effective deterrence strategy should focus on increasing

[1] Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), 3. Maj. Timothy Goines, USAF is a faculty member of the Department of Law, U.S. Air Force Academy.

[2] See generally, George and Smoke, *Deterrence in American Foreign Policy*.

[3] George and Smoke, *Deterrence in American Foreign Policy*, 48.

[4] Department of Defense (DOD), Deterrence Ops Joint Operating Concept, Version 2.0 (Washington, DC: Office of the Secretary of Defense, December 2006), http://www.dtic.mil/doctrine/concepts/joint_concepts/joc_deterrence.pdf; and DOD, Department of Defense Cyber Strategy (Washington, DC: Office of the Secretary of Defense, April 2015).

[5] George and Smoke, *Deterrence in American Foreign Policy*, 48.

anticipated costs and decreasing anticipated benefits. This article focuses on the former in the cyber domain. Specifically, how should the United States increase the anticipated costs of cyber actions in order to effectively deter adversaries?

The key to increasing anticipated costs in the cyber domain is not novel or unique; nations have effectively communicated and continue to communicate consequences to their adversaries within other domains (i.e. air, land, and sea) through declaratory policies, signaling, and response actions. Therefore, the solution to increasing anticipated costs in the mind of the adversary within the cyber domain is a familiar one. But, perhaps the most difficult aspect of communicating cyber consequences is not the *ways* to increase costs, but the selection of the appropriate *means* to effectively communicate within the cyber domain—one that possesses the appropriate characteristics. This article proposes a solution, which is, loud cyber weapons.

Loud cyber weapons are cyber weapons that can be definitively traced to the deterring party. When using these new cyber weapons, the "deterrer" does not obscure the operation or its source from being discovered by the victim and correctly attributed. Currently, much of military cyber operations are kept secret in an attempt to avoid detection by the target nation and, if discovered, attribution. Loud cyber weapons would turn this paradigm on its head, exposing its means, methods, and source to target nations and the international community.

This article first explores the foundations of an effective deterrence strategy, evaluating examples that demonstrate it in practice, and affirming the importance of communication for effective deterrence policy. In the second part, this article highlights the lack of communication within the cyber domain, delineates the characteristics of effective signaling and follow-through, discusses how each is present in effective signaling examples, and uses these characteristics to evaluate the proposed solution—use of loud cyber weapons.

DETERRENCE THEORY FOUNDATIONS

Requirements

George and Smoke articulated three requirements of deterrence: "(1) the full formulation of one's intent to protect a nation; (2) the acquisition and deployment of capacities to back up the intent; and (3) the communication of the intent to the potential 'aggressor.'"[6] Each of these three requirements serve a critical purpose, giving rise to particular attributes of an effective deterrence strategy: a system of rules, credibility, commitment, and communication. A short discussion of these requirements and attributes will assist in identifying characteristics of effective communication, which will be used to analyze the proposed solution for the cyber domain.

The first requirement, the full formulation of one's intent to protect a nation, is distilled into a system of rules. In this context, a system of rules is a domestic policy wherein the deterring state defines its thresholds for certain adverse actions (considering specific domestic targets and competing actors) and corresponding responses. It is created by considering a number of factors, including "the decision to attempt deterrence in a given case…the perception and analysis of the threat…the U.S. national interests in the case, and the determination of what kinds of responses…" are appropriate.[7] The process of fully forming intent serves two purposes

[6] Ibid., 64.

[7] Ibid.

for a deterring state. First, it organizes the deterring state's thoughts on unwanted adverse actions into a practical, rule-based approach. Secondly, it informs the deterring state's executive on what actions are to be deterred and what institutional tools are available for policy implementation.

Second, a deterrence strategy must include the acquisition and deployment of capacities to back up the intended response. This serves to lend credibility to a deterrence strategy and to demonstrate that a deterring state is committed to enforce its system of rules. Naturally, if the adversary is not convinced that the deterring state has capability to impose costs, the actor is unlikely to be deterred. For example, if the deterring state has a system of rules that requires a response when an adversary enters its territorial waters, yet it lacks adequate Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) or naval assets, then deterrence, when tested, is likely to fail.

Finally, an effective deterrence strategy must communicate intent to the potential aggressor. While the first two requirements of deterrence are critically important (and the emphasis of George and Smoke's extensive study), the focus of this paper is on this third requirement—communicating potential consequences to the adversary. If an actor does not know about potential costs, the actor cannot justify changing its behavior. Within this requirement, other attributes of deterrence strategy are empowered. For example, in order for a system of rules to be effective, they must be communicated to inform the adversary. Likewise, the credibility of a deterring state's intent is only effective if its capabilities are understood by the adversary, convincing a challenger that cost imposition by the defense is possible. Lastly, a nation must communicate its commitment to a deterrence strategy, convincing the target actor that political will for cost imposition is likely.

Oftentimes, communication of a deterrence strategy is accomplished in three ways, typically employed sequentially: declaratory policy, signaling, and follow-through. First, a deterring state should make their system of rules public through declaratory policy. This communicates to adversaries which actions and targets will produce a negative response and the likely magnitude of this response. Historically, with respect to nuclear deterrence, the United States declared that any launch of a nuclear weapon would result in a retaliatory strike.

In the event declaratory policy itself does not deter and a malicious act is anticipated, a deterring state may seek to further communicate their credibility and commitment through the use of signaling. Signaling by a deterring state demonstrates intent to enforce its system of rules.[8] For example, if a country has a system of rules that declares an invasion will be met with significant force, this state may demonstrate its credibility and commitment by amassing troops along the border. It should be noted that signaling can take many forms, from a traditional "show of force" to less direct methods, like conducting a public test on a new weapons system.[9]

Finally, if deterrence is still not successful after signaling, a state may actually impose the corresponding costs in response to the malicious act; in other words, it may follow-through on the threatened costs by imposing

[8] Ibid.

[9] See, for example, the recent Chinese ASAT test – Bill Gertz, "China ASAT Test Part of Growing Space War Threat," *Washington Free Beacon* (February 23, 2018).

them. This further reinforces the state's credibility and commitment to its system of rules. While it may not serve the deterrent function for the initial challenge, it does serve as a deterrent for future malicious acts. For example, if another state probes a deterring state (despite the various warnings), the state may respond with considerable force in order to communicate their capabilities and commitment against future invasions.

