The Logic of Coercion in Cyberspace

Erica D. Borghard & Shawn W. Lonergan

Routledge
Taylor & Francis Group

The Logic of Coercion in Cyberspace

Erica D. Borghard and Shawn W. Lonergan

ABSTRACT

What are the dynamics of coercion in cyberspace? Can states use cyber means as independent tools of coercion to influence the behavior of adversaries? This article critically assesses traditional coercion theory in light of cyberspace's emergence as a domain in which states use force, or its threat, to achieve political objectives. First, we review the core tenets of coercion theory and identify the requisites of successful coercion: clearly communicated threats; a cost–benefit calculus; credibility; and reassurance. We subsequently explore the extent to which each of these is feasible for or applicable to the cyber domain, highlighting how the dynamics of coercion in cyberspace mimic versus diverge from traditional domains of warfare. We demonstrate that cyber power alone has limited effectiveness as a tool of coercion, although it has significant utility when coupled with other elements of national power. Second, this article assesses the viability and effectiveness of six prominent warfighting strategies in the traditional coercion literature as applied to the cyber domain: attrition, denial, decapitation, intimidation, punishment, and risk. We conclude that, based on the current technological state of the field, states are only likely to achieve desired objectives employing attrition, denial, or decapitation strategies. Our analysis also has unique implications for the conduct of warfare in cyberspace. Perhaps counterintuitively, the obstacles to coercion that our analysis identifies may prompt states to reevaluate norms against targeting civilian infrastructure.

Cyberspace has definitively emerged as the latest frontier of militarized interactions between nation-states. Governments, as they are wont to do in an anarchic international system, have already invested considerable resources to develop offensive and defensive military capabilities in cyberspace. It remains to be seen, however, how and to what extent these tools can be employed to achieve desired political objectives. Put simply, what is the logic of coercion in cyberspace? Can governments use cyber power to deter state adversaries from taking undesirable actions

Erica D. Borghard is an assistant professor in the Department of Social Sciences and Executive Director of the Grand Strategy Program at the United States Military Academy at West Point. Shawn W. Lonergan is an assistant professor and research scientist at the Army Cyber Institute at the United States Military Academy at West Point.

or compel them to bend to their wills and, if so, how and under what conditions?[1] This analysis draws on the large corpus of coercion theory to assess the extent to which existing frameworks can shed light on the dynamics of coercion in cyberspace. The article proceeds as follows. First, we outline the theoretical logic of coercion theory and identify the factors necessary for successful coercion. Each element of coercion is immediately followed by a discussion of how it applies to the cyber domain and an assessment of how the particularities of the domain reflect on the requirements of successful coercion. We demonstrate that, based on current capabilities, cyber power has limited effectiveness as an independent tool of coercion. Second, we explore the extent to which cyber power could be used as part of a war-fighting strategy to target an adversary's ability or willingness to resist and suggest which strategies are likely to be more versus less effective.[2] We assert that, based on current capabilities, attrition, denial, and decapitation strategies are most likely to be effective in cyberspace. Finally, we conclude with recommendations for policymaking and further research.

Coercion Theory

As Thomas C. Schelling so eloquently articulated, coercion is fundamentally about affecting an adversary's behavior using the threat or limited application of military force; "[i]t is the *threat* of damage, or of more damage to come, that can make someone yield or comply."[3] Coercion involves producing a desired behavior or outcome on the part of an adversary by forcing her to confront a cost–benefit calculus, such that the adversary believes it is less costly to concede to the threatener's preferred course of (in)action than to defy the latter's demands.[4] Coercion is distinct from brute force. In the latter case, one state defeats another militarily and then imposes a political settlement on the defeated power; in the former case, the target of coercion retains the military capacity to resist or concede, and the coercer seeks to achieve a political settlement short of full-scale

---

[1]Thomas C. Schelling makes the important distinction between compellence and deterrence. The former involves the threat or limited application of force to change an adversary's behavior, while the latter involves the threat of force (or pain, in Schelling's parlance), to preserve the status quo. See Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960) and idem., *Arms and Influence* (New Haven, CT: Yale University Press, 2008), 69–86. Robert J. Art elaborates on this concept. See Robert J. Art, "To What Ends Military Power?" *International Security* 4, no. 4 (Spring 1980): 3–35.

[2]The authors are grateful to Jack Snyder for pointing out the distinction between coercion and warfighting strategies.

[3]Schelling, *Arms and Influence*, 3. Emphasis in the original. Alexander L. George et. al. also emphasize that coercion can involve both the threat or limited application of military power. See Alexander L. George, David K. Hall, and William R. Simons, eds., *The Limits of Coercive Diplomacy: Laos, Cuba, Vietnam* (Boston: Little, Brown and Company, 1971), 2, 18. Lawrence Freedman distinguishes between coercion, as defined by Schelling, and "strategic coercion," which is "the deliberate and purposive use of overt threats to influence another's strategic choices." See Lawrence Freedman, "Strategic Coercion," in *Strategic Coercion: Concepts and Cases*, ed. Lawrence Freedman (Oxford: Oxford University Press, 1998), 15.

[4]Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996), 4. It is important to note, however, that Pape's reference to coercion in this context is distinct from deterrence; Schelling uses the umbrella term "coercion" to refer to both compellence and deterrence. See also Daniel L. Byman and Matthew Waxman, *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might* (Cambridge: Cambridge University Press, 2002), 3.

war by manipulating the cost–benefit calculus of the target state.[5] While coercion has always been a fundamental element of the exercise of state power, the advent of nuclear weapons and mutual assured destruction has made coercion even more critical. As Schelling explains, the prospect of civilization-ending nuclear warfare, coupled with advances in technology making it possible to target an enemy's population centers and hold its society at risk without first defeating its armed forces, has turned statecraft into the diplomacy of violence.[6] The significance of coercion for interstate relations has not decreased with the advent of cyber warfare; if anything, it has increased. Indeed, like nuclear weapons, cyber weapons enable governments to target adversary populations while bypassing the latter's military forces. For example, cyber weapons could be employed to target a state's critical infrastructure to render key pieces of a state's military systems inoperable at decisive times, as was allegedly the case when Syrian air defense systems failed to respond to an Israeli bombing operation against a purported Syrian nuclear enrichment facility in 2007.[7]

Notwithstanding the central role coercion plays in states' strategies, successful coercion—both its deterrent and compellent varieties—is difficult to achieve.[8] There is a large body of empirical literature that assesses the reasons for failed coercion, particularly focusing on examples of failed coercion in American foreign policy during the Vietnam War and through the use of air power in the post-Cold War international system.[9] In general, using the threat or limited application of military force to affect an adversary's behavior is difficult to accomplish because there are many factors that are necessary conditions for successful coercion, some of which are in tension with others. Moreover, if coercion is difficult to achieve through the threat or use of conventional military power, we argue that it is even more challenging in cyberspace. The literature on coercion suggests that four fundamental conditions must be met for coercion to succeed: the coercive threat must be clearly communicated; it must be linked to a cost–benefit calculus such that the

---

[5]Schelling, *Arms and Influence*, 2–6. Pape, *Bombing to Win*, 13.

[6]Schelling, *Arms and Influence*, 18–34. Schelling links technological advances in the power to hurt with the increased "importance of war and threats of war as techniques of influence, not of destruction; of coercion and deterrence, not of conquest and defense; of bargaining and intimidation," 33.

[7]Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2012), 1–8.

