DRAFT

Back to Reality: Cross domain deterrence and cyberspace

Author: Aaron F. Brantly

Abstract:

This paper examines cross domain deterrence strategies involving cyber incidents. By focusing on efforts to halt Russian and Chinese cyber operations against the United States this paper examines the importance of developing, maintaining and implementing (when necessary) cross domain deterrence strategies. This paper departs from more theoretic debates on the value and potential success, or lack thereof relating to cyber deterrence strategies and focuses on two cases in which cross domain retaliations were utilized to halt adversary behavior. From these two cases this paper posits a preliminary theory of cross domain deterrence applicable to cyber interactions between states and advances the debates in the field by shifting the center of gravity away from within domain responses to other mechanisms to deter adversary behavior.

Deterrence in cyberspace is a vexing problem plagued a range of challenges including attribution, proportionality and capability.[1] For the better part of the last two decades scholars and practitioners have sought out solutions to the cyber deterrence conundrum by leaning heavily on nuclear analogies or conventional International Relations or criminological paradigms.[2] Parallels to more conventional kinetic attacks are hampered for a variety of reasons, largest of which appears to be a lack of cognitive equivalence between kinetic and cyber means to achieve the same effect.[3] This lack of equivalence often constrains decision-making to within domain response options often predicated on deterrence strategies by denial or punishment within cyberspace. Rarely do cyber activities at the nation state level result cross-domain responses.

Tim Maurer lists the two cyber actors most threatening based on capabilities as Russia and China.[4] Both China and Russia have, over the last 20 years, engaged in substantial cyber operations against the United States in the form of attacks against critical infrastructure or sustained economic espionage. The United States has engaged in moderate efforts at deterring both actors external to cyberspace. These efforts have had markedly different effects on the types and continuance of cyber-attacks against the United States.

The data pool of cross-domain deterrence in response to cyber-attacks is limited within the public domain. The two most prominent cases to date are U.S. efforts to deter for-profit economic espionage by Chinese actors and efforts to deter Russian information operations and cyber intrusions into U.S. election processes and infrastructures. This chapter focuses on these two instances of cross-domain responses and assesses the strategic impact of these actions on the status quo of state to state interactions. This chapter argues that by signaling to an attacking nation a clear and credible cross-domain response the United States is able to alter the framing and lack of

[1] Brantly, Aaron F. 2018 "The Cyber Deterrence Problem." In The 10th International Conference on Cyber Conflict. Tallinn: NATO Cyber Defense Center of Excellence. 31–54.
[2] Mandel, Robert. 2017. *Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks*. Georgetown University Press; Nye, Joseph S, Jr. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41 (3); Glaser, Charles. 2011. "Deterrence of Cyber Attacks and U.S. National Security." GW-CSPRI-2011-5. Washington, DC: Cyber Security Policy and Research Institute.
[3] Farrell, Henry, and Charles L Glaser. 2017. "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine." *Journal of Cybersecurity* 6 (March): 46–11.
[4] Maurer, Tim. 2018. *Cyber Mercenaries: the State, Hackers, and Power*. Cambridge: Cambridge University Press.

cognitive equivalence of between kinetic and cyber-attacks while simultaneously managing potential escalatory concern. Cross-domain responses begin the process of establishing clear "red-lines" beyond which cross-domain escalation is likely and establishes norms for expected state responses to cyber-attacks.

This chapter proceeds by assessing the relevant literature on cross-domain deterrence within other domains of state interactions and the existing literature on cyber-cross-domain deterrence. Following the establishment of a framework for cross-domain deterrence two prominent case examples are examined in detail and the impact of cross-domain deterrence in each case is assessed. The chapter concludes by examining potential policy recommendations.

Crossing Domains to Deter Adversaries

Before parsing out cross-domain deterrence (CDD) it is helpful to provide the basic contours of deterrence theory within which the argument fits. Deterrence is the dissuasion of an adversary from engaging in a behavior or action directed against a target either proximate or non-proximate to a state's core interests.[5] Deterrence dissuading proximate actions or behaviors against a target is referred to as direct or central deterrence. By contrast, deterrence dissuading non-proximate actions or behaviors is referred to as extended deterrence.[6] Historically proximity in relation to deterrence has been defined geo-spatially and indicates that as the distance of an adversary's action or behavior against a target increases relative to the territorial boundaries of a state the perceived threat shifts from direct to indirect.[7]

Deterrence mechanisms can be broken down in a variety of different ways, three of which stand out in research on cyberspace. The first and most commonly analyzed form of deterrence is deterrence by threats of punishment.[8] Threats of punishment indicate that once an adversary

[5] Freedman, Lawrence. 2016. "General Deterrence and the Balance of Power." *Review of International Studies* 15 (2): 199–210; George, Alexander L, and Richard Smoke. 1989. "Deterrence and Foreign Policy." *World Politics* 41 (02); Nye. 2017. "Deterrence and Dissuasion in Cyberspace."
[6] Freedman, Lawrence. 2016. "General Deterrence and the Balance of Power." *Review of International Studies* 15 (2): 199–210.
[7] Wilner, Alex S. 2015. *Deterring Rational Fanatics*. Philadelphia: University of Pennsylvania Press.
[8] Wilner, Alex. 2013. "Fencing in Warfare: Threats, Punishment, and Intra-War Deterrence in Counterterrorism." *Security Studies* 22 (4): 740–72. doi:10.1080/09636412.2013.844524.

engages in an action or behavior it will suffer costs imposed by the deterring state. A second form of deterrence commonly analyzed in relation to cyberspace actions and behaviors is deterrence by denial.[9] Deterrence by denial creates conditions under which an actor is dissuaded by ex-ante costs associated with engaging in certain behaviors or actions. Joseph Nye further added to the debate on deterrence mechanisms by indicating that states could be entangled in such a manner so as to foster "self-deterrence". Deterrence by entanglement occurs when the deterrer and the attacker come to a consensus that the benefits sought by the attacker will result in self-imposed costs in excess of expected gains.

For the purpose of studying the impact of CDD on adversary behavior in cyberspace the analysis below is constrained to CDD mechanisms emphasizing deterrence by threats of punishment. While it is conceivable to extend CDD to denial and entanglement strategies that is beyond the scope of this chapter. Furthermore, deterrence by punishment offers a level of simplicity in an action-reaction pairing that simplifies analysis on a range of associated issues.