The bottom line is that these forms of communication are critical to the success of a deterrence strategy because they apprise an adversary of potential costs, increasing their estimation of the anticipated costs. A crucial component of any deterrence strategy is to ensure the communications piece is addressed and employed.

Case Studies of Deterrence in Practice

States routinely employ this methodology when attempting to deter other states from engaging in certain conduct. The following is a brief discussion of four relevant examples where the deterring state used tactics in an effort to communicate its system of rules, credibility, and commitment to adversaries. In some cases, their efforts were effective; in others, a missing component undermined their larger deterrence policy.

1. U.S. Deterrence of a Soviet Union Nuclear Strike

Perhaps the best example of where a deterring state made repeated efforts to communicate the potential costs of a particular action is the United States attempt to deter the Soviet Union from engaging in nuclear warfare throughout the Cold War. Notably, the United States successfully employed the three requirements for an effective deterrence strategy. First, through the trials of the Cold War and its aftermath, the United States fully formed its intent to protect itself and its allies against potential nuclear strikes and, in the event of a nuclear attack, to respond with a retaliatory strike. Second, the United States developed, and still maintains, the acquisition and deployment capacities to back up the intent.

Most importantly, though, the United States communicated this policy, and used signaling to convince potential adversaries that it was committed to the policy and that the threat was credible. Over the course of the Cold War, the United States threatened the Soviet Union that any nuclear launch would lead to a "massive retaliation" whereby the United States would destroy the full range of value targets in the Soviet Union.[10] When the declaratory policy alone did not appear to be deterring the Soviet Union, the United States then demonstrated its credibility and commitment to this threat through signaling.

In this instance, signaling was not amassing troops along a border, but rather, the development, testing, and deployment of nuclear weapons across the nuclear triad. For example, the United States conducted 1,024 tests of their nuclear weapons from 1945–1992, more than any other country.[11] This testing sent a strong message to the Soviet Union that the United States had both the commitment and credibility necessary to enforce its policy. As a result, the Soviet Union could better estimate the potential costs and factor them into its decision calculus.

2. U.S. Deterrence of North Korea

A more contemporary example can be found in recent events between the United States and North Korea. Since its establishment in the 1950s, North Korea's nuclear

[10] Amy Woolf, *U.S. Nuclear Weapons: Changes in Policy and Force Structure*, CRS Report for Congress (January 23, 2008).

[11] Rebecca Harrington, "The dark history of nuclear testing reveals one uber-powerful front-runner," *Business Insider* (January 6, 2016).

development program has been the subject of intense scrutiny from the United States and the international community.[12] With varying degrees of success, many diplomatic efforts have been attempted throughout the years to stop the program and halt the proliferation of nuclear weapons.[13] Upon the election of President Donald Trump, the U.S. approach to North Korea became a more aggressive deterrence approach—the United States sought to deter North Korea from developing and testing nuclear weapons through more aggressive rhetoric and signaling.

For example, after North Korea launched its twentieth ballistic missile in 2017 and tested what many believed to be a thermonuclear device, President Trump announced that he was stationing three carrier strike groups in the area of operations in close proximity to North Korea.[14] A single carrier strike group is typically comprised of an aircraft carrier, which can hold up to sixty aircraft (including F/A-18 strike fighters), along with destroyers and cruisers, both of which are equipped with the Aegis anti-ballistic missile system and Tomahawk cruise missiles.[15] They can also be accompanied by attack submarines, but their locations remain secret.[16] While stationed near North Korea, the three carrier strike groups conducted a joint exercise, with participation from South Korean and Japanese warships.[17]

As with the first example, the United States followed the expected pattern, ensuring each of the three requirements were met. First, as mentioned above, the United States during the Cold War fully formed its nuclear weapons policy—making a clear statement that the use of nuclear weapons is not tolerated.

However, in recent years, the United States has gone even further, focusing not only on the use of nuclear weapons, but also their development and testing. For example, the United States ratified the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) in 1968 in an effort to reduce the spread of nuclear weapons technology.[18] More recently, after the Cold War, the United States signed two Strategic Arms Reduction Treaties (START and New START) to reduce the superpower stockpiles of nuclear weapons.[19]

The two efforts make clear that the United States wants to limit the number of nuclear weapons and the number of nations with nuclear weapons capabilities. For example, when reports surfaced that Iran was violating its commitment to the NPT and developing its nuclear program, the United States attempted to thwart it, eventually reaching a (temporary) deal with Iran to stop their nuclear weapons development.[20] Given these measures, the United States has fully formed its desire to stop the proliferation of nuclear weapons.

Second, to back up its intent, the United States indicated that it will use either the threat of nuclear strike or conventional weapons to prevent the proliferation of

[12] Nuclear Threat Initiative, "North Korea," *NTI*, https://www.nti.org.

[13] Ibid.

[14] Ankit Panda, "What 3 U.S. Supercarriers in the Asia-Pacific Means for North Korea," *The Diplomat* (October 30, 2017).

[15] Brad Lendon, "North Korea: 3 U.S. aircraft carriers creating 'worst ever' situation," *CNN* (November 20, 2017).

[16] Ibid.

[17] Ibid.

[18] "Treaty on the Non-Proliferation of Nuclear Weapons (NPT)." UN Department for Disarmament Affairs, United Nations, http://disarmament.un.org/treaties/t/npt.

[19] Department of State – New START Treaty, "Treaty Between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms" (April 8, 2010).

[20] BBC News, "Iran nuclear deal: Key details," *BBC.com* (October 13, 2017).

nuclear weapons. In either case, the United States has the acquisition and deployment capacities to use either option, lending credibility to the potential costs.

Finally, the United States communicated this policy and, more recently, employed signaling to demonstrate its resolve. For example, the United States communicated this policy directly to North Korea and its closest ally, China. First, the United States made clear through press releases and otherwise that it would not tolerate North Korea's continued development of nuclear weapons.[21] Through the course of this administration and the previous one, there is no question on the U.S. stance.

Unfortunately, this policy alone did not deter North Korea from further developing its nuclear weapons program. As a result, President Trump took the next step in the deterrence communication process and signaled U.S. commitment and capability by stationing the three carrier strike groups in the area of operations. This sent a powerful message. By stationing these groups near North Korea, which have the capacity to shoot down ballistic missiles with the onboard Aegis system, the U.S. communicated both the credibility of its intent and the commitment to follow through. This communication allowed North Korea to conduct a more accurate assessment of the potential costs of their nuclear weapons development.