[8]It is widely accepted that deterrence may be easier to achieve, but harder for social scientists to observe due its negative object (for example, we only observe deterrence failures). Conversely, compellence is easy to observe but more difficult to achieve for precisely the same reason—there are reputational costs associated with being seen to back down and concede to an adversary's demands. Leaders who are successfully deterred could point to a variety of reasons they chose to not alter the status quo without losing face. See the discussion in Schelling, *Arms and Influence*, 74–75; Robert J. Art, "Coercive Diplomacy: What Do We Know?" in *The United States and Coercive Diplomacy*, eds. Robert J. Art and Patrick M. Cronin (Washington, DC: United States Institute of Peace Press, 2003), 361–62.

[9]See, for example, Pape, *Bombing to Win*; Todd S. Sechser, "Goliath's Curse: Coercive Threats and Asymmetric Power, *International Organization* 64, no. 4 (October 2010): 627–60; Wallace J. Thies, *When Governments Collide: Coercion and Diplomacy in the Vietnam Conflict, 1964–1968* (Berkeley: University of California Press, 1980); Alexander L. George, *Forceful Persuasion: Coercive Diplomacy as an Alternative to War* (Washington, D.C.: United States Institute of Peace Press, 1991); Art, "Coercive Diplomacy;" Alexander L. George and William E. Simons, eds., *The Limits of Coercive Diplomacy*, 2nd ed. (Boulder, CO: Westview Press, 1990); Byman and Waxman, *Dynamics of Coercion*; Thomas J. Christensen, *Worse Than a Monolith: Alliance Politics and Problems of Coercive Diplomacy in Asia* (Princeton, NJ: Princeton University Press, 2011).

target's costs of conceding are less than the costs of not complying; it must be credible; and there must be an element of reassurance.[10]

Communication

The essence of successful coercion is clear communication.[11] The target of a coercive threat has to know precisely the behavior in which the coercing state wants the target state to engage (or refrain from engaging), the timeframe in which the coercing state expects the target to comply, and the costs associated with cooperation versus defection. The target state must understand "what behavior of his will cause the violence to be inflicted and what will cause it to be withheld."[12] Ideally, coercion takes the form of an ultimatum: if State B does not do action X within timeframe Y, State A will take specified action Z. However, in the vast majority of international crises, political leaders default to ambiguity, rather than clarity, of threats; leaders often prefer to retain flexibility to escape from costly or imprudent commitments or be adaptive in their responses to an adversary's behavior, especially if they lack domestic political support.[13] The fundamental fact of anarchy complicates clear communication because it leads to poor, fragmentary information and creates incentives to misrepresent private information—indeed, this is a cause of war.[14] Beyond incentives for strategic ambiguity, clear signaling is complicated by misperceptions stemming from both cultural differences and cognitive limitations.[15] Insights from cognitive psychology have demonstrated that recipients of a signal tend to fit incoming information into preexisting beliefs, interpret signals based on implicit theories about their meaning, prefer simplicity over complexity, and are influenced by motivated biases.[16] Put simply, signaling often fails "because the perceiver does not understand what message the actor is trying to communicate."[17] Communication is

---

[10]Of course, this is not an exhaustive list of all of the factors that contribute to successful coercion. For example, George and Simons identify nine conditions that favor coercive diplomacy: clarity of objective, strong motivation, asymmetry of motivation, sense of urgency, strong leadership, domestic support, international support, fear of unacceptable escalation, and clarity of terms. See George and Simons, eds., *Limits of Coercive Diplomacy*, 279–91. However, we propose that these various lists and factors could be grouped into the four main conditions identified above.

[11]However, it is important to note a caveat that, in some instances, sending ambiguous signals can be advantageous for the purposes of coercion. Particularly in the context of nuclear bargaining, the threat that leaves something to chance—precisely because the risk of nuclear war generates extraordinary costs—may help a coercing state. See Schelling, *Strategy of Conflict*, chap. 8.

[12]Idem., *Arms and Influence*, 3–4.

[13]Jack Snyder and Erica D. Borghard, "The Cost of Empty Threats: A Penny, Not a Pound," *American Political Science Review* 105, no. 3 (August 2011): 429; Robert Jervis, "Deterrence Theory Revisited," *World Politics* 31, no. 2 (January 1979): 303; Richard Ned Lebow, *Between Peace and War: The Nature of International Crises* (Baltimore, MD: Johns Hopkins University Press, 1981), 29–27; Glen H. Synder and Paul Diesing, *Conflict Among Nations: Bargaining, Decision Making, and System Structure in International Crises* (Princeton, NJ: Princeton University Press, 1977), 213–15, 220. Even Schelling acknowledges that "most commitments are ultimately ambiguous in detail," *Arms and Influence*, 67.

[14]Freedman, "Strategic Coercion," 18; James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (Summer 1995): 379–414.

[15]Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976).

[16]Ibid., 117–202. Robert Jervis, "Signaling and Perception: Drawing Inferences and Projecting Images," in *Political Psychology*, ed. Kristen Renwick Monroe (Mahwah, NJ: Lawrence Erlbaum Associates, 2002), 306–8. See also Robert Jervis, *The Logic of Images in International Relations* (New York: Columbia University Press, 1970).

[17]Jervis, "Signaling and Perception," 304.

facilitated when actors can agree on a shared meaning of a particular type or vehicle of signaling (such as diplomatic language). In the case of diplomatic language, for example, clarity is easier to achieve because "both the signaler and the perceiver agree as to the message that the former is trying to convey."[18]

Communication in Cyberspace

Understanding intent is exceptionally difficult in the cyber domain. Many scholars and US government-sponsored studies have noted that cyber operations create a high probability of misunderstanding the coercing state's intentions.[19] Unlike diplomatic channels, in cyberspace there is no agreed-upon language that guides policymakers to a common understanding that helps divine the meaning behind a cyber signal. Moreover, in cyberspace, most operations are interactions between humans and machines facilitated by code for which there are few, if any, norms governing the exchange.[20] That many high-level decision makers lack even a basic understanding of the cyber domain and, therefore, are likely to be intellectually unprepared during a time of crisis, compounds this uncertainty. Furthermore, the signaler may be uncertain about what kind of cyber tool she should select to communicate in cyberspace because the actual effects of a cyber attack may be unpredictable ex ante—even to the signaler.[21]

Signaling in cyberspace is the most problematic of all the domains (land, sea, air, space, and cyber) because the signal may go unrealized. In other words, in cyberspace only the initiator may perceive the engagement.[22] Moreover, even if a target state realizes it has been attacked, it is difficult to infer the intent behind a cyber signal based solely on an observed incursion. This ambiguity has the potential to trigger unintended escalation because it is difficult to distinguish between hostile and benign intentions when an outside actor is perceived to have accessed a critical system.[23] In a

---

[18]Ibid., 300.

[19]For further reference, see Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard National Security Journal* 3 (December 2011): 85–142; Robert Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *Journal of National Security Law and Policy* 5 (October 2011): 539–629; William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009).