All forms of deterrence require clear signaling of both warnings and consequences.[10] The absence of clarity in warnings creates a situation in which adversaries are unable to identify redlines and will "probe" the resolve of the deterring state to determine where those red lines exist. Public or private declarations about what will or will not be tolerated and continuing to reinforce and convey the boundaries of acceptable behavior or actions informs the rational decision-making calculus of an adversary. Clearly signaling consequences increases the level of mutual information about costs and potential benefits between an attacker and deterrer. Clear signaling of costs further fills out the rational decision-making calculus of an adversary and establishes the foundation for deterrence by threats of punishment. Clarity requires specificity. Specificity is the identification of what and potentially why and how targets (or categories of targets) might be attacked by an adversary. Specificity of both targets and means that would result in the actuation of a punishment strategy provides information to adversaries about where red lines are and how they can be triggered. Furthermore, specificity also includes the identification of where, what, why and how costs will

[9] Brantly, Aaron F. 2018 "The Cyber Deterrence Problem." In The 10th International Conference on Cyber Conflict. Tallinn: NATO Cyber Defense Center of Excellence. 31–54.
[10] George, Alexander L, and Richard Smoke. 1974. *Deterrence in American Foreign Policy: Theory and Practice*. New York: Columbia University Press.

be imposed in response to clearly identified behaviors or actions undertaken by an attacker. Both clarity and specificity inform the decision-making calculus of adversaries and offer a potential avenue for mitigating escalatory actions when a punishment is being exacted in response to a violation.

Beyond clearly and specifically signaling both warnings and consequences, it is necessary for states to ensure these signals are credible.[11] As stated by Jon Lindsay and Erik Gartzke: "Deterrence is also an information problem as defenders seek to generate credible signals of resolve and intent for challengers".[12] Insufficient credibility weakens signals and creates information imbalances within a rational deterrence calculus. As will be discussed below credibility is a challenging problem for both conventional within domain deterrence in cyberspace and for CDD. Credibility is both offensive and defensive in nature. Simply possessing the power to punish does not indicate the ability to punish accurately. Responding to kinetic attacks requires radar, sonar, or other detection systems that can provide sufficient evidence to indicate the perpetrator of a given attack. Similarly, to respond to a cyber-attack also requires sufficient defensive capabilities to provide reasonable attribution within a timely manner.[13]

Often in discussions on deterrence emphasis is placed on the credible development of means of punishment. While in the kinetic realm, such means can be accomplished through the acquisition of missiles, planes, tanks or other kinetic devices, each of which clearly demonstrates an approximate level of response capability, similar demonstrations in cyberspace are far more difficult to achieve but are equally necessary. It is not credible to say that in response to a cyber-attack a state will threaten via cyberspace to attack a comparable (i.e. proportionate target). Such attacks take time and effort to establish and require sufficient intelligence preparation of the battlefield.[14] Whereas in the kinetic sense it is more reasonable to say, "if you bomb my power plant, I will bomb your power plant," in cyberspace saying, "if you hack my power plant, I will

[11] Mearsheimer, John J. 1990. *Conventional Deterrence*. Ithaca: Cornell Univ. Press
[12] Lindsay, Jon, and Erik Gartzke. 2017. "Cybersecurity and Cross-Domain Deterrence." In *US National Cybersecurity International Politics, Concepts and Organization*, edited by Damien Van Puyvelde and Aaron F Brantly, 12-27. Abingdon: Taylor and Francis.
[13] Rid, Thomas, and Ben Buchanan. 2015. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38 (1). Routledge: 4–37.
[14] Brantly, Aaron Franklin. 2016. *The Decision to Attack : Military and Intelligence Cyber Decision-Making*. Athens: University of Georgia Press.

hack yours," is not an equivalent statement. While in the first instance both might have the material resources to accomplish the task, in the second having the human and technical capital to accomplish task does not provide equivalent destructive capacity. Cyber weapons are transitory in nature and specific to targets.[15]

Finally, for deterrence to be effective states must either be rational or have a fundamental understanding of how to assess the cognitive deficiencies of their adversaries. Evidence over time indicates that states are generally rational actors both in cyberspace and in conventional kinetic war.[16] However, rationality is conditional and bounded. To further nuance the calculus of potential attackers concepts of cognitive bias can help further refine and generate effective deterrence strategies.[17] For simplicity this chapter makes basic assumptions about state actors as rational unitary actors.

Moving beyond the basic tenets of deterrence by punishment to a more inclusive concept, CDD, does not severely stress its functionality. First, deterrence theory rarely if ever says anything about how threats of punishment should be composed. Historical examples of deterrence from Athens and Sparta[18], to Rome and Persia[19], to more modern conflicts including Syria[20] have provided ample examples of CDD in practice. Attacks in one domain are almost always matched with attacks in another domain or in such a way that affords the deterrer the least costly means to impose proportionate costs on an attacker or violator of the established status quo within a deterrence framework. The most common concern associated with deterrence is not that an adversary receives the same punishment in return for the costs that it caused to the state it attacked. Rather, the

[15] Smeets, Max. 2018. "A Matter of Time: on the Transitory Nature of Cyberweapons." *Journal of Strategic Studies* 41 (1). Routledge: 6–32.
[16] Bueno de Mesquita, Bruce. 1983. *The War Trap*. New Haven: Yale University Press; Fearon, J D. 1995. "Rationalist Explanations for War." *International Organization* 49 (3): 379–414; Brantly, Aaron Franklin. 2016. *The Decision to Attack : Military and Intelligence Cyber Decision-Making*. Athens: University of Georgia Press.
[17] Berejikian, Jeffrey D. 2002. "A Cognitive Theory of Deterrence." *Journal of Peace Research* 39 (2): 165–83.
[18] Thucydides, R W Livingstone, and Richard Crawley. 1943. *The History of the Peloponnesian War*. New York: H. Milford, Oxford University Press.
[19] Bullough, Vern L. 1963. "The Roman Empire vs. Persia, 363-502: a Study of Successful Deterrence." 7 (1): 55–68.
[20] Schmitt, Michael N, and Christopher M Ford. 2017. "Assessing U.S. Justifications for Using Force in Response to Syria's Chemical Attacks: an International Law Perspective." *Journal of National Security Law & Policy* 9: 283–303.

objective is to meet out a proportionate response to the costs incurred.[21] The concept known as *jus ad bellum* constrains states and attempts to limit punishments and reprisals to violations of international law. Too often in discussions of deterrence scholars and practitioners artificially constrain punishment strategies to equivalencies rather than proportionalities. This equivalency fallacy is due largely to the study of nuclear deterrence.

Nuclear deterrence is unique in the field of deterrence studies. It is unique for a variety of reasons. First, nuclear weapons are the ultimate weapon a state can possess it terms of shear destructive force and likely also in long term effects after use. Second, only a select few nations, eight as of this writing, possess nuclear weapons. Third, nuclear weapons have a taboo about their use that constrains their use in most cases only to those instances in which a state is itself the victim of a nuclear attack.[22] These attributes make the use of nuclear weapons as a punishment mechanism for nearly anything other than a nuclear attack disproportionate and make nuclear weapons the only viably proportionate response to a nuclear attack. Deterrence theorists such as Bernard Brodie, Arnold Wolfers, Percy Corbett, William Fox and Frederick Dunn[23], Thomas Schelling[24], Lawrence Freedman[25] and numerous others have all examined the conundrums associated with deterrence involving nuclear weapons. These and a variety of other factors combine to make nuclear deterrence qualitatively different from every other weapon system developed to date, including cyber capabilities.