Fortunately, a follow-through was not required as North Korea made a commitment to halt their nuclear weapons program.[22] In turn, the United States softened their deterrence efforts towards North Korea. Whether this commitment will be successful is yet to be seen; however, the use of deterrence to get North Korea to negotiate with the United States was rather successful.

3. China's Deterrence of Space-Based Operations

In 2018, China conducted another Anti-Satellite weapon (ASAT) test under the guise of a missile defense interceptor trial.[23] In the test, China used the DN-3 anti-satellite interceptor, which is capable of being launched from land, directly ascending, and striking a satellite orbiting Earth.[24] For the United States, which relies heavily on satellites for communication, location data, and intelligence, the message was loud and clear: China has the commitment and credibility to engage in space warfare and disable space-based operations. However, when considering what larger deterrence message China was attempting to send, the message is more ambiguous.

China has likely fully formed its intent to protect their nation, and the ASAT test (and the many before it) demonstrates that China possesses the acquisition and deployment of capacities to back up the intent. But, as far as the communication requirement, China failed in the first step—to communicate a declaratory policy or system of rules. As a result, what are the United States and other similarly situated nations supposed to take from this ASAT test and its predecessors? Without a clear system of rules, the target states are left with little information to predict future behavior and calculate potential costs.

[21] President Trump has repeatedly tweeted about North Korea and its leader, Kim Jung Un. See, for example, Peter Baker and Michael Tackett, "Trump Says His 'Nuclear Button' Is 'Much Bigger' Than North Korea's," *New York Times* (January 2, 2018).

[22] Joshua Berlinger, "Singapore Summit: Asia Reacts to the Trump-Kim meeting," *CNN*, 12 June 2018, wwww.cnn.com.

[23] Bill Gertz, "China ASAT Test Part of Growing Space War Threat," *Washington Free Beacon* (February 23, 2018).

[24] Ibid.

So, while China’s ability to wage space war is undisputed, the larger deterrence message is lost on potential adversaries.

With that said, there can be some strategic benefits to ambiguity (e.g., How will China use ASAT capabilities in the future? What could trigger an ASAT response? What action is China trying to deter?). This ambiguity could serve China well, given the United States and other countries’ reliance on space assets and their significant vulnerabilities. Ambiguity could cause doubt in the mind of adversaries, fearing that certain actions may result in certain conduct. Even so, this level of decision-making paralysis is unlikely. What is more likely is that, given a lack of clear rules, adversaries will use this ambiguity as justification to “poke and prod” China to determine what they can do and what provokes a response.

What is clear is that China’s ASAT test did communicate something, but the scope of its deterrent effect is less certain. This emphasizes the importance of each step of an effective deterrence strategy, including the need to communicate the system of rules.

4. U.S. Deterrence of China’s Claim to the South China Sea

In August of 2017, the U.S.S. John S. McCain, a U.S. Navy destroyer, traveled close to Mischief Reef in the Spratly Islands, an area over which China has territorial disputes with its neighbors, including Brunei, Malaysia, the Philippines, Taiwan, and Vietnam.[25] The United States has long criticized China’s construction of islands, used for military purposes, throughout the South China Sea and has asked for more international participation regarding the area.[26] There is little doubt that this maneuver was meant to send a message regarding the U.S. position. In fact, this was the third mission of this kind (a freedom of navigation operation [FONOP]) during the Trump presidency, with the administration vowing to conduct more operations in the area.[27]

While it may seem at first glance that this was not a deterrence operation, it was. The United States was attempting to deter China from continuing to claim the South China Sea as its territory. This particular scenario follows the expected pattern. First, the United States declared its dissatisfaction for the tactic used by China to expand its territorial waters, especially over a highly traversed area in the South China Sea, and repeatedly warned that it will not recognize the area as China’s territory. Second, the United States demonstrated the acquisition and deployment capacities to be able to back up its intent that this area remain international waters; namely, by traversing it with naval sea craft.

Finally, the United States communicated its stance on the South China Sea to China and the international community on several occasions, demanding that China stop claiming land within the area.[28] The United States attempted diplomatic efforts to stop China’s militarization. For example, President Obama urged a peaceful resolution in May 2016.[29] The United Nations found that China had no legal basis to claim historic rights for the bulk of the South China Sea (which the United States supported).[30] Unfortunately, such efforts were unsuccessful. Thus, the United States moved

[25] Idrees Ali, “U.S. destroyer challenges China's claims in South China Sea,” *Reuters* (August 10, 2017).
[26] Ibid.
[27] Ibid.
[28] William Pesek, “Making Sense Of The South China Sea Dispute,” *Forbes* (August 22, 2017).
[29] Katie Hunt, “South China Sea: Court rules in favor of Philippines over China,” *CNN* (July 12, 2016).
[30] Ibid.

to the next step in the process—signaling—by sending the U.S.S. John S. McCain into the area.

It is important to note that the United States used a U.S. Navy Destroyer to conduct this FONOP. Instead of using commercial sea craft, which might communicate a desire to have freedom of navigation, the United States used a U.S. Navy ship, essentially informing China that the United States desires to have freedom of navigation in this area and will ensure this by force, if necessary. So, when the U.S.S. John S. McCain was approached by two Chinese warships, the destroyer had the necessary weapons to respond, if provoked.

While resolution of China's claims over the South China Sea is yet to be determined, this operation is a good example of deterrence strategy in action. The operation was the latest in a series meant to signal U.S. displeasure with China's policy and a willingness to engage, if necessary. As the United States continues its stance on China's policy, the recent series of FONOPs leave little doubt over U.S. resolve, commitment, and credibility.

THE CYBER DOMAIN AND DETERRENCE

Given the number of nations with cyber capabilities, the cyber domain has become a viable space to employ deterrence actions. Although it is a different domain analytically, the requirements of an effective deterrence strategy *remain the same* and the need to communicate the potential consequences remains paramount. The second part of this article explores how to best communicate a state's deterrence policy within the cyber domain. This begins with recognition of a fundamental problem with the current employment of cyber actions. Then, it evaluates requirements of a signal and follow-through sequence, discussing how these can be found in examples of deterrence in practice. Finally, it applies these requirements to the proposed solution—loud cyber weapons.