[20]For more on norms and international law as they pertain to the cyber domain, see Catherine Lotrionte, "A Better Defense: Examining the United States' New Norms-Based Approach to Cyber Deterrence," *Georgetown Journal of International Affairs* 8, no. 10 (April 2014): 75–88; Martha Finnemore, "Cultivating International Cyber Norms," in *America's Cyber Future: Security and Prosperity in the Information Age*, ed. Kristin M. Lord and Travis Sharp (Washington, DC: Center for a New American Security, 2011); Tim Maurer, "Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cyber-Security," *Belfer Center for Science and International Affairs* (September 2011); Oona A. Hathaway, et al., "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (August 2012): 817–85; David E. Graham, "Cyber Threats and the Law of War," *Journal of National Security Law and Policy* 4 (2010): 87–102; Jack Goldsmith, "How Cyber Changes the Laws of War," *European Journal of International Law* 24, no. 1 (2013): 129–38.

[21]The authors are grateful to Robert Jervis for illustrating this.

[22]For instance, it is easy to imagine how a single signal could get lost in the over eighty-eight thousand petabytes of IP traffic that are estimated to transverse the Internet per month.

[23]For further discussion of risks surrounding the ambiguity of intent in cyberspace, see Shawn W. Lonergan, "Cooperation under the Cybersecurity Dilemma," in *Confronting Inequality: Wealth, Rights, and Power*, ed. Hugh Liebert, Thomas Sherlock, and Cole Pinheiro (New York: Sloan, 2016). Also see Robert Jervis, "Some Thoughts on Deterrence in the Cyber Era," *Journal of Information Warfare* (forthcoming): 8–9.

hypothetical example, Japan may have an intelligence requirement to monitor the uranium enrichment efforts of North Korea. However, Japan's access to a network at a North Korean enrichment facility does not necessarily suggest that it intends to destroy North Korea's nuclear ambitions through cyber means; Japan could simply be monitoring the program to meet its own defensive requirements, which is widely accepted by international convention to be a necessary state practice.[24] Actors could exploit this uncertainty to their advantage, but it may also lead to unintended conflict.[25] Herbert Lin notes this ambiguity in cyberspace and concludes that the cyber domain presents an increased risk of accidental escalation: "In the absence of direct contact with those conducting such operations—sometimes even in the presence of such contact—determining intent is likely to be difficult and may rest heavily on inferences made on the basis of whatever attribution is possible. Thus, attempts to send signals to an adversary through limited and constrained military actions—problematic even in kinetic warfare—are likely to be even more problematic when cyber attacks are involved."[26]

Attribution problems complicate effective communication in cyberspace because they create problems for both target and initiator. From the perspective of the target state, a fundamental impediment to deciphering the intent behind a cyber signal is the difficulty of identifying the actor who sent it. This presents a challenge to policymakers because, if a cyber action is uncovered, the true meaning of the signal may not be ascertained without attribution. While some actions in themselves may send a clear signal without attribution, typically the identity of the signaling state is critical for coercion to succeed. For instance, in the prior scenario we assumed North Korea attributed the cyber incursion to Japan. However, what if North Korea were unable to attribute the access to Japan and had to surmise the intent of the incursion devoid of attribution? The spectrum of possible motivations of such an incursion ranges from a preparation for a preemptive attack from a rival such as Japan or the United States on one end of the spectrum, to a benign case of espionage from an ally such as China on the other. In this hypothetical case, not only is the signal obfuscated because intent cannot be deduced without attribution, but North Korea also does not know what is an appropriate response and against whom to respond. If these conditions are not met, coercion is by definition not possible.

There are, however, several methods to assign attribution following a cyber incursion.[27] The easiest ascription approach is when the perpetrator publically accepts responsibility for the action and the target state believes that the self-identified attacker possessed both the capability and motivation to carry it out.

[24]Geoffrey B. Demarest, "Espionage in International Law," *Denver Journal of International Law and Policy* 24 (1995): 321–48.

[25]Jervis, *Logic of Images in International Relations*, 86–87.

[26]Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly* 47 (2012): 57.

[27]For further reference on attribution, see Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37; Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of Cybersecurity* 1, no. 1 (2015): 1–15.

Another attribution technique mandates that the target state had access to the attacker's network from which the incursion originated and either witnessed the operation in real time or recorded it. This second method is difficult because it requires that the target state had access to the specific network from which the aggressor initiated an attack; that they observed the onslaught developing in real time and intentionally refrained from establishing tailored defenses or engaging in a preemptive attack to block the assault; or that that they had complete intelligence collection of all cyber operations from the adversary's network, which is typically technically difficult to consistently collect. However, in some instances governments may decide that the intelligence value of maintaining access outweighs the likely damage from the attack. Another attribution method is when sensors placed either at Internet service providers or key nodes in the Internet run algorithms that analyze raw data flows and scan for anomalies and variants of known attack signatures. However, the real-time use of such technology is still in a nascent stage and there is currently no guarantee that, once detected, the source of the malware could be traced back to the true originator.[28] The final method of assigning attribution occurs when the signature of the attack (the coding) is so unique that it could be traced to a specific actor or threat network. Yet, this method heightens the risk of falling victim to deceptive techniques, such as embedding remarks in a foreign language of a noninvolved party, which may confound forensic experts seeking to assign attribution. Recently, however, there have been advances in signature recognition software designed to scour millions of lines of code to compile unique profiles of the developers.[29] Moreover, from the target's perspective, even if she is able to successfully attribute an attack to a particular actor, she may be hesitant to reveal her ability to do so because it would likely require going public with valuable information that could compromise her own capabilities and accesses. For instance, the United States' decision to quickly attribute the Sony hack in late 2014 to North Korea likely revealed and compromised American accesses to other governments' cyber infrastructure.[30]

[28]Gerhard Munz and Georg Carle, "Real-Time Analysis of Flow Data for Network Attack Detection" (paper presented at the 10th IFIP/IEEE International Symposium on Integrated Network Management, Munich, Germany, 21 May 2007).

[29]Developing unique signatures of attackers and code developers is becoming more common as exploits become increasingly sophisticated and threat data is shared among cyber security practitioners. Stuxnet, for instance, was nearly fifteen thousand lines of code that comprised over five hundred thousand bytes. That is the equivalent amount of digital data as a large textbook. Governments have been keen to invest in digital forensic technology, as evident in then Secretary of Defense Leon Panetta's 11 October 2012 address from the deck of USS *Intrepid*, where he noted: "The department has made significant advances in solving a problem that makes deterring cyber adversaries more complex: the difficulty of identifying the origins of that attack. Over the last two years, [the] DoD has made significant investments in forensics to address this problem of attribution and we're seeing the returns on that investment. Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America," see Leon Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," 11 October 2012, http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136. For a review of Panetta's speech, see Jack Goldsmith, "The Significance of Panetta's Cyber Speech and the Persistent Difficulty of Deterring Cyberattacks," *Lawfare*, 15 October 2012.

[30]The authors thank Robert Jervis for this comment.

Attribution issues create problems not only for the target state attempting to infer the intent behind a signal, but also for the coercing state seeking to send a clear signal. The conventional wisdom on cyber operations posits that states typically seek to avoid attribution when conducting cyber exploitation and espionage operations. However, coercion in cyberspace requires attribution to be effective. A coercing state may employ several methods to ensure attribution. First, a state could couple the action in cyberspace with a formal diplomatic message, elucidating the meaning the signal (the cyber attack) was intended to convey.[31] Coupling a cyber operation with a diplomatic message may be the least costly method to ensure ascription for the coercer, but it must also be credible. This technique was observed in March 2016 when Secretary of Defense Ashton Carter, in a formal public statement, acknowledged that the United States conducted a cyber attack against the Islamic State of Iraq and Syria's command and control systems in Mosul, Iraq.[32] However, a coercing state must ensure that the target believes its self-declared attribution. This could present a problem for the coercing state if, in order to demonstrate that it was the one sending a signal, it had to reveal capabilities and accesses that it may prefer to keep private. Second, if coupling is not an available avenue, some have postulated several technical methods to ensure attribution, such as embedding unique signatures in code.[33] This type of ascription technique demands that some trace of the cyber operation remain on the target's machines.