Jeffery Knopf notes four distinct waves of deterrence theorizing within which analysis of cyberdeterrence falls within the fourth wave.[26] Knopf writes: "The most noteworthy new development in this literature is a trend toward no longer viewing deterrence in terms of nuclear

[21] Schmitt, Michael N, Liis Vihul, and NATO Cooperative Cyber Defence Centre of Excellence. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge; New York: Cambridge University Press.
[22] Nina Tannenwald. 1999. "The Nuclear Taboo: the United States and the Normative Basis of Nuclear Non-Use." *International Organization* 53 (3): 433–68.
[23] Dunn, Frederick Sherwood, and Bernard Brodie. 1964. *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt.
[24] Schelling, Thomas C, Harvard University., Center for International Affairs. 1966. *Arms and Influence*. New Haven: Yale University Press.
[25] Freedman, Lawrence. 1989. "General Deterrence and the Balance of Power." *Review of International Studies* 15 (2): 199–210.
[26] Knopf, Jeffrey W. 2010. "The Fourth Wave in Deterrence Research." *Contemporary Security Policy* 31 (1): 1–33.

or even conventional military means".[27] Knopf's concept of a fourth wave of deterrence builds on previous arguments by Jervis who highlighted the first three waves which sought to develop theories on conventional and nuclear deterrence and included concepts of shear destructive force (First Wave), game theoretic modeling (Second Wave), and cognitive or psychological concepts (Third Wave).[28]

Although Knopf writes of a fourth wave, deterrence theories applied to cyberspace are not a new field of study. Within military journals deterrence in cyberspace as a concept has been examined off and on for the better part of 20 years. The general consensus among scholars is that deterrence in cyberspace is plagued by a number of issues.[29] There are at least three core challenges associated with cyber deterrence. First, victims of cyber-attacks are often unaware that an attack has occurred. The average discovery time for victims of data breaches in 2017 was 191 days.[30] Distinguishing between random or expected malfunctions in networks and systems and deliberately induced malfunctions is difficult and requires substantial resources, both human and financial. Moreover, after initial detection - data breaches in 2017 averaged 66 days between identification and containment.[31]

Second, beyond identification and containment of a cyber-attack, attribution to a specific actor is often imprecise or dependent on either substantial forensic analysis and/or contextual geo-political factors that provide reasonable attribution to a given actor. Often, as in the case of Russian hacks of the Democratic National Committee (DNC) in 2015-2016 actor techniques, tactics and procedures provide both the forensic and geo-political context necessary for reasonable attribution. Thomas Rid and Ben Buchanan note that "attribution unwinds incrementally".[32] Jon Lindsay in writing on the challenge of attribution states: "attribution requires great technical expertise and

[27] Ibid.
[28] Jervis, Robert. 1979. "Review: Deterrence Theory Revisited." *World Politics* 31 (2): 289–324.
[29] Goodman, Will. 2010. "Cyber Deterrence: Tougher in Theory Than in Practice?." *Review of International Studies* 4 (3): 102–35; Valeriano, Brandon, and Ryan C Maness. 2015. *Cyber War Versus Cyber Realities : Cyber Conflict in the International System*. New York: Oxford University Press.
[30] 2017. "2017 Cost of Data Breach Study." Ponemon Institute.
[31] Ibid.
[32] Rid, Thomas, and Ben Buchanan. 2015. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38 (1-2). Routledge: 4–37. doi:10.1080/01402390.2014.977382.

analytical skill, and organizational coordination…"[33] Lindsay further rightly identifies that despite the attribution problem being really hard to solve - it is most difficult in less vital instances of attack than it is in comparably important instances in which the amount of available information from both forensic and non-forensic (geo-political) means increases. Martin Libicki goes on to note in the context of a credible deterrence attribution is important.[34] The absence of accurate and reasonably substantiated attribution can lead to unnecessary escalation and retaliation against a third-party actor who did not perpetrate a cyber-attack. A response predicated on faulty attribution or based on attribution with insufficient evidence would constitute a new wrongful cyber act and consequently be in violation of international law.[35]

Third, the calibration of a proportionate response to a cyber-attack is confounded by several factors including, temporal constraints, cognitive perceptions of proportionality, and technical capacity to respond in kind. As identified above, the time to recognition that an attack is underway or has taken place is almost 200 days. Moreover, the time to contain such an attack is 60 days. Such an action-reaction delay in deterrence by punishment weakens the credibility associated with threats of punishment. If a state waits 6 months to respond to a conventional kinetic attack much less a nuclear attack credibility of punishment would be almost entirely lost. Even following 9/11 it only took the United States a few weeks to have the first CIA and special forces on the ground engaging in retaliatory actions against the Taliban and Al'Qaeda. Time is a critical component of deterrence at any level from punishing a criminal within a "statute of limitations" to punishing states to violate a red line. Calibrating the timing of the attack and the subsequent reception of that attack by an adversary so that they know they are being punished in a timely fashion in cyberspace alone is difficult. If a retaliation through cyberspace occurs but the state being punished doesn't recognize it has been attacked for more than 200 days, it is uncertain whether the punishment is in response to a violation of a stated red line or if it is itself a new attack. Calibrating a response within a timely manner is critical to the establishment of credible deterrence.

[33] Lindsay, Jon R. 2015. "Tipping the Scales: the Attribution Problem and the Feasibility of Deterrence Against Cyberattack." *Journal of Cybersecurity*, 1(1)
[34] Libicki, Martin C. 2016. *Cyberspace in Peace and War.* Annapolis: Naval Institute Press.
[35] Schmitt, Michael N, Liis Vihul, and NATO Cooperative Cyber Defence Centre of Excellence. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge; New York: Cambridge University Press.

Beyond the calibration of the timing of a punishment is the proportionality of a punishment such that it fits within the law of armed conflict and minimizes the likelihood of escalation. Stephen Lukasik writes "while response to a cyber attack does not need to be a cyber counter-attack, international principles of armed conflict speak to proportionality of response and escalation control favors responding in kind."[36] Attacks that occur in the kinetic physical world are perceived fundamentally differently than those experienced in and through cyberspace. No one makes the perception argument more clearly than Thomas Rid, who through a Clausewitzian interpretation, finds that most cyber-attacks lack the attribute of violence that correlates with acts of war.[37] Because of the "perception problem" states that cross domains to retaliate are likely to be perceived as escalating.