At the outset, it should be noted that this article focuses on how best to employ actions within the cyber domain for the purpose of deterrence, whether those actions deter an adversary in the cyber domain or in other domains (i.e., land, sea, air, or space). In other words, deterrence actions can have an intra-domain effect and a cross-domain effect. This article does not attempt to distinguish between the two, as most traditional deterrence actions have similar potential effects. Rather, this article focuses on how to employ actions within the cyber domain to deter adversaries both inside and outside of the cyber domain.

A Fundamental Problem with Current Cyber Employment

Previous examples serve to demonstrate the importance of communicating a deterrence strategy through declaratory statements, signaling, and follow-through; communication allows the adversary to understand the system of rules, commitment, and credibility and better calculate the potential costs. Unfortunately, communication within the cyber domain has proven elusive. Herein lies a fundamental problem with the current cyber employment. In short, cyber capable nations employ virtually no tactics in the cyber domain in an effort to communicate potential costs, the credibility of potential cost imposition, or its commitment to imposing these costs. There are various reasons for this.

One significant contributing factor is that nearly all cyber operations are classified as "Top Secret." For example, the Presidential

Policy Directive that used to govern U.S. cyber operations policy (PPD 20) itself was classified as Top Secret. It was recently replaced by President Trump, but the new order is also classified.[31] Another example of the classified nature of cyber operations is the Vulnerabilities Equities Process (VEP). Only recently, President Trump released an unclassified version of the document, describing the process by which the United States assesses known cyber vulnerabilities and risks to national security, the American people, and the dissemination of information.[32] This process existed, in some form, since 2008. While a redacted version of the document emerged through a Freedom of Information Act request in 2016, it was only recently communicated to the U.S. public in un-redacted form.[33]

Regardless of the reason for its classification, the covert nature of cyber operations creates a lack of communication within the cyber domain. For example, there have been virtually no publicly acknowledged cyber actions by the United States within the last twenty years. This is not to say that there have not been cyber actions conducted by the United States. For example, the cyber-worm "Stuxnet" unleashed on Iran's nuclear facility has been reportedly attributed to a joint operation between the United States and Israel.[34] Similarly, Edward Snowden released documents in 2013 that revealed a cyber operation involving the United States hacking into Tsinghua University and Huawei, China's largest telecommunications company.[35] Likewise, in the early years of the Obama administration, the United States reportedly developed a cyber operation, Nitro Zeus, which was designed to disable Iran's air defenses, communications systems, and power grid.[36] The operation was meant to be employed if diplomacy failed to curb Iran's nuclear weapons program.[37]

None of these operations were ever acknowledged by the United States, which means that an adversary has little-to-no information regarding U.S. capabilities, the credibility of its threat to impose costs, and the U.S. commitment to imposing them. Instead, from a potential adversary's perspective, the absence of cyber operations conveys that the United States lacks the capability to impose costs, credibility regarding threats, the commitment to follow through, or a combination of these three, within the cyber domain. This does little to alter the decision-making calculus or increase the likelihood of deterring the adversary.

COMMUNICATING CONSEQUENCES IN THE CYBER DOMAIN

Given this fundamental problem, the key to increasing anticipated costs in the cyber domain is to communicate the potential consequences through cyber actions; specifically, consequences that an adversary

[31] Ellen Nakashima, "Trump Gives the Military More Latitude to Use Offensive Cyber Tools against Adversaries," *The Washington Post* (August 16, 2018).

[32] White House, "Vulnerabilities Equities Policy and Process for the United States Government," (November 15, 2017), accessible at https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

[33] Electronic Privacy Information Center, "Vulnerabilities Equities Process," Epic.org, accessible at https://epic.org/privacy/cybersecurity/vep/.

[34] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired* (3 November 2014), accessible at https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[35] Kenneth Rapoza, "U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press," *Forbes* (June 22, 2013).

[36] David E. Sanger and Mark Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *The New York Times* (February 16, 2016).

[37] Ibid.

could suffer within the cyber domain. As noted above, the use of cyber actions in this manner is not limited to intra-cyber domain deterrence. Potential consequences within cyber can deter adversary actions both inside and outside the cyber domain.

This is not a novel or unique solution. As noted in our previous examples, nations effectively communicated and continue to communicate consequences to their adversaries within other domains (i.e., air, land, and sea) through a declaratory policy, signaling, and follow-through. Thus, the notion of increasing anticipated costs in the mind of the adversary within the cyber domain is a familiar one. However, the challenge arises when a deterring state must determine the means to effectively communicate signaling and follow-through within the cyber domain. This challenge becomes particularly difficult when considering both signaling and follow-through.

Declaratory Policy

The initial step of communication (a declaratory policy) is fairly straight forward. A deterring state should communicate its declaratory policy through press releases, speeches, and other engagements with the international community. Providing a system of rules to potential adversaries makes it clear what actions the deterring state intends to respond to and what targets it intends to protect. In regards to cyber actions, a deterring state should clarify their intent to use cyber actions as a mechanism to impose costs, specifically highlighting the potential use of cyber acts to deter adversaries regardless of the domain.

For example, the United States has already engaged in a version of this throughout the last ten years. In fact, the National Cyber Strategy, updated by President Trump in September 2018, articulates that the United States will impose consequences "to deter future bad behavior."[38] Admittedly, this policy, and its predecessors, lack clarity and specificity. For example, it states that it will impose consequences on "malicious cyber actors in response to their activities against our nation," but it does not define "malicious" or what activities would trigger a response action.[39]

Additionally, aside from these rather ambiguous proclamations, the United States rarely communicates more specific threats. For example, in the Stuxnet and Nitro Zeus operations above, the United States could have communicated a specific declaratory policy to Iran that any continued development of their nuclear weapons program would result in a debilitating cyber response. At the very least, this would have drawn a clear line in the sand, allowing Iran to better understand the possible costs and consider those costs prior to continuing their nuclear weapons program.

The importance of a clear declaratory policy should not be undervalued. Lack of clarity does not usually serve to benefit the deterring state. As noted in the Chinese ASAT test discussed above, failure to communicate the system of rules typically serves to confuse the adversary and frustrate deterrence efforts. Naturally, adversaries are more likely to use this ambiguity as an excuse to "poke and prod" a deterring state to determine what provokes a response.