This suggests that simply gaining access to a network and conducting cyber espionage is not sufficient to send a coercive signal in cyberspace—even if such accesses may be necessary to support a coercive signal.[34] While much of the discussion in the public domain conflates cyber espionage and cyber military operations, these are in fact distinct, just as they are in conventional domains. All forms of espionage, whether conducted in cyberspace or elsewhere, are fundamentally about collecting private information against another actor. Conversely, to be coercive, a cyber signal must be attributable and aim to disrupt, deny, degrade, and/or destroy data resident on computers and computer networks, or the systems themselves.

---

[31]Jervis, *The Logic of Images in International Relations*, 139–44.

[32]Damian Paletta and Felicia Schwartz, "Pentagon Deploys Cyberweapons against Islamic State," *Wall Street Journal*, 29 February 2016.

[33]Goldsmith, "Panetta's Cyber Speech."

[34]This, of course, creates something of a paradox for a coercing state because it may need to gain prior access to a system or network (which requires obfuscation and avoiding attribution) to send a subsequently attributable coercive signal. The one caveat to this is that cyber espionage could be used to conduct a data breach of sensitive information that can later be released to embarrass or otherwise intimidate some actor. Though cyber espionage may be a complex operation, depending on how well defended the network or computer the targeted information was resident on is, it is not a costly coercive cyber signal. Rather, cyber is being used as a vehicle to acquire information. It is not being employed as a signaling mechanism in itself. Due to this, the 2015 Sony hack is not a coercive cyber operation because it did not seek to destroy or disrupt and systems, but rather was used to steal embarrassing insider information. In this instance, if North Korea were to use the information gleaned from its alleged cyber attack on Sony's systems to coerce the company into refraining from releasing a movie, its cyber espionage would constitute a tool that was the component of a broader coercion strategy, but the fact that North Korea breached Sony's networks to steal information was not in itself sending a costly signal to the company. Cyber espionage is a routine aspect of interstate interactions in cyberspace and, in itself, does not meet the threshold of a costly signal. It is possible that cyber espionage activities could be coupled with other costly signals but, independently, it is not one.

Cost–Benefit Calculus

Coercion theory assumes that states are rational actors who make cost–benefit calculations when determining how to respond to threats and inducements posed by other actors in the international system. The benefit side of the calculus involves how much the adversary values a particular course of action, while the cost side entails the price she anticipates paying in order to carry it out.[35] Coercion, put simply, forces the target state to choose between "making concessions or suffering the consequences."[36] Therefore, to be effective, a coercing state must issue a threat such that the target perceives it to be more costly to suffer those consequences than to concede.[37] To succeed, the coercer must know what the target state values and, therefore, what it can hold at risk to get the target to comply; or, in Schelling's parlance, "[c]oercion requires finding a bargain, arranging for him to be better off doing what we want—worse off not doing what we want—when he takes the threatened penalty into account."[38] More important than an objective measure of costs versus benefits, however, is how the adversary perceives them, which stems from "the magnitude of the dangers and profits the adversary sees ahead for a given path and the probability of their occurrence."[39] At its core, therefore, coercion is the manipulation of the target's perceptions of the cost–benefit balance of a particular course of action.[40]

Affecting an adversary's cost–benefit calculus may seem deceptively simple; in practice, it could fail across multiple dimensions. Coercion could fail because the target does not understand what the adversary values and, therefore, does not know how to appropriately tilt the cost–benefit calculus. This could stem from poor intelligence or, more fundamentally, from the fact that leaders are not always rational, utility-maximizing economic individuals. It may be difficult to quantify what a target state values if it involves something intangible (such as prestige) and, therefore, hard to assign a numerical value to the cost a coercer must threaten to impose to achieve a desired behavior. Relatedly, coercion could fail because states are not unitary actors and, therefore, there may be domestic political or bureaucratic organizational considerations that factor into what a target state values, how it perceives costs versus benefits, and acceptable levels of risk that the coercing state does not take into account. Moreover, even if the coercer knew what the adversary values, it could be politically difficult to make a sufficiently costly threat. Finally, coercion could fail due to cognitive limitations on the part of the target. Insights gleaned from prospect theory, for instance, have illustrated that individuals often fail to make rational, cost–benefit calculations when assessing risk (such as being more averse to losses than gains) and misunderstand sunk costs.[41]

[35]Byman and Waxman, *Dynamics of Coercion*, 11.
[36]Pape, *Bombing to Win*, 12.
[37]Byman and Waxman, *Dynamics of Coercion*, 10. Pape, *Bombing to Win*, 15–16.
[38]Schelling, *Arms and Influence*, 4.
[39]Byman and Waxman, *Dynamics of Coercion*, 11.
[40]George, *Forceful Persuasion*, 11–14. George also points out that the more expansive or extreme the demands of the coercing state are, the costlier the threat must be to secure compliance.
[41]Byman and Waxman, *Dynamics of Coercion*, 10–14. Schelling, *Arms and Influence*, 86. Jack S. Levy, "Prospect Theory, Rational Choice, and International Relations," *International Studies Quarterly* 41, no. 1 (March 1997): 87–112.

Cost–Benefit Calculus in Cyberspace

In cyberspace, the state issuing a coercive threat must calculate what target to go after and the effect it seeks to deliver against it. Similarly, the target must also calculate whether it can absorb the cost and, if so, whether the coercer can ratchet up the cost to the target while avoiding too much cost itself. There are several categories of targets a state may consider attacking in cyberspace to coerce another state. Generally speaking, the class of target that inflicts the highest level of cost, a state's critical infrastructure, is typically the hardest to gain access to due to the technical complexities stemming from custom, tailored uses and advanced physical and virtual defensive measures commonly emplaced around these vital capabilities. The United States Department of Homeland Security has defined these crucial nodes as" … systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters."[42] This category includes critical infrastructure that is essential for everything from the safeguarding of nuclear regulatory systems to gas pipelines, and control systems that enable communication systems to work.[43] In the United States, many of these critical systems are ran by private industry, but in states with parastatal enterprises (such as China), they remain centrally controlled by the government. Not all pieces of critical infrastructure, however, are universally valued across states. For instance, diverging state opinions over the ideal relationship between the citizen and the Internet has changed what states may consider critical infrastructure. Indeed, one accomplished Chinese academic with senior-level party connections noted to the authors that their "Great Fire Wall," which restricts citizen access to Western media sources, is considered part of China's critical infrastructure.[44] In this case, attacking a vital node that the state links to regime stability would be significantly costlier for China than the destruction of other types of critical infrastructure. Similarly, the recent hack of the US Democratic National Committee, allegedly committed by Russia or Russian-sponsored groups, is an example of how a state could target a critical component of a democratic regime—its electoral system.[45] This creates the potential for unintended escalation dynamics if the coercing state did not accurately calculate the extent to which the target values its electoral process.

Military capabilities may also be targeted by cyber attacks. These targets include everything from software running on advanced avionic platforms, to air defense

---

[42]"National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency," *Department of Homeland Security*, 2009, https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[43]Control Systems are defined as, "Computer-based systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators)," ibid., 109.