Although both timing and perceptions both constrain proportional responses, likely nothing more effectively constrains, deterrence by punishment in cyberspace than readily available technical capacity to engage in a proportional response. The development timeline for cyber capabilities available and applicable for achieving proportional effects against an adversary for the purpose of punishment requires substantial planning and foresight. Rebecca Slayton notes in her analysis of the development of the Stuxnet worm a lengthy timeline requiring the technical skills of programmers, nuclear engineers, security and intelligence professionals.[38] The development of code capable of punishing an adversary does not occur overnight. Even if the appropriate skillsets are brought together to create a capability able to punish an adversary in response for a cyber-attack, such a capability must still be delivered to an appropriate target within a timely manner. And as noted by Max Smeets, the shelf-life of cyber capabilities is limited.[39] The same challenges are not present in kinetic forms of punishment because as noted in a speech by Stanley Baldwin before Parliament in 1932, "the bomber will always get through." Despite being hyperbolic, the reality remains that kinetic weapons are comparatively easy to leverage for punishment because they are readily available and difficult to defend against in most instances.

---

[36] Lukasik, Stephen J. 2015. "A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains". In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington D.C.: National Academies Press.

[37] Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (November): 37–41.

[38] Slayton, Rebecca. 2017. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41 (3).

[39] Smeets, Max. 2018. "A Matter of Time: on the Transitory Nature of Cyberweapons." *Journal of Strategic Studies* 41 (1-2). Routledge: 6–32.

These core within domain response challenges elevate the applicability of CDD as a means of punishment. Despite a perception that CDD from cyber to conventional attacks is inherently escalatory, this need not be the reality in cyberspace and it is not the reality in conventional deterrence. In nearly every case in which the United States has engaged in deterrence it has leveraged all or many of the tools of state at its disposal. In response to the positioning of Nuclear missiles on Cuba, the United States engaged in a quarantine (blockade) of the island. In Iraq in 1991 the United States used combined land, air, and naval forces to expel Iraqi forces from Kuwait. In response to consistent provocations including the development of nuclear weapons by the Democratic People's Republic of Korea (DPRK) the United States employed diplomatic and economic sanctions to impose costs. Even in instances of espionage, the United States has played its hand strategically. For instance, when 10 Russian spies were discovered in the United States they were traded for four former US spies. While not deterrence per say, the incident shows that the capture and threat of punishment can be turned to a strategic or tactical advantage.

The United States is not alone in its use of cross-domain strategies. In response to amphibious landings by Argentine during the Falklands war, the United Kingdom utilized, land, sea, and air power to expel the Argentine forces and restore British rule. In each of these cases the act of punishment while proportionate to the violation did not lead to extended wars with the parties involved and at times led to a resolution within a short timeframe. Not all instances of cross-domain retaliation result in a limited escalation as evidenced by U.S. involvement in Vietnam, but there are ample cases where the limited use of a proportionate cross domain response resulted in an intended effect of altering the behavior of an adversary through the imposition of costs.

Despite the ability of proportionate cross domain retaliation to impose costs in many instances, George and Smoke note three main typologies that result in deterrence failure.[40] First, the absence of credible deterrent threat. In situations where an insufficient deterrence threat is present the attacking party will suffer no consequences and therefore will rationally conclude it will benefit

[40] George, Alexander L, and Richard Smoke. 1974. *Deterrence in American Foreign Policy: Theory and Practice*. New York: Columbia University Press; Achen, Christopher H, and Duncan Snidal. 1989. "Rational Deterrence Theory and Comparative Case Studies." *World Politics* 41 (02): 143–69.

from engaging in a violation. Second, deterrence fails when a violation fails to exceed a threshold warranting the actuation of a deterrent threat. The cost of actuating a threat is either too costly for the deterrer relative to the violation or unable to be proportionate to the violation. Third a violation by an attacker is unconventional or highly asymmetric in a manner that is not easily countered with tools of deterrence.

Although cross-domain deterrence is central to U.S. Strategy in a multitude of instances, cross-domain cyber deterrence, while a stated policy, is rarely practiced. The U.S. Department of Defense Cyber Strategy declares:

The United States has been clear that it will respond to a cyberattack on U.S. interests through its defense capabilities. The United States has articulated this declaratory policy in the 2011 United States International Strategy for Cyberspace, in the Department of Defense Cyberspace Policy Report to Congress of 2011, and through public statements by the President and the Secretary of Defense. The United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law.[41]

This declaratory policy has been reiterated by both President Obama and several Secretaries of Defense. Yet the despite rhetorical consistency its implementation record across all cases is lacking in relation to conventional deterrence cases. Before privileging the notion of unwanted escalation it is first necessary to address what George and Smoke identify as the second cause of deterrence failure.

George and Smoke identify that a relative weakness of a challenge by an attacker is insufficient to warrant a deterrent response deterrence will fail. This failure creates what Achen and Snidal identify as a learning mechanism that informs an adversary as to the capabilities and intentions of its target.[42] In cyberspace the overwhelming majority of attacks fail to rise to a level of significance to warrant an attack. An analysis of significant cyber incidents from 1986 to 2012

[41] 2015. *The DoD Cyber Strategy*. Washington, D.C: Department of Defense.
[42] Achen, Christopher H, and Duncan Snidal. 1989. "Rational Deterrence Theory and Comparative Case Studies." *World Politics* 41 (02): 143–69.

reveals that while many cyber-attacks are painful in terms of lost intelligence, temporary losses in the availability of systems and the moderate degradation of command and control, few if any attacks have been substantial enough to warrant retaliation. The attacks that were substantial enough to warrant retaliation were targeted against states that possessed insufficient capacity to do so.[43] Three attacks stand out. First, the non-state cyber-attacks against the Republic of Georgia prior to and during armed hostilities with the Russian Federation in 2008.[44] Second, the Stuxnet attack, likely initiated by the United States and Israel against Iran's nuclear facilities at Natanz.[45] And third, the two black energy attacks carried out by the Russian Federation against the Ukrainian electric infrastructures in both the Western and central portions of the country.[46] In all three cases the victims of the attacks had insufficient capabilities to respond to cyber-attacks against the aggressor nation(s) or their proxies. In two of the three cases of substantial cyber-attacks the victims still possess insufficient conventional or cyber capacity to respond. Iran by contrast has spent substantial resources developing a moderate capability to respond and has demonstrated its increasing ability to respond in cyberspace with attacks against a variety of private sector entities including the Sands Casino in Las Vegas, a small spillway dam in New York, and Saudi Aramco.[47] Despite developing capabilities to respond, in each case the level of attacks subsequently perpetrated by Iran failed to rise to a level necessary to trigger a proportional counter response by the United States or other affected parties.