[38] President, *National Cyber Strategy of the United States of America* (Washington, DC: Office of the President of the United States, September 20, 2018).

[39] Ibid.

Therefore, as in other domains, a critical first step to successfully employing cyber acts to communicate potential consequences is to establish a clear declaratory policy and communicate that policy to potential adversaries.

Signaling and Follow-Through

Once a clear declaratory policy has been established, a deterring state should be prepared to utilize the next steps in the communication process to ensure adversaries understand its system of rules, commitment, and credibility and better calculate the potential costs. These next steps are the use of signaling and follow-through.

Unfortunately, in the cyber domain, the use of signaling and follow-through is nascent. For example, neither the United States nor any other nation has ever publically acknowledged employing a cyber operation, much less used a cyber operation for pure signaling reasons. However, deterring states have used signaling and follow-through mechanisms throughout history in other domains. These can be used to form a baseline of what is required for an effective signal and follow-through.

Based on a study of successful signaling and follow-through actions, there are five essential characteristics:

1. Deterring State Self-Identification

Any effective signal and follow-through must communicate the deterring state's identity. Identification is important in order for the adversary to link the action to the declaratory policy and to confirm the intended or actual enforcement of the system of rules, the commitment to enforcement, and the credibility of future threats. If a challenger does not know who conducted the signal or response, they are less likely to consider these actions in future decisions regarding that state, losing the desired effects of the operation.

In the cyber domain, the difficulty of attribution (the ability to identify the actor) is a recurring issue. Some states tend to capitalize on this technical challenge when engaging in covert operations. As a result, states who are the victim of cyber acts may be unwilling to respond (in any domain) out of the fear of inaccurate attribution. Thus, an argument could be made that signaling could undermine this tactical advantage.

Importantly, this article does not advocate for the complete elimination of covert cyber operations. Rather, covert cyber operations could still be utilized, when appropriate; similarly to how states continue to employ both covert and overt air, land, or sea operations. There is no doubt that these covert operations can have a deterrent effect. However, with signaling and follow-through actions, it is important to identify the actor because the purpose of the signal or response is to communicate a message. That message is lost if the deterring state is not clearly identified.

2. Clear Message

Any signal or follow-through should communicate the commitment and credibility in clear terms. In other words, the message must indicate that the deterring state is committed and their threat is credible; there is rarely a benefit to ambiguity in this regard. Additionally, the message should be closely linked to the system of rules/declaratory policy.

Ideally, a signal would communicate a message along these lines: "You appear to be preparing to do [x]. According to our declaratory policy, we will respond to your action by doing [y]. We have the capability and commitment to respond in this manner. This action is to confirm our intent to follow-through on this declaratory policy." Similarly, a follow-through action should communicate a message along these lines: "You have done [x]. According to our declaratory policy, we informed you that we would response to your action by doing [y]. We have conducted this action in accordance with our declaratory policy."

3. Capability Demonstration

Communication via signaling and follow-through requires that the deterring state adequately demonstrate the capability to conduct the actions specified in their declaratory policy. If the deterring state cannot demonstrate their capacity to impose the threatened costs, it is unlikely to factor into an adversary's decision calculus. If, for example, the Chinese ASAT missile test was not successful, a space faring nation that was contemplating a challenge would not give any weight to the threatened costs. Similarly, in the cyber domain, if a threatened action is not demonstrated as being technically feasible, it will have little effect on an adversary's calculus.

4. Tailoring to the Target

A signal or response must be carefully tailored to the adversary, focusing on how the capability is likely to impact their cost determination. In other words, the message must "speak the language" of the adversary and concentrate on those costs that will persuade the adversary. For example, if the challenger lacks any functioning satellite, it is doubtful that China's recent ASAT missile test would alter their decision calculus. Similarly, if a state lacks a dependency on cyber capabilities, employing adverse cyber acts would prove fruitless.

This can be the most complicated of the requirements because knowing what the adversary values is not always obvious. Nuclear deterrence was simpler because total destruction is a universally feared cost. However, determining what North Korea's leader, Kim Jong-un, values is exponentially harder, and threatening total destruction tends to lose its effectiveness without any follow-through. Nevertheless, it is the job of the deterring state to identify what the adversary values and then tailor a signal or response to increase their anticipated costs.

5. Adversary Identification

While it is inherent in the previous characteristics, it is important to expressly state the significance of identifying the adversary in a signal or follow-through action. In other words, the deterring state should identify the target state. This characteristic has two parts. First, the deterring state should properly identify the target state before any signaling or follow-through action. This ensures the response is properly tailored, demonstrating the correct capability, and sending the correct message. In the event a deterring state misidentifies the adversary and then uses the above requirements to tailor a signal or response, this effort will have little effect on the actual challenger. In fact, it might even embolden an actor who believes they can operate without consequence.

Second, it must also identify the target within the signal or follow-through. This ensures the intended receiver knows they are the intended receiver. This particular aspect tends to be more important in the domains that lack clear borders (i.e., cyber). In a traditional domain, proximity to a state's border, territorial waters, or airspace was sufficient to identify them as the target state. However, in a borderless domain, a deterring state must be more overt, ensuring any errant recipients of the message are aware of its intended target.

Case Studies: Revisited

The deterrence examples provided in Part I illustrate how the five characteristics for communicating consequences determine successful signaling in other domains.

1. U.S. Deterrence of a Soviet Union Nuclear Strike

When the declaratory policy of "massive retaliation" alone did not appear to be deterring the Soviet Union, the United States demonstrated its credibility and commitment through signaling. In this instance, signaling was the development, testing, and deployment of nuclear weapons for the nuclear triad. As a prominent example, this analysis focuses on development and testing of nuclear weapons and delivery systems (Intercontinental Ballistic Missiles, or ICBMs).

Aside from the second characteristic (a clear message) which is discussed below, the testing of nuclear weapons and ICBMs met the requirements of a successful signal. First, during the height of the Cold War, there was no question regarding which country was developing nuclear weapons and ICBMs and then testing various prototypes. The tests were detectable around the world, and the United States did not hide these tests.