[44]Professor at Peking University, Beijing, China, in discussion with the authors, 17 June 2015.

[45]David E. Sanger and Eric Schmitt, "Spy Agency Consensus Grows That Russia Hacked D.N.C.," *New York Times*, 26 July 2016.

assets, communication systems, and satellites tied into the Global Positioning System (GPS). Setting one's cyber sights on these military systems is similar in terms of costliness to targeting civilian critical infrastructure in that both are custom engineered and are typically difficult to gain access to and, therefore, mandate a highly tailored capability to exploit. Additionally, given that military systems are designed to be used during times of conflict, they tend to be more secure than civilian infrastructure because they are created with the expectation that they may be attacked via cyber means and, therefore, there is a greater emphasis placed on survivability and resilience early on in the development cycle.

From the target's perspective, attacks against critical national infrastructure and military capabilities are the most costly types of attacks, precisely because governments rely on these to survive in the international system and perform their basic functions. Coercing states may also choose to target the corporate sector of another state, depending on permissibility allowed by its own domestic legal regimes. Targets could include the online banking ability of a particular bank, the network of a leading defense contractor, or consumer information held by retailers. There is variation in terms of the cost to a coercer of targeting a particular company or sector of the economy, and this variation is largely a function of the resiliency and defenses that private actors choose to incorporate into their networks and systems. However, in terms of the perceived cost to the target state, generally speaking, cyber attacks against a private company are of a lower magnitude than attacks against critical national infrastructure and military capability, including command and control capabilities. Therefore, these kinds of attacks would only be useful to coerce a target state into conceding on relatively minor issues, if at all. This is analogous to conventional domains—dropping ordnance on a Walmart is fundamentally different from dropping ordnance on a communications node. However, there are two important caveats to this analysis. First, there may be some reputational costs a target may incur if attacks against certain private sectors actors are perceived to undermine the legitimacy of the regime. Second, there is likely to be important variation stemming from regime type, because some kleptocratic states may rely on the support of key industries or even companies to maintain regime stability. In these cases, attacks against business or industry may be comparable in terms of perceived cost to attacks against critical national infrastructure.

Regardless of the nature of the target, when sending a coercive signal in cyberspace, a policymaker must decide if she wants to produce a disruptive or destructive effect, the most salient distinction in the domain. Thus, a policymaker employing cyber attacks as a coercive instrument of state power must make a calculation of what effect is necessary to achieve the desired outcome. Destructive cyber attacks take two forms: the rare cyber attacks that generate an effect felt in the physical world, and the more common destruction of digital information, which can be almost as dire as a physical attack for many pieces of infrastructure. Disruptive attacks, conversely, seek to operationally diminish a system to the point that a user lacks confidence in its ability to perform some function. The latter may be more appealing to a coercing government

because disruptive attacks enable functionality of the affected system to be restored once the attack is ceased and, thus, may aid in reassuring the target state, as will be discussed in a later section. Notwithstanding the above discussion, states may be unable to perfectly tailor a cyber signal to affect a target's cost–benefit calculus. In other words, the technical complexities of certain types of costly operations may force less capable states into sending less costly signals that don't sufficiently alter the target's calculations. Governments may find cheap, fast, and easy cyber operations appealing even when they are less effective for the purposes of coercion. Put simply, governments may hit what they can get, rather than the optimal target to coerce another state.

Credibility

Beyond being costly, a coercer's threat must be credible—the target must believe that the coercer will actually carry it out. A threat is credible if it is in a state's interests to carry it out and if that state has both the capability and the resolve, or political will, to do so.[46] Credibility is arguably one of the most difficult aspects of coercion, which is why Schelling devotes an entire chapter of *Arms and Influence* to "the threats that are hard to make, the ones that are not so inherently credible."[47] While it is challenging to assess a coercing state's ability to carry out a threat, it is even more difficult to discern and demonstrate resolve.[48] Furthermore, in games of chicken, testing resolve through the limited application of force only tends to harden resolve even more, because the very act of probing resolve engages a state's political legitimacy and reputation, making leaders more likely to dig in before they give in.[49] A target may doubt a coercer's resolve because it doesn't believe that it is in the latter's interests to carry out the threat (this was particularly important in the context of nuclear deterrence); or because it doubts that the leader has sufficient domestic political support to carry out the threat;[50] or because the coercer has not established a reputation for carrying out past threats.[51] How individuals actually assess credibility, however, is poorly understood.[52]

Because credibility is difficult to convey but essential for coercion, states attempt to enhance the credibility of their threats by making them costly—through sending costly

---

[46]Schelling, *Arms and Influence*, 36.
[47]Ibid. Of course, one of the reasons Schelling found credibility so confounding was the problem of coercion in the nuclear age, where carrying out a threat would mean immeasurable costs to oneself as well as one's adversary.
[48]Stephen Biddle, for example, discusses how assessing the raw, quantifiable capabilities of states' militaries is a poor predictor of battlefield outcomes because it does not take into account force employment. See Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, NJ: Princeton University Press, 2006). For difficulties ascertaining resolve, see Art, "Coercive Diplomacy," 365.
[49]Ibid., 365–66. See also Snyder and Diesing, *Conflict Among Nations*, 118–22.
[50]Randall L. Schweller, *Unanswered Threats: Political Constraints on the Balance of Power* (Princeton, NJ: Princeton University Press, 2008).
[51]Schelling asserts that a country's image—others' expectations about how it is likely to behave—is "one of the few things worth fighting for." This is due to what Schelling describes as the interdependence of threats. See Schelling, *Arms and Influence*, 124, 55–59. Also see Herman Kahn, *On Thermonuclear War* (Princeton, NJ: Princeton University Press, 1960), 566. For a critique of the importance of having a reputation for resolve, see Jonathan Mercer, *Reputation and International Politics* (Ithaca, NY: Cornell University Press, 1996).
[52]Robert Jervis, "Deterrence and Perception," *International Security* 7, no. 3 (Winter 1982–1983): 9.

signals. James D. Fearon asserts that, "to be credible, a threat must have some cost or risk attached to it that might discourage an unresolved state from making it."[53] That's because talk is cheap: "words are cheap, not inherently credible when they emanate from an adversary, and sometimes too intimate a mode of expression."[54] There are two mechanisms states can employ to generate costly and, therefore, credible signals. First, states can tie their hands, limiting their choices and increasing the costs of backing down in the event the target of coercion does not comply with the terms of the threat. Second, states can sink costs, taking actions that are costly up front, such as mobilizing troops.[55] Using a similar framework, Robert Jervis describes how states can use indices to generate costly signals. Indices are "behaviors (either verbal or nonverbal) that the perceiver believes are inextricably linked to a characteristic that helps predict what the actor will do in the future."[56] Democracies, it has been argued, may have an advantage in costly signaling because they can more easily tie their hands through incurring audience costs.[57] Generating costly signals does not come without risks— indeed, costly signaling, paradoxically, is designed to increase the risk of war through locking in coercers to the use of force in order to (hopefully) avoid it.[58] Furthermore, there are myriad reasons states may seek to avoid a perfectly committing threat through sending an unambiguous costly signal, as previously noted.