Most cyber-attacks exist below the threshold necessary to trigger punishment.[48] The effect is that although no single attack is able to induce sufficient pain necessary to trigger retaliation, attacks by a single actor cumulatively constitute a campaign that should or rather - could warrant a retaliatory response. Uri Tor notes that the manner in which many countries, the U.S. included

[43] Healey, Jason. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. New York: Cyber Conflict Studies Association.
[44] Beehner, Lionel, Liam Collins, Steve Ferenzi, Robert Person, and Aaron Brantly. 2018. "Analyzing the Russian Way of War." West Point: Modern War Institute.
[45] Zetter, Kim. 2014. "Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon." Crown Publishers.
[46] Dragos, Inc. 2017. "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations," June, 1–35.
[47] Kagan, Frederick W, and Tommy Stiansen. 2015. "The Growing Cyberthreat From Iran." Washington, D.C: CriticalThreats.org and Norse; Bronk, Christopher, and Eneken Tikk-Ringas. 2013. "The Cyber Attack on Saudi Aramco." *Survival* 55 (2): 81–96.
[48] Jasper, Scott. 2017. *Strategic Cyber Deterrence the Active Cyber Defense Option*. Lanham: Rowman & Littlefield.

understand and interpret deterrence is as an absolute.[49] For attacks to trigger retaliation under a premise of absolute deterrence they must necessarily exceed a threshold above which counter actions by the attacked party are justified. As is noted both in through historical case analysis and empirical analysis by Brandon Valeriano and Ryan Maness such a threshold is not common.[50]

By contrast Tor identifies Israeli deterrence behaviors as restrictive. Tor writes of the Israel experience: "in this deterrence paradigm, the use of force is not the harbinger of collapse in the deterrence regime, but rather an inherent part of maintaining the effectiveness of deterrence posture".[51] Tor identifies restrictive deterrence by summing the concept up as cumulative deterrence. The simultaneous use of macrolevel superiority and consistent and repeated responses to microlevel threats and aggressions.[52] This concept of cumulative deterrence is in line with Robert Mandel identifies as broad inclusive deterrence defined as the use of a "fluid, integrated mix of strategies that are far more multipronged than those in classic deterrence…" {Mandel:2017vg}. And is encompassing of non-exclusive options embedded within US doctrine that span diplomatic, legal, economic and military dimensions.[53]

U.S. deterrence in cyberspace has been hamstrung by an over-reliance on models of absolute deterrence designed to prevent strategic loss within a nuclear context. Although the policy and strategic documents have stated deterrence can and should be multi-domain, the reality has been that cyber-attacks have tended to be viewed as discrete incidents insufficient to trigger retaliation. The overarching policy for the use of offensive cyber in the United States, PPD-20, a classified Presidential Policy Directive required, until August 2018[54], any and all responses to cyber-attacks to receive Presidential approval. The constraints imposed on strategic deterrence by PPD-20

[49] Tor, Uri. 2015. "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence." *Journal of Strategic Studies*, December, 1–26. doi:10.1080/01402390.2015.1115975.
[50] Healey, Jason. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. New York: Cyber Conflict Studies Association; Valeriano, Brandon, and Ryan C Maness. 2015. *Cyber War Versus Cyber Realities : Cyber Conflict in the International System*. New York: Oxford University Press.
[51] Tor. 2015. "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence."
[52] Ibid.
[53] Jasper, Scott. 2017. *Strategic Cyber Deterrence the Active Cyber Defense Option*. Lanham: Rowman & Littlefield.
[54] Reports indicate that PPD-20 is being revised by the Trump administration to provide more decentralized administration of response to cyber-attacks as of Mid-August 2018.

superseded many of the stated policy objectives from the 2015 DoD Cyber Strategy and President Obama's 2011 International Strategy for Cyberspace.

CDD can be used to respond to threats and acts in a manner that moves deterrence away from absolutism to a restrictive strategy capable of responding to cumulative attacks in which retaliatory acts address individual violations do 191t exceed a retaliatory threshold. As noted by Gartzke and Lindsay, "deterrence is no longer a game of chicken with the survival of civilization in the balance, if it ever was, but rather an ongoing tapestry of moves and countermoves at different timescales and levels of analysis".[55] The challenge to date is not that CDD is not applicable to deterrence in cyberspace, but that the view of cyber-attacks to date as discrete rather than cumulative constrains retaliation.

If policies align and foster the cumulative view of cyber-attacks as warranting responses within a restrictive pattern similar to that argued for by Tor, then CDD fits nicely within a broader tapestry of moves and countermoves available to states. It appears that in the cases of sustained economic espionage by China and information and cyber assaults on U.S. Political, informational and election infrastructures by Russia that policies are, in some instances, aligning behind a cumulative interpretation of attacks constituting a singular effect able to be elevated to a level warranting a response. The appropriate use of CDD offers solutions to several challenges identified above that constrain retaliation within cyberspace. First, CDD can mitigate temporal problems associated with the development or utilization of cyber capabilities, and it further maintains existent capabilities for later use if necessary. Second, CDD provides a range of targets and options not available within cyberspace that provide specific, clear signals to attackers. A CDD response is less likely to be missed or misinterpreted by an adversary. Third, while initial attempts at CDD may fail to achieve proportionality their overtness in both signaling and effects can be additive, meaning that it is reasonable to start out with limited retaliatory activities and to increase the scale and proportion of retaliation to generate a signal sufficient to dissuade and adversary. Fourth, CDD strategies break the cognitive equivalence gap and demonstrate tangible effects for perceived

[55] Lindsay, Jon, and Erik Gartzke. 2017. "Cybersecurity and Cross-Domain Deterrence." In *US National Cybersecurity International Politics, Concepts and Organization*, edited by Damien Van Puyvelde and Aaron F Brantly, 1–17. Abingdon: Taylor and Francis.

violations. Combined, CDD offers a readily understood strategy already being utilized nearly all other instances of deterrence by punishment below the nuclear threshold.

CDD Efforts Against China and Their Effects

Chinese information warfare strategy can date its modern roots to the 1998 publication of *Unrestricted Warfare* by Colonels Liang Qiao and Wang Xiangsui.[56] In their book the authors emphasize the dependence of the United State military on ICT related technologies as a major vulnerability. This major vulnerability in their assessment provided the PLA with a strategic opportunity and an asymmetric advantage. The identification of strategic and tactical weakness in the United States by the PLA slightly predated a broader shift within the Chinese policy and thought on information warfare.