Second, each test served to demonstrate the U.S. capability to strike the Soviet Union. Third, the message was tailored to the Soviet Union. While nuclear deterrence did not require much, if any, tailoring, the United States did tailor their testing to the Soviet Union, the only other peer competitor in the development and deployment of nuclear weapons and ICBMs. Fourth, identifying the target of U.S. signaling was rather easy since there were few nuclear capable states and even fewer to deter. If there was any question, the development of ICBMs that possessed the range to reach the Soviet Union was fairly clear evidence that the Soviet Union was the primary target.

With regard to clarity of the message, the testing conducted by the United States was an attempt to clearly communicate U.S. commitment to developing, maintaining, and deploying functional nuclear weapons. Unfortunately, this message was open to misperception. Ideally, the United States should have declared: "The Soviet Union appears to be preparing to launch a nuclear strike. According to our declaratory policy, the United States will respond to any nuclear strike by engaging in a massive retaliatory strike, effectively destroying the full range of value targets in the Soviet Union. The United States has the capability and commitment to respond in this manner. This test of [a nuclear weapon or its delivery system] is to confirm U.S. intent to follow-through on this declaratory policy." However, this message was often lost, leaving many within the Soviet Union to believe that the United States was preparing to launch a first strike. This was a version of the "security dilemma," leading to multiple crises and near-breakdowns of deterrence throughout the Cold War.[40]

2. U.S. Deterrence of North Korea

After North Korea launched its twentieth ballistic missile in 2017 and tested what many believed to be a thermonuclear device, President Trump announced that he was stationing three carrier strike groups in the area of operations in close proximity to North Korea. Once there, the U.S. Navy conducted a joint exercise with participation from South Korean and Japanese warships. This was, in

[40] Robert Jervis, *Perception and Misperception in International Politics* (Princeton, N.J.: Princeton University Press, 1976). For examples, see Nate Jones, Ed., *The Soviet Side of the 1983 War Scare, Briefing Book #647*, National Security Archive, The George Washington University, https://nsarchive.gwu.edu/briefing-book/aa83/2018-11-05/soviet-side-1983-war-scare, accessed 5 November 2018; and also The John F. Kennedy Presidential Library and Museum, *Cuban Missile Crisis*, https://www.jfklibrary.org/learn/about-jfk/jfk-in-history/cuban-missile-crisis, accessed 8 November 2018.

no uncertain terms, a signal to North Korea that possessed each of the five characteristics.

First, the deterring state was identified. When the carrier strike groups arrived off the coast of North Korea, there was no confusion over whether they were assets of the United States. President Trump announced the stationing of the naval assets to the area, and each flew the U.S. flag. It should be noted that it is rare for the United States to announce the location of their carriers, so the publication served to remove any doubt that these assets belonged to the United States.[41]

Second, the message was clear; given the timing of President Trump's deployment of the naval assets, which occurred shortly after North Korea's twentieth test of a ballistic missile, the stationing of the carrier strike groups properly linked the actions of North Korea to the response action. It was then further linked to the U.S. declaratory policy on stopping nuclear proliferation. Third, the mere presence of the carrier strike groups in the vicinity demonstrated U.S. capability to be in Korean waters within a matter of days. Further, while inside the Seventh Fleet Area of Operations, the carrier strike groups conducted an exercise, demonstrating their ability to work together against a common target.

Fourth, the message was tailored to North Korea and Kim Jung-un, whose actions confirmed that he does not respond to a light touch and that he pays close attention to the movements of U.S. strategic assets near the Korean peninsula.[42] Finally, the United States properly identified North Korea as their target state. This was accomplished through statements by President Trump, the timing of the response action (shortly after the missile test), and the proximity of the naval assets to North Korea.

While the overall success of the U.S. deterrence strategy for North Korea is still being determined, this signaling example appears to have been a successful communication of U.S. intent, commitment, and credibility.

3. China's Deterrence of Space-Based Operations

China recently conducted another ASAT test of the DN-3 anti-satellite interceptor, which is capable of being launched from land, directly ascending, and striking a satellite orbiting Earth. As discussed in Part I, this action was not as effective as it could have been if it had accomplished the first step of communicating a deterrence strategy—communicating the declaratory policy. Consequently, adversaries were unable to determine the threshold for such a response action or to make sense of China's intent.

Despite this, there were some deterrence benefits of the test, and it did possess many of the requirements of an effective signal. First, due to the nature of the operation and the constant monitoring of space launches, it was obvious to determine the identity of the launching state. Second, this was, if nothing else, a capability demonstration—ensuring everyone capable of detecting the launch was aware of China's ability to strike space assets from a terrestrial launch. Third, it was tailored to, what we assume is, the target states—all space-faring nations. While most signals should consider engaging in a more tailored approach, in rare circumstances (for example, nuclear deterrence), no specific tailoring is needed if simply trying to communicate a capability.

[41] Ankit Panda, "What 3 U.S. Supercarriers in the Asia-Pacific Means for North Korea," *The Diplomat* (October 30, 2017).

[42] Ibid.

The two most glaring omissions from China's ASAT test were that the message was not clear and the target states were not identified. This is largely due to the disguising of the launch as a missile defense interceptor test. As a result, China's message was ambiguous, not tied to a declaratory policy, and lacking any indication of a system of rules. Coupled with the lack of a clear identification of the target states, an adversary is unlikely to know whether they were an intended recipient and what message to take from this action.

These omissions hinder the deterrent effect of China's ASAT test. As a result, there continues to be uncertainty regarding space assets and China's position.

4. U.S. Deterrence of China's Claim to the South China Sea

When the U.S.S. John S. McCain, a U.S. Navy destroyer, traveled close to Mischief Reef in the Spratly Islands, there was little doubt that this maneuver was meant to send a message regarding the U.S. position over the disputed area. In fact, this was the third FONOP mission during the Trump presidency, with the administration vowing to conduct more operations in the area.[43] This signaling measure met the requirements for an effective signal.