Credibility in Cyberspace

As the coercion literature has elucidated, making a credible threat requires both the capability to impose the threatened cost and the will to employ it if the party to be influenced does not comply with the issuer's demands. Credibility in cyberspace could be established via two mechanisms. First, establishing indices could create a venue for states to better communicate and demonstrate capability. However, indices of cyber power do not yet exist and are likely to be difficult to form. Therefore, at present, credibility is most likely to be inferred through costly signaling.

Cyber Power Indices

Establishing indices of cyber power contributes to the credibility of threats in cyberspace because it helps ascertain a state's capability.[59] Perfect information of another state's cyber capabilities does not exist; therefore, indices facilitate a state's

---

[53]James D. Fearon, "Signaling Foreign Policy Interests: Tying Hands Versus Sinking Costs," *Journal of Conflict Resolution* 41, no. 1 (February 1997): 69.

[54]Schelling, *Arms and Influence*, 150.

[55]Fearon, "Signaling Foreign Policy Interests," 70. Schelling also refers to these dynamics in his discussion of commitment through the use of bridge burning, trip wire forces, plate glass windows, and engaging a nation's honor and prestige through public commitments. Schelling, *Arms and Influence*, 44–49.

[56]Jervis, "Signaling and Perception," 300.

[57]The idea that democracies have an advantage in costly signaling has been the conventional wisdom in the literature, although Jessica L. Weeks argues that autocratic regimes are also capable of generating audience costs. Jessica L. Weeks, "Autocratic Audience Costs: Regime Type and Signaling Resolve," *International Organization* 62, no. 1 (Winter 2008): 35–64. For a different critique of audience costs logic, see Snyder and Borghard, "The Cost of Empty Threats."

[58]Fearon, "Signaling Foreign Policy Interests," 82–83.

[59]Robert Jervis, *The Logic of Images in International Relations*, 26–28.

assessment of another state's ability to carry out threats. In cyberspace, these indices include budgets, growing and training cyber forces, establishing commands, and advertising participation in major cyber exercises.[60] When assessing capabilities in cyberspace, it is also critical to analyze how the latter would be employed. In particular, states in this domain may feel less constrained by international laws and norms (or even the threat of assured retaliation because, as this analysis demonstrates, these threats are difficult to credibly convey). This is because actors in the cyber domain tend to prefer to obfuscate their identities, leading some state actors to be more willing to act in ways that they would not otherwise be willing to on a battlefield or via formal diplomatic channels.

Estimating the capability of a cyberspace actor is a conundrum that has challenged scholars because the opaque nature of the domain confounds measurement efforts.[61] In the nuclear and chemical warfare arenas, there are methods to estimate the stockpiles of arms a nation holds and for which there exist treaties, accords, and international oversight institutions that monitor and limit the quantities of these weapons. However, in the cyber world there is no measure of relative strength; one cannot simply count the number of cyber tools the way one can count the number of warheads or the pounds of poison gas a country possesses. This is because offensive cyber capabilities are not universally lethal. A shroud of secrecy surrounds a nation-state's cyber capability and, therefore, creates a situation of imperfect information from which a policymaker must judge another state's actions and intent. Unlike in the conventional or nuclear realms, where states can reveal their capabilities to bolster credibility (or where the technology necessitates public tests to assess their effectiveness, such as nuclear tests), in the cyber realm states typically prefer to—and can—keep capabilities secret because revealing them would enable adversaries to defend against them and render the capabilities impotent. In other words, it is harder for states to reveal private information in cyberspace to enhance the credibility of their threats.[62] Moreover, governments face unique difficulties deriving intent based on observed capabilities because many states in the cyber domain find themselves coercing with the weapons they have, rather than the ones they may want or need. In other words, there may be a large gap between capabilities and intent. A distinction should be made here between what a state can measure about its own cyber capabilities and what its adversaries can assess. Measuring a rival's military strength has always been more difficult than introspective assessment due to military secrecy. However, the difference in cyberspace is that self-assessments of cyber capabilities (at least currently) also happen to be much harder to conduct because effective metrics have yet to be

---

[60]It general sense, it may be easier for democracies to showcase their level of cyber power due to greater institutionalized transparency over military organizations and budgets compared to authoritarian regimes.

[61]For example, see H. J. Seo, Yoon-Cheol Choy, and SoonJa Hong, "A Study on the Methodology to Evaluate the Level of Nation's Capability for Cyber War" (paper presented at the 12th Annual International Workshop on Information Security Applications, Korea, August 2011).

[62]The authors are grateful to Robert Jervis for clarifying this point.

devised. This, in turn, makes assessing another state's cyber-military might even more difficult than for other domains and types of weapons.

Furthermore, measures of cyber power include factors beyond raw estimates of the size of cyber forces. While human capital and skill levels are important contributors to capability in the conventional domain, they are arguably even more vital in the cyber domain. Simply counting the number of cyber forces that a country may openly report as an assessment of cyber power does not take into account the differences in skill levels and a state's relative depth of cyber operations. A lack of homogeneity of material resources and technically proficient human capital across states means that one cannot precisely compare cyber capabilities between states. Comparing quantities of cyber forces is akin to comparing quantities of ships in a navy without distinguishing between tugboats and aircraft carriers. Regime type also factors into capabilities. Some states, such as Russia and China, place a greater emphasis on developing cyber forces to monitor their citizenry to detect unrest and preserve regime stability. From a technical standpoint, these operations are markedly different from conducting a destructive cyber attack against a state adversary. Democratic states have the advantage of devoting fewer cyber resources to population monitoring and, therefore, are freer to invest in adversary-centric capabilities.[63] Finally, what matters for capability in cyberspace is having the right operator, armed with the right capability, with access to a vulnerable target, rather than a numerical advantage. Capability and access imply that, regardless of how skilled an individual operator is, she will always be constrained by the cyber tools with which she has been equipped.

Cyber Operations as Costly Signals

In order to bolster the credibility of a threat, states often engage in costly signaling that ranges from national leaders' threats and troop mobilizations, to onshore trip wires, to the movement of aircraft carriers during times of crises.[64] All of these serve

---

[63]Authoritarian states have gone to extensive efforts to institute hierarchies in their Internet infrastructure so that they can keep their citizens from accessing material that they deem may threaten regime stability. However, the West has pursued a free and open Internet that is largely devoid of state censorship. These conflicting visions for the Internet was evident in the 2012 breakdown of the United Nation's International Telecommunications Union's World Conference on International Communication (WCIT) when, in the wake of Arab Spring, many Middle Eastern states joined a voting bloc led by China and Russia to press for a treaty that limited the openness of the Internet and removed protections on free speech and human rights. In response, Canada, the United States, and many European states refused to ratify the treaty. This divide has given rise to extensive debates about Internet governance, state sovereignty in cyberspace, and the "Balkanization" of the Internet. See James D. Fielder, "The Internet and Dissent in Authoritarian State," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton, FL: Taylor and Francis, 2014); Daniel W. Drezner, "The Global Governance of the Internet: Bringing the State Back In," *Political Science Quarterly* 119, no. 3 (Fall 2004): 477–498; Stephen K. Gourley, "Cyber Sovereignty," in *Conflict and Cooperation in Cyberspace*; Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013); Dana Polatin-Reuben, and Joss Wright, "An Internet with Brics Characteristics: Data Sovereignty and the Balkanisation of the Internet" (paper presented at the 4th USENIX Workshop on Free and Open Communications on the Internet, San Diego, CA, 18 August 2014).