Beginning in 2000 Jiang Zemin, the former General Secretary of the Communist Party established in three speeches the trajectory of China's information society.[57] The speeches addressed towards the National People's Congress, the Chinese People's Political Consultative Conference (CPCC) and the Central Military Commission (CMC) established the necessity of developing a robust information society. The development of a national information plan in in 2006 outlined in broad strokes the priorities to be undertaken by China over a 14-year period. This plan and subsequent policy documents and plans establish a China seeking to not merely evolve in the Information Sphere that is cyberspace, but to mold it both domestically for its national interests as well as Internationally in governance. The identification of information technology as critical to national development coincided and paralleled developments in China's economic policies, most notably its notion of a "Peaceful Rise".[58] Although China's ambition was a "Peaceful Rise" its timing indicated that such a rise would be rapid and disruptive. At the beginning of its informatization China lacked the human capital necessary to achieve its aspirations and therefore began a crash

[56] Inkster, Nigel. 2016. *China's Cyber Power*. Abingdon: Routledge.
[57] Austin, Greg. 2014. *Cyber Policy in China*. New York: Polity Press.
[58] Inkster, Nigel. 2015. "The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R Lindsay, Tai Ming Cheung, and Derek S Reveron. Oxford: Oxford University Press.

series of national plans for educational reform and development emphasizing national STEM rejuvenation.[59]

Concurrent to national educational reforms the CMC considered its existent information warfare capacity weak at best. In contrast to U.S. efforts to utilize cyberspace to enable warfare in other domains, China established a priority of defending and exercising sovereignty over its information.[60] Initial indicators of what the Chinese efforts in cyberspace would become began in earnest in 2003 with what was named in the United States "Operation Titan Rain".[61] Titan Rain was the first major advanced persistent threat (APT) attributed to China.[62] Titan rain targeted DoD military research laboratories including the Defense Information Systems Agency (DISA), the National Aeronautics and Space Administration NASA, and others.[63] Despite being one of the largest breaches of US information infrastructures to date, the Titan Rain operations did not constitute a in and of themselves an attack, but rather an evolving pattern of intelligence collection for state gain that would increase substantially in the coming years.

The number, diversity and volume of attacks from 2003 through 2013 increased substantially. Targets expanded beyond purely intelligence related collection and included the Congressional office of US Representative Frank Wolf in 2006, US NGOs, the Dali Lama and various firms in sustained and coordinated operation identified by the Citizen Lab called Ghost Net[64], breaches of major defense industrial base firms, Google and other tech firms operating in China (Operation Aurora), collections against the IMF and NGOs (Byzantine Haydes), energy firms (Night Dragon) and dozens of others.[65] The robust and diverse nature of Chinese cyber espionage campaigns waged against actors spanning governments, NGOs, public and private sector resulted in what many scholars and practitioners argue constituted one of the largest transfers of wealth in human

[59] Austin. 2014. *Cyber Policy in China*.
[60] Ibid.
[61] Hagestad, William T. 2012. *21st Century Chinese Cyberwarfare*. Cambridgeshire: IT Governance Pub.
[62] Thornburgh, Nathan. 2005. "Inside the Chinese Hack Attack." *Time*, August 25.
[63] Thornburgh, Nathan. 2005. "The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them)." *Time*, September 5.
[64] 2009. "Tracking GhostNet: Investigating a Cyber Espionage Network," The SecDev Group and The Munk Centre for International Studies. March, 29. 1–53.
[65] Lindsay, Jon R, and Tai Ming Cheung. 2015. "From Exploitation to Innovation: Acquisition, Absorption, and Application." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R Lindsay, Tai Ming Cheung, and Derek S Reveron. Oxford: Oxford University Press.

history.[66] Yet each act of espionage, each target, viewed in isolation did not constitute a violation of international law sufficient to equate to either the use of force or an armed attack against the United States. The cumulative result was a loss of intellectual property, strategic and tactical advantage that would be unachievable even during major hostilities. The responses to the repeated breaches were to investigate, name and shame and attempt to further secure systems in anticipation of continued or new breaches.

Major efforts to counter Chinese intrusions into US national security, defense industrial base, public and private organizations came to a head in 2013 when the cybersecurity firm Mandiant (now FireEye) released a comprehensive report detailing the activities of what it referred to as Advanced Persistent Threat 1 (APT 1).[67] The APT 1 report identified the operations of PLA unit 61398, an advanced cyber espionage unit within the PLA. The report went on to detail the command and control structure, the organizational planning, targeting and attack lifecycles of its various exploits. In May 2013 the Department of Defense released a report identifying and outlining Chinese threats to the United States Department of Defense in and through Cyberspace {Anonymous:2013wy}. In May 2014 the Department of Justice (DoJ) presented evidence before Grand Jury which decided to indict five PLA hackers from unit 61398 on 31 different counts.[68] In August 2014 the DoJ indicts a Chinese businessman Su Bin for his role in stealing proprietary technology related to the C-17, F-22 and F-35 aircraft and transferring that information to China.[69] On April 1 2015 President Barack Obama issued executive order 13694 entitled: "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities". The order directly targets cyberespionage threats and emphasizes clear ramifications for individuals or sponsoring entities involved in the perpetration of cyber espionage or attacks. On August 30th, in advance of a planned summit between Chinese Premier Xi Jinping and President Obama, numerous sources, including Ellen Nakashima of the Washington Post report "The Obama administration is developing a package of unprecedented economic sanctions against Chinese

[66] Rogin, Josh. 2012. "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History'." *Foreign Policy*. July 9. https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.
[67] 2013. "APT1 Exposing One of China's Cyber Espionage Units." Mandiant Threat Intelligence Center.
[68] 2015. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," July. U.S. Department of Justice.
[69] 2016. "Chinese National Pleads Guilty to Conspiring to Hack Into U.S. Defense Contractors' Systems to Steal Sensitive Military Information." *U.S. Department of Justice*.

companies and individuals who have benefited from their government's cybertheft of valuable U.S. trade secrets".[70] In response to reports of purported sanctions China sent an advance delegation to seek out and negotiate with US officials to prevent the implementation of sanctions.[71] One week prior to the Xi – Obama summit president Obama was quoted as saying: "We are preparing a number of measures that will indicate to the Chinese that this is not just a matter of us being mildly upset, but is something that will put significant strains on the bilateral relationship if not resolved".[72] The resultant summit statement made clear that the signaling conducted by the Unite States in the two years leading up to Obama and Xi sitting down had substantive impact. Subsequent reports by FireEye indicated that the combined applications of clear signaling of potential sanctions and indictments indicating the United States had the defensive capacity to identify violators resulted in a shift in Chinese behavior and consequent reduction in overall non-national security espionage attempts.[73]

Despite substantial reductions in Chinese cyber espionage penetrations outside of national security organizations the problem has not been eliminated. But what the case demonstrates is that clear, sustained, multi-faceted CDD leveraging non-kinetic, but criminological, diplomatic, and economic threats of punishment improved upon a rapidly deteriorating status quo. The development programs of China remain heavily focused on the incorporation of information technologies within society, the development of Artificial Intelligence, and the facilitation of strategic and tactical advantages through national security cyber espionage. Yet, in spite of all these goals, deterrence remains applicable, not within domain and through equivalencies, but cross domain by leveraging the strengths of the United States as the deterrer relative to those of China to achieve changes in behavior.