First, similarly to the carrier strike group stationed off the coast of North Korea, the identification of the U.S. destroyer was indicated by the flags flown aboard. In addition, when approached by the Chinese sea craft, the U.S.S. McCain identified itself, and China later declared the U.S. action as "provocative."[44]

Second, the message was clear, albeit not necessarily articulated in the manner proposed above. Instead of publicly voicing the purpose of the mission, the United States relied on a common practice associated with international waters and the law of the sea—freedom of navigation.[45] While uninformed observers might be confused by the action, the message was clear to a savvy international diplomat. Notably, the Chinese understood the message, later condemning the operation by stating that "the operation had violated international and Chinese law and seriously harmed Beijing's sovereignty and security."[46]

Third, the sending of the U.S.S. McCain, a destroyer, was a demonstration of the capability of the U.S. Navy. While it did not engage in a hostile act (according to U.S. policy), the ability to project power in the area was an indication of the ability to do so later. Fourth, this action was tailored to the Chinese and their claim over the South China Sea, specifically communicating the U.S. position on the nature of the area. Finally, given the proximity of the operation to both China and the disputed area, the target state was identified. The success of this signaling action can be seen by the Chinese response, which stated, "China is resolutely opposed to this kind of show of force . . . ."[47]

Cyber Consequences

The same requirements for an effective signal and follow-through action in other domains can be translated to the cyber domain. Therefore, any suggested cyber signaling or follow-through must meet each of the above characteristics for the best chance of being effective. Consequently, any proposed solution must (a) disclose the identity of the deterring state; (b) clearly communicate the message; (c) demonstrate the capabilities of the deterring state; (d) be

[43] Ibid.

[44] Idrees Ali, "U.S. destroyer challenges China's claims in South China Sea," *Reuters* (August 10, 2017).

[45] Ibid.

[46] Ibid.

[47] Ibid.

tailored to the target adversary; and (e) properly identify the adversary.

1. Proposed Solution: “Loud” Cyber Weapons

If the United States employed “loud” cyber weapons as signals and follow-through actions within the cyber domain, it would have a better chance of effectively communicating its system of rules, its commitment, and the credibility of its threats. As defined above, loud cyber weapons are cyber weapons that can be definitively traced to the actor; they do not disguise the source, the nature, or the effects. When employing loud cyber weapons, the actor does not obscure the operation or its source from being discovered by the victim and correctly attributed.

As proposed, the United States would employ loud cyber weapons consistent with their declaratory policy and in response to adverse actions—whether these actions were employed in the cyber domain or other domains. These would functionally serve as a cyber “show of force,” commonly practiced in other domains. When evaluated under the requirements outlined above, loud cyber weapons meet all the requirements of an effective signal and follow-through.

a. Self-Identification

By its nature, a loud cyber weapon identifies its origin and architect; it does not disguise these in an effort to achieve surprise. This provides the needed link between the act, the effects, and the deterring state. It informs the adversary about who carried out the act, confirms enforcement of the deterring state’s system of rules, and demonstrates the deterer’s commitment to enforcement and maintaining credibility of future threats. The result is that the challenger has no question about who coordinated the act and is able to determine the deterring state’s intent. With covert cyber weapons, an adversary may know of the effects of an act, but not know who was behind it. This undermines the effectiveness of signal and follow-through. Employing loud cyber weapons allows adversaries to better estimate the costs of any potential response from the deterring state. Consequently, future deterrence messages and threats will likely be taken more seriously and should increase the adversary’s anticipated costs.

b. Clear Message

Loud cyber weapons offer a unique advantage over covert cyber weapons and conventional weapons. With both covert cyber weapons and conventional weapons, the message can be lost if not properly executed or linked to the initial action and declaratory policy. Loud cyber weapons, on the other hand, can communicate the message more overtly, through incorporation into code. Since covert cyber operations attempt to disguise their identity, a deterring state is unwilling to put identifying information within the code; in fact, they often attempt to hide such indicators. Even if the deterring states does not wish to be so direct, it can fall back to employing cyber weapons in the same manner as conventional signaling and follow-through actions. This can be done by linking loud cyber operations through public statements or conducting the operation soon after the triggering event. In either case, the adversary is able to receive a clear message, which will be factored into their future decision calculus.

c. Capability Demonstration

This is perhaps the most beneficial aspect of loud cyber weapons. With the current covert nature of cyber weapons, many state and non-state actors suspect that the world powers, including the United States, have significant cyber capabilities. However, there is confusion over their actual capabilities because they are rarely publically acknowledged. As a result, an adversary is left to guess the potential costs that would be imposed by these deterring states. The only guidance they have in anticipating the costs are vague policies by the world powers. For example, one U.S. policy declares that it will respond "through its defense capabilities . . . at a time, in a manner, and in a place of our choosing . . . ."[48] This does little to communicate the anticipated costs to potential challengers.

Furthermore, many adversaries might not anticipate *any* cost imposition due to a lack of publicity of past efforts by these world powers to respond to cyber acts or signal their intent to do so. Much like an ASAT missile test that fails to launch successfully, a lack of known cyber responses does little to deter adversaries.

Loud cyber weapons offer a solution to this. By not disguising the effects, they broadcast the deterring state's capabilities to adversaries and beyond while demonstrating state commitment to enforcing rules and bolstering the credibility of threats. For example, many adversaries might actually be subject to a signal or follow-through response from the United States, but due to the covert nature of the operation, the effects (and therefore, the capabilities) are unknown to the target. More overt use of cyber weapons clears up any ambiguity surrounding cyber operations and fully informs adversaries of the deterring state's policy. Consequently, potential challengers are better equipped to calculate anticipated costs associated with an adverse action.

d. Tailoring to the Target

Like conventional tactics, loud cyber weapons offer the flexibility to be tailored to the specific target actor. Importantly, though, loud cyber weapons expand the spectrum of options available to deterring states when determining how to signal or follow-through, both within the cyber domain and outside of it. For instance, if the United States wanted to signal to North Korea that it would not tolerate their continued nuclear weapon development, they could employ options ranging from a traditional show of force (i.e., aircraft flying in close proximity, a carrier strike group being stationed in the area, or amassing troops in South Korea) or it could employ a loud cyber weapon. Thus, loud cyber weapons provide an expanded set of viable options to tailor the message to the target actor's specific interests. Accordingly, the deterring state is better equipped to tailor its cost impositions, and consequently, an adversary is better positioned to assess the range of likely costs the deterring state may impose.

e. Adversary Identification

As explained above, this requirement has two functions. First, proper identification helps the deterring state better tailor the signal or follow-through to the target state. Second, it helps identify the target state, which is particularly important when operating within a borderless domain.