[64]Fearon, "Signaling Foreign Policy Interests." Schelling, *Arms and Influence*. Christian Le Mière, "The Return of Gunboat Diplomacy," *Survival* 53, no. 5 (October–November 2011): 53–68. Dr. Strangelove's Doomsday machine is perhaps the ideal embodiment of Schelling's perfect coercive capacity. We are grateful to an anonymous reviewer for making this analogy.
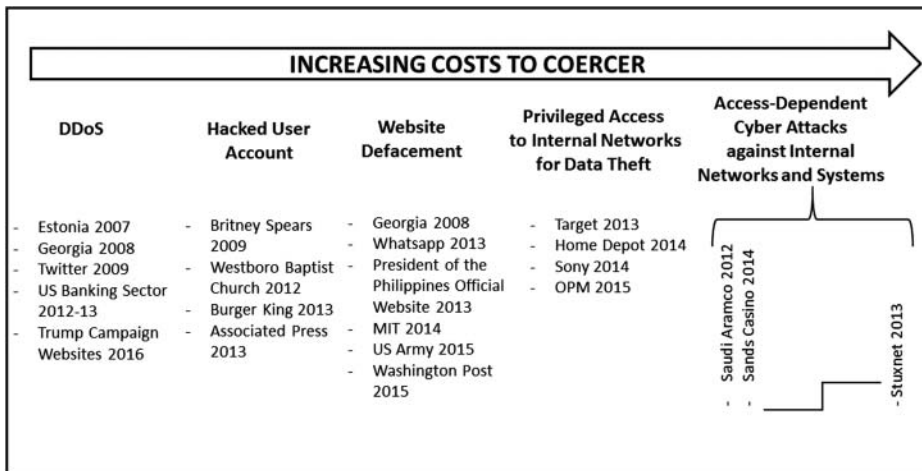
Figure 1. Spectrum of coercive cyber operations.[65]

to demonstrate a state's capability and willingness to follow through with the terms of a threat. The greater the cost to the initiating state of producing a given signal, ceteris paribus, the more effective the signal is as an indication of the initiating state's resolve. Therefore, leaders could use cyber operations to convey their commitment to a particular course of action if they are sufficiently costly to produce.[66] Not all cyber operations are equally costly for the coercing state, however. Some operations are resource intensive, whereas other types of operations, such as a Distributed Denial of Service (DDoS) attacks and website defacements, can be conducted using minimal resources. In this regard, it is helpful to conceptualize interstate cyber signaling as existing along a spectrum where the greater the resource requirements, the costlier the signal is to produce, and the more resolve it demonstrates.

As Figure 1 demonstrates, states could send signals via five broad categories of cyber attacks that are increasingly costly. The cheapest way to attack another entity is to conduct a DDoS attack. This is an operation where multiple compromised systems are

---

[65]Several of the examples provided in this graphic include cyber operations conducted by nonstate actors that were not necessarily coercive cyber operations. Though this study addresses state-initiated cyber operations, the listed examples are used to provide the reader with highly publicized cyber operations to assist with conceptualization. Furthermore, note the gap between the attacks against the Sands Casino and Saudi Aramco on the one hand, and Stuxnet on the other. There is a dramatic capability difference between the former examples and Stuxnet, which is assessed to have taken the work of thousands of individuals and millions of dollars over a several year time span. For further reference to the complexity of Stuxnet and the resources necessary to develop such a capability, see Ralph Langner, "Stuxnet's Secret Twin," *Foreign Policy*, 19 November 2013. Furthermore, it is important to note that there can be exceptions to the linear increase in costs depicted in this graphic. In other words, some types of attacks may be relatively more costly than how they are categorized in this graphic under unique conditions. For example, a DDoS attack against an extremely hardened target may be more costly to carry out than gaining access to a social media account.

[66]Though nonstate actors may engage in these activities, the scope of this article is limited to state-to-state exchanges. Furthermore, while Fearon discusses both tying hands and sinking costs as mechanisms for generating costly signals, we focus on cyber operations as sunk costs because the tying hands logic is a poor fit for the cyber domain. The only likely allegory to tying hands in cyberspace is the ability, in some instances, to create automaticity by initiating an autonomous offensive cyber response.

directed by a central computer to flood another computer with information requests. When enough compromised computers are connected together they act as one botnet (a network of enslaved information technology devices that can be centrally controlled) and, if the network is large enough, it may overwhelm the processing capabilities of the intended target and force it to shut down. Examples of this include the alleged Iranian-based DDoS attacks against the US financial sector in 2013, which took down the retail pages of over twenty-six corporations over a four-month time span.[67] These operations are on the far left of the spectrum because they are not inherently expensive to conduct (even though they may force the target to absorb high costs). The current going rate for a 24-hour DDoS attack is approximately $400–800 USD on the black market, depending on the size of the botnet being employed.[68] Furthermore, these operations are access agnostic in that, in order to conduct the operation, the attacker does not have to be pre-positioned with a back door into the target's network to facilitate the attack.

To send a costlier signal, a state could engage in operations designed to hack user accounts, including email and social media accounts. These are slightly costlier than DDoS attacks because they involve acquiring the credentials of an individual with access to the specific target (unless, in the unlikely scenario, the perpetrator can guess the target account's password). A well-known example of this is the 2013 hack of the Associated Press's Twitter feed, where hackers tweeted that there were two explosions in the White House and that the president was injured, prompting volatility in the stock market.[69]

Website defacement represents an additional level of cost for several reasons. First, it requires a minimal level of knowledge of webpage design coding. Second, website defacements involve delivering an effect to produce the observed defacement or redirection. Third, it is dependent on gaining access to the website administrator's account. Notable examples include the defacement of the United States Army's official website in 2015 and the Syrian Electronic Army's hack of a *Washington Post* website in 2015.[70]

Even more costly is gaining privileged access to internal networks for the purposes of data theft. This is more difficult than gaining access to a typical end user's account because it often relies on gaining access to internal systems and data repositories to which end users typically lack access. Most companies limit privileged accesses of this nature and compartmentalize this kind of information due to the potential consequences of a breach perpetrated against even a single actor with such extraordinary accesses (or by the actor herself). There is also an element of scale in these types of cases because attackers can acquire large amounts of private information, such as the contents of corporate email servers, billing records, personally identifiable

[67]Deloitte CIO Journal, "DDoS Attacks on U.S. Banks: Worst Yet to Come?" *Wall Street Journal*, 19 February 2013.
[68]Data comes from black markets accessed on the Dark Net on 17 March 2016. We are grateful to "BillyBear" for his assistance with this.
[69]David Jackson, "AP Twitter Feed Hacked; No Attack at White House," *USA Today*, 23 April 2013.
[70]Polly Mosendz, "Syrian Electronic Army Claims to Have Hacked US Army Website," *Newsweek*, 8 June 2015. Brian Fung, "The Syrian Electronic Army Just Hacked the *Washington Post*, Again," *Washington Post*, 14 May 2015.

information, and confidential information and documents pertaining to corporate strategy and development efforts. Two well-publicized examples of this kind of attack include the hack of the Department of Defense's Office of Personnel Management in 2015, allegedly committed by China, which compromised the personal information of nearly twenty-two million federal employees and their friends and family; and the 2014 attack against Sony Picture Entertainment, attributed by the US government to North Korea, which released embarrassing corporate communications, policies, and personally identifiable information of employees.[71]