[70] Nakashima, Ellen. 2015. "U.S. Developing Sanctions Against China Over Cyberthefts." *The Washington Post*. August 30. https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html.
[71] Sanger, David E. 2018. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Crown Publishers.
[72] 2015. "Obama Warns China on Cyber Spying Ahead of Xi Visit." *Reuters*. September 16. https://www.reuters.com/article/us-obama-roundtable-cybersecurity-idUSKCN0RG2AS20150916.
[73] 2016. "Redline Drawn: Chin Recalculates Its Use of Cyber Espionage." FireEye.

Recent reports indicate an uptick in non-national security related cyber espionage.[74] Such increases are not unexpected. Deterrence beyond the nuclear realm is not a one and done strategy. It is an iterative process of understanding the intentions of the adversary and how to efficiently threaten costs and at times through retaliation impose costs to achieve desired outcomes. The process of iterating and continuing to signal clearly with multiple potential tools the potential for the imposition of costs as retaliation for violations. Calibrating deterrence over time is costly and requires the use of the entire toolbox of state.

CDD Efforts Against Russia and Their Effects

Beginning in 2014 a Kremlin linked corporation, the Internet Research Agency (IRA), began the initial stages of developing a well resources campaign of information warfare against the United States.[75] This campaign was multifaceted and leverage multiple social media platforms with the intent of fostering discord within the U.S. political system. The U.S. House of representatives release more than 8.8 gigabytes of advertisements developed by Russian agents with the intent of creating discord during the U.S. elections.[76] This trove of data consisted of more than 3,519 paid advertisements on Facebook reaching more than 11.4 million Americans. An additional 470 IRA-created Facebook pages containing 80,000 pieces of organic content reached more than 126 million Americans.[77] In addition to information operations on Facebook, more than 36,000 Russian-linked bot (automated) accounts tweeted about the U.S. Election generating more than 288 million impressions. The IRA was directly linked to the publication of 130,000 tweets.[78]

Concurrent to the information warfare efforts undertaken by the IRA and other organizations with links to the Kremlin, in 2015 the FBI noticed and subsequently reported indicators of Russian attempt to infiltrate the Democratic National Committee (DNC).[79] Despite the FBI contacting the

[74] 2018. "Foreign Economic Espionage in Cyberspace." Washington, D.C.: National Counter Intelligence and Security Center.
[75] Masters, Jonathan. 2018. "Russia, Trump, and the 2016 U.S. Election." *Council on Foreign Relations.* February 26. https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election.
[76] 2017. "Exposing Russia's Effort to Sow Discord Online: the Internet Research Agency and Advertisements | U.S. House of Representatives." *Democrats-Intelligence.House.Gov*. November 1. https://democrats-intelligence.house.gov/social-media-content/.
[77] Ibid.
[78] Ibid.
[79] Sanger, David E. 2018. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Crown Publishers.

DNC, the technical staffers at the DNC, who were hired as contractors, were initially slow to verify both the source of the warning, the FBI, and the magnitude of the warning. The leadership of the DNC remained largely unaware of the attempted intrusions until 2016. The intrusions into the DNC and other political parties continued well into 2016. The hackers who breached the DNC released on Friday July 22nd, 2016 19,252 emails and 8,034 email attachments and included the top leadership of the DNC for a period of 1 year prior to the hackers.[80] The leaks of emails also followed reports that the DNC's database of opposition research was also stolen.[81]

Beyond hacking attempts against the DNC, Russian linked hackers also targeted key staff within the Hillary Clinton 2016 Presidential Campaign. Senior campaign staffers were sent phishing emails (spoof emails designed to social engineer the recipient into divulging login information). Campaign Chairman John Podesta, after attempting due diligence with campaign IT staff fell victim to the Phishing campaign and subsequently had more than 50,000 emails stolen, of which 20,000 were released by Wikileaks.[82]

Cybersecurity firm Crowdstrike in a series of blog posts and reports pointed the finger towards two different hacking organizations it identified as being affiliated with the Russian SVR (Foreign Intelligence Server) and the GRU (Russian Military Intelligence).[83] Crowdstrike subsequently named these two actor groups Cozy Bear (or Cozy Duke) APT 28 and Fancy Bear (Sofacy) APT 29.[84] Crowdstrike's initial findings have been largely supported by other cybersecurity firms and by the Intelligence community.[85] Beyond hacking the campaigns, the Department of Homeland Security (DHS) contacted election officials in 21 states to notify them they have been the targets

[80] Hamburger, Tom, and Karen Tumulty. 2016. "WikiLeaks Releases Thousands of Documents About Clinton and Internal Deliberations." *The Washington Post*. Washington, D.C. July 22. https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/.
[81] Ibid.
[82] Chang, Alvin. 2018. "How Russian Hackers Stole Information From Democrats, in 3 Simple Diagrams." *Vox*. July 16. https://www.vox.com/policy-and-politics/2018/7/16/17575940/russian-election-hack-democrats-trump-putin-diagram.
[83] Alperovitch, Dmitri. 2016. "Bears in the Midst: Intrusion Into the Democratic National Committee »." *Crowdstrike.com*. June 15. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.
[84] Ibid.
[85] Lemay, Antoine, Joan Calvet, François Menet, and José M Fernandez. 2018. "Survey of Publicly Available Reports on Advanced Persistent Threat Actors." *Computers & Security* 72 (January). Elsevier Ltd: 26–59. doi:10.1016/j.cose.2017.08.005.

of Russian government hackers.[86] DHS alerted election officials that Russian hackers were trying to hack both voter registration files and public election sites.[87]

In addition to the targeted information campaigns via social media, the theft of emails and their subsequent distribution via Wikileaks, Russian hackers register and launch websites including DCLeaks.com which further distributed stolen emails and documents while purporting to be run by Americans. These websites were implicated in further distorting the information environment.