Loud cyber weapons do not necessarily offer an advantage over conventional and covert cyber weapons in the first function of this requirement; it is equally important to properly identify the actor in all domains in order to properly tailor the signal or follow-through action. But, perhaps it is more important to correctly identify the target actor when employing loud cyber weapons. As compared to covert cyber weapons, loud cyber weapons will actually make matters worse in the event that a deterring state misidentifies the challenger. For example, if a covert cyber weapon were targeted at the wrong actor, the target might not even know

[48] DOD, Cyber Strategy, 11.

they were the victim of a deterrence response; the same is not true for loud cyber weapons. The issue does arise in other domains, albeit, with less difficulty of attributing responsibility to deterring states.

Much is made of the attribution problem for identifying adversaries in cyber operations. Fortunately, many of the world powers are getting better at attributing cyber actions. Instead, the more recent challenge is timely attribution, and this complicates, but does not foreclose, deterrence operations. After all, it is the deterring state's obligation to link the previous adverse act to its response, even if delayed.

Additionally, the second function is equally important. Because the cyber domain is borderless and nations are interconnected, there is always possible an errant spread of the cyber weapon (for example, a worm that propagates further than intended). So, it is important for loud cyber weapons to specifically name the target to avoid potential misperception and escalation. All things considered, as long as a state properly identifies the target actor, loud cyber weapons meet the requirements of an effective signal/response.

2. Challenges

While loud cyber weapons offer an effective method for signaling and follow-through actions, certain challenges exist in practically employing them.

First, the effectiveness of a deterrence strategy relies heavily on anticipated cost imposition; however, in the cyber domain, the costs are all relatively low compared to other domains. For example, in nuclear deterrence, the likely cost is a retaliatory strike that would most likely result in significant (if not, total) destruction. An adversary is less willing to provoke this result; there is a significantly narrow margin of error in nuclear deterrence. For the cyber domain, the most likely damage for a signal or follow-through action is relatively minor (perhaps a computer or network is temporarily inoperable or data is lost), and the cost is relatively small. A passionate adversary is unlikely to be deterred by such an insignificant consequence.

However, the key to employing loud cyber weapons (like deterrence in all domains) lies in the tailoring of the response to the target; after all, not all actors will be deterred by the same costs. For those actors who will not be deterred by cyber weapons (whether covert or overt), imposing such a cost would not be effective, and the deterring state should consider other signals or follow-through options (for example, a different domain).

Further along these lines, due to the likelihood of low cost imposition, many adversaries will be more willing to test the deterring state's resolve. This is in marked contrast to other domains. As discussed above, in nuclear deterrence, the margin of error is narrow, but in the cyber domain, drastic retaliation is unlikely, and may offer little added signaling value. Given a panoply of available cross-domain options, challengers may poke and prod the cyber deterring state in an effort to determine whether it is truly committed to its system of rules.

However, this only cements the importance of fully forming a deterrence strategy. A deterring state must contemplate various scenarios and tailored responses, even outside of cyber weapons and the cyber domain. This should be distilled in the nation's system of rules. Furthermore, low magnitude, cross-domain retaliation reinforces the need to tailor signals and follow-through actions to the effects which will most likely impact an actor's decision calculus.

Second, there are often questions regarding the legality of using cyber weapons, especially when there is a use of force implication. Due to the many questions on how international law applies to cyber operations (an area that is very unsettled at this point), this is a complex topic that should be more fully evaluated. In any case, it does not foreclose use of loud cyber weapons entirely. Instead, it is incumbent upon the deterring state to examine international law applicable to cyber operations and carefully craft a signal and follow-through action that does not run afoul of international law. With that said, the use of loud cyber weapons may actually help states provide more clarity to the international community on their position regarding the law governing cyber operations, which is currently being defined and refined by academics.[49]

Third, given the nature of cyber weapons (they suffer from being rendered obsolete over time and can rarely be used after an actor learns of their vulnerability), there is a significant chance that using loud cyber weapons could compromise a nation's cache of cyber weapons. Furthermore, considering the various disparate agencies within a government that operate in the cyber domain and the somewhat finite availability of cyber weapons, use of loud cyber weapons could cause internal conflicts and degrade some operations. Therefore, if loud cyber weapons are employed, a deterring state must carefully consider these practical complications.[50]

Fourth, use of loud cyber weapons may create problems of misperception and escalation. For misperception, the clarity of the state's message and, ironically, its capacity to authenticate against "false flag" operations will largely control the potential for misperception. Understandably, however, this is not fool-proof. Therefore, a deterring state must be prepared for potential misperception and accept an enhanced element of transparency for their loud cyber operations. For escalation, it is possible for cyber weapons to aggravate matters; two nations may go back-and-forth, increasing tensions rather than resolving them. This is an issue that is not unique to loud cyber weapons. Any signal or follow-through action can escalate matters. Therefore, it is up to the deterring state to consider this potential consequence and factor that into their decision.

CONCLUSION

A necessary component to any deterrence strategy is communication; it allows the adversary to better estimate costs, preparing the way for a more accurate decision calculus. Unfortunately, finding a cyber equivalent for deterrence communication has been somewhat illusory. Nevertheless, the key to communicating potential costs in the cyber domain is not groundbreaking; nations need only look to their traditional methods from other domains (i.e., signaling and follow-through). What is unique, on the other hand, is the suggested solution—loud cyber weapons. Upon closer examination of loud cyber weapons, there is support for their use in the characteristics of traditional signaling and response actions.

While this paper argues for use of loud cyber operations, there are many other concerns that must be addressed prior to their employment. For example, what actions would generate a response? What effects would be employed?

[49] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, UK: Cambridge University Press, 2017).

[50] For a potential solution, see Timothy M. Goines, "Overcoming the Cyber Weapons Paradox," *Strategic Studies Quarterly* Vol. 11, No. 4 (Winter 2017): 86-111.

How should a deterring state better incorporate loud cyber weapons into a unified deterrence posture? These concerns should be considered and discussed.

Regardless, the proposal here represents a viable solution to lack of communication within the cyber domain. In short, loud cyber weapons provide nations with a useful tool for deterrence in the cyber domain to effectively communicate potential costs of a challenger's action, thereby affecting the decision calculus of adversaries and increasing the likelihood of success.