In summation, for more than two years with increasing intensity Russian linked organizations both private, the IRA, and governmental, SVR and GRU, were heavily involved in efforts to attack the integrity of the US Electoral process at multiple different levels, ranging from the information environment, to the political parties and potentially to the voting systems themselves. In much the same way that President Obama approached challenge of Chinese hacking, he sought to avoid escalation while simultaneously halting Russian behaviors. However, unlike in the case above regarding Chinese cyberespionage the timeline in which President Obama was severely constrained. President Obama warned Russian President Vladimir Putin in a Private ninety-minute meeting on September 5, 2016 to knock off interfering in the U.S. election, in particular, he warned Putin not to interfere in the election itself or else he would use American economic might to severely disrupt the Russian economy.[88] Obama's discrete warning in a private meeting was subsequently followed up by a joint public statement from the Directors of Homeland Security and the National Intelligence one month later. [89]

Following the election the Intelligence Community released a nearly unanimous assessment on Russian interference in the 2016 election and President Obama ordered his administration to expel 35 diplomats, and impose retaliatory sanctions on Russia, including the closure of two Russian compounds.[90] These measures occurred post hoc and appeared to have limited impact on Russian

[86] Horwitz, Sari, Ellen Nakashima, and Matea Gold. 2017. "DHS Tells States About Russian Hacking During 2016 Election." *The Washington Post*. September 22. https://www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html.
[87] Ibid.
[88] Sanger. 2018. *The Perfect Weapon:*
[89] Ibid.
[90] 2016. "Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment." *Obamawhitehouse.Archives.Gov*. Washington, D.C.: Office of the Press Secretary.

operations in the United States. The measures have been rhetorically weakened by Trump administration.[91]

In the buildup to the 2018 mid-term elections most indicators point towards a renewed, albeit scaled back, attempt by Russian linked actors to meddle in U.S. Elections.[92] Microsoft as of August released substantial coordinated ongoing efforts to engaging in hacking ahead of the 2018 mid-terms.[93] These renewed efforts indicate a failure of U.S. retaliatory actions to sufficiently deter future hostile actions by the Russian Federation.

The case of Russian meddling in U.S. elections also does not meet the necessary prerequisites of armed attack or use of force. Yet the potential destructiveness of the meddling is readily apparent. As in the case of Chinese cyberespionage attempts at retaliation were cross domain and again emphasized diplomatic and economic mechanisms. Yet, the Russian case differs from the Chinese case in several respects. First, it was time sensitive in that efforts to forestall meddling needed to be in effect prior to the 2016 Presidential elections. Only when the threats prior to election failed were retaliatory actions undertaken. These post-hoc retaliatory efforts were too late and were akin to shutting the fence after all the cows already left the pasture. Second, the scale of threat and retaliation relative to the actor was insufficient to deter and the inconsistency of policy between administrations has weakened the signals being sent to the Russian Federation about the continued resolve of the United States relating to election meddling. Simply making noise about the meddling without any true consequence for the meddler does not result in deterrence.

Discussion

In neither the case of sustained Chinese espionage nor Russian interference in the 2016 election did any single act perpetrated by an adversary rise to a level equivalent to the use of force or an armed attack. Yet, in both instances the United States, with divergent effects was able to develop a CDD strategy to counter adversary behavior. In both instances within markedly different

[91] Pifer, Steven. 2017. "Trump, Russia, and Sanctions." *Brookings*. Washington, D.C. June 27. https://www.brookings.edu/blog/order-from-chaos/2017/06/27/trump-russia-and-sanctions/.
[92] Abbruzzese, Jason. 2018. "Russia's Political Meddling Efforts Go Beyond Midterms, Experts Say." *NBC News*. August 21. https://www.nbcnews.com/tech/tech-news/russia-s-political-meddling-efforts-go-beyond-midterms-experts-say-n902486.
[93] Newman, Lily Hay. 2018. "How Microsoft Tackles Russian Hackers—and Why It's Never Enough." *Wired.com*. August 21. https://www.wired.com/story/microsoft-russia-fancy-bear-hackers-sinkhole-phishing/.

timelines the United States interpreted discrete incidents cumulatively and attempted to aggregate the incidents and propose that both the United States and the perpetrator view the acts as constituting a violation of acceptable behavior warranting a retaliatory response. In both incidents while counter-cyber operations were proposed, the overt signal sent to the adversary was via threats of a diplomatic and economic nature. In both cases the U.S. government only substantially engaged in deterrent behavior in response to cumulatively interpreted cyber actions after private sector actors publicly brought forth substantial forensic and contextual evidence indicating the perpetrators of the violation. In both cases the United States viewed retaliatory threats as one-time events and failed to maintain or continue to develop potential mechanisms to pressure the adversary state. This tactic assumes immediate rather than iterated learning, something which is not supported by the literature.[94] Such a tactic is consistent with nuclear deterrence literatures in which the resultant retaliation imposes costs so substantial that further costs are unable to be imposed. Such a tactic is ill-suited to iterative learning in restrictive deterrence environments such as those identified by Tor.[95]

In both cases the challenge of responding to cyber-attacks in a timely fashion arises. Whereas the continuous cyberespionage activities of the Chinese necessitate a response, the response had no temporal constraints. The development of a CDD strategy targeted to specifics of the adversary and the threat posed allowed the Obama administration to build a suite of deterrence measures to effectively retaliate against China. The detailed analysis by the United States Government and private actors of a multitude of cyber-attacks combined with indictments, and the threat of severe and well-time sanctions to signal and achieve an impact reduced certain types of behaviors. In contrast to the CDD retaliations against China, the timeframe available to the United States to respond to the information warfare and cyber activities of the Russian Federation against the electoral processes of the United States was severely constrained. The constrained timeline necessitated rushed forensic and contextual analysis, furthermore the impact of the attacks was

[94] Axelrod, Robert. 1981. "The Emergence of Cooperation Among Egoists." *The American Political Science Review* 75 (02). University Libraries - Virginia Tech: 306–18; Axelrod, Robert. 1986. "An Evolutionary Approach to Norms." *American Political Science Review* 80 (4): 1095–1111.
[95] Tor, Uri. 2017. "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence." *Journal of Strategic Studies* 40 (1-2). Routledge: 92–117.

uncertain as opposed to the clear impact of sustained cyberespionage and theft. Both the shortened timeline and uncertain impact made timely decisions on potential deterrence strategies difficult. Moreover, domestic politics surrounding the election constrained the Obama administration's options for pre-election response and limited the impact of post-election response.

Conclusion

CDD strategies are not a silver bullet solution to the challenges presented by adversaries in cyberspace. What is clear however, is that based on the available evidence both within cyberspace and beyond is that artificially constraining deterrence strategies that seek to punish actors for cyber-attacks to retaliations occurring in and through cyberspace is inefficient and impractical. Just as a state wouldn't constrain itself to respond through equivalencies in other domains it should not seek to constrain itself within cyberspace. Moreover, the evidence to date indicates that strategies of CDD in cyberspace as in other domains below the nuclear threshold should not be absolute, but rather restrictive through iterative retaliatory mechanisms consistently assessed and modified to achieve a proportional response capable of altering an adversary's rational decision-making calculus. Yet even with all the considerations that support and highlight the potential effectiveness of CDD for providing a framework for deterring cyber-attacks, it is likely to take time to calibrate CDD to the actors a state such as the United States seeks to deter.