The costliest type of signaling is a cyber attack that requires gaining access to well-defended or closed networks and seeks to disrupt or destroy key systems. Within this category, there is wide variation in the resources required to conduct these operations. The cost depends on the complexity of the attack and the relative difficulty of gaining access to the targeted systems. Since these types of operations disrupt or destroy data, they require customized tools that will produce the desired effect once inside the network. Furthermore, transacting in what is often a well-defended, restricted area is difficult not only because of the code-based language of exchange, but also because gaining access to closed and defended networks requires a significant investment of materiel resources and human capital. This investment includes not only the development of cyber tools to gain access to specific systems, but also the development of capabilities to exfiltrate information resident on the system and/or, more invasively, to completely subjugate the targeted machine. This investment extends beyond the development of cyber arms; it also requires extensive testing against a mockup of the intended target for both the developer and eventual cyber operator. The combination of technical knowhow with financial resources severely limits the number of states that can be called genuine cyber powers—particularly since such investments may be long-term commitments without guaranteed successful outcomes. Indeed, some cyber operations may take years from the time the concept is conceived until the operation is implemented. Operations that involve gaining access to hardened systems that use closed networks not connected to the open Internet, such as the Stuxnet attack against Iran to delay its uranium enrichment program, are significantly costly. In the case of Stuxnet, custom-engineered cyber capabilities containing over fifteen thousand lines of code were required to manipulate Iran's customized Supervisory Control and Data Acquisition (SCADA) systems; this would certainly be costlier than a cyber attack that simply deleted information from servers to which an actor had gained access.[72] In this example, the Stuxnet attack would be significantly more costly to conduct than the 2012 Saudi Aramco breach, which destroyed data

---

[71]Julie Hirschfeld Davis, "Hacking of Government Computers Exposed 21.5 Million People," *New York Times*, 9 July 2015. David E. Sanger and Nicole Perlroth, "U.S. Said to Find North Korea Ordered Cyberattack on Sony" *New York Times*, 17 December 2014.

[72]Langner, "Stuxnet's Secret Twin." Eric Oliver, "Stuxnet: A Case Study in Cyberwarfare," in *Conflict and Cooperation in Cyberspace*. Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (July–September 2013): 365–404.

resident on over thirty thousand corporate computers, due to the time, material, and personnel requirements that would be mandated by the former compared to the later. Finally, this category of cyber attacks could require incurring the additional cost of gaining physical access to a network, particularly if it is closed, through using human operators.[73]

Operating militarily in cyberspace requires a skill set that is not uniformly distributed across all states and takes years to develop. Moreover, unlike traditional means of signaling, sending a signal via cyberspace is uniquely costly because, once an attack capability is used, it often cannot be used again. While it may be possible to replicate a capability, as already noted, there is little universality of cyber capabilities. Most critical targets are unique, and potential victims can prevent exploitation once the threat signature has been identified and incorporated into their defenses, which also compounds the difficulty of a sustained assault. Furthermore, once these tools are deployed they have a limited lifespan as routine defensive techniques and vulnerability patching may render a tool that took years to develop obsolete within seconds of employment.

Governments can also generate costly signals through manipulating the shared risk of war. This concept was championed by Schelling, who submits that credibility can be enhanced by exhibiting risky behavior, particularly during times of crisis.[74] States can demonstrate resolve through acting in a manner that increases the risk of war and/or increases political costs to the party issuing the threat, but falls short of initiating an attack. For instance, a state can raise the alert status of its forces or move naval fleets into close proximity of an area of hostiles. Neither of these signals is inherently costly; however, during a time of increased tension, such maneuvers increase the likelihood of war due to the potential misperception of intent and miscalculation. Furthermore, leaders can generate political costs through tying hands. In other words, politicians that are subjected to electoral sanctioning may generate self-imposed reputational costs by committing themselves to a course of action, which could put their political future in jeopardy if they waiver from it.[75]

In cyberspace, risk generation occurs by acting in overt ways that ensure the receiver perceives the signal, but falls short of a cyber attack. These types of actions include actively scanning networks, pinging pieces of key infrastructure, and perhaps even deploying beacons on compromised infrastructure. These operations can increase the risk of war because their intent cannot be surmised and could be interpreted as a precursory step to offensive cyber operations. However, these operations generate tradeoffs between intelligence collection and coercion strategies that policymakers should take into account.

---

[73]Owens, Dam, and Lin, eds., *Cyberattack Capabilities*, 83–89.
[74]Schelling, *Arms and Influence*, chap. 3.
[75]Fearon, "Signaling Foreign Policy Interests." For an alternative point of view, see Snyder and Borghard, "The Cost of Empty Threats."

Reassurance

Finally, to succeed, a coercive threat must have an element of reassurance, such that the target is made to believe that compliance with the terms of the threat will ensure the coercer does not mete out the threatened punishment regardless.[76] In other words, "the pain and suffering have to appear contingent on his behavior; it is not alone the threat that is effective—the threat of pain or loss if he fails to comply—but the corresponding assurance, possibly an implicit one, that he can avoid the pain or loss if he does comply."[77] Related to reassurance, Schelling also describes the importance of saving face—leaving a backdoor that enables that adversary to back down without paying too high a price in its own reputation and integrity. Coercers should therefore deliver the threat in a way that "decouple[s] an adversary's prestige and reputation from a dispute."[78]

Reassurance is also a difficult aspect of coercion. Todd S. Sechser argues that great powers encounter problems reassuring weaker states that are the targets of compellent threats because the very military capability that enhances the credibility of the stronger state's coercive threat makes it more difficult for the target to believe that the stronger state won't simply make more demands following the former's compliance with the initial threat.[79] This sheds light on the inherent tension between the actions that enhance credibility versus those that buttress reassurance; the more a target believes the coercer will actually carry out a threat (credibility), the less likely the target believes the coercer will refrain from doing so in the event she complies (reassurance). Credibility is enhanced when the coercer is forced to inflict some punishment on a target in a way that makes it difficult for the coercer to back down or renege—but the more likely it is that the target believes the coercer will use force, the more insurmountable the task of simultaneously reassuring the target that the threat will be walked back, especially if the coercer's prestige and reputation are engaged in the process of enhancing credibility. In a similar vein, reassurance can be difficult for domestic political reasons; the leader of the coercing state may worry that sending a reassuring signal to an adversary in the context of a crisis situation makes her look weak and irresolute to her domestic public.[80]

Reassurance in Cyberspace

Assuring a target state that, once it capitulates to the aggressor's demands, the punishment will cease is perhaps the greatest obstacle to successful coercion in cyberspace. Effective command and control of a cyber attack are essential for reassurance. However, this is often exceedingly difficult in cyberspace depending

---

[76]For a broader discussion of assurance strategies, see Jeffrey W. Knopf, "Varieties of Assurance," *Journal of Strategic Studies* 35, no. 3 (April 2002): 375–399.
[77]Schelling, *Arms and Influence*, 4.
[78]Ibid., 125.
[79]Sechser, "Goliath's Curse.
[80]If this is the case, it would imply that democracies may encounter greater difficulties than autocracies when it comes to reassurance.

on how and by whom an attack is carried out. For instance, 128 distinct cyber attacks were recorded against Estonian websites during May 2007 in response to the Estonian government's decision to relocate a Soviet-era war monument.[81] Since these assaults lacked a centralized controller, it would have been difficult for a unitary actor to provide the Estonian government with a credible assurance that the attacks would cease if the statue were returned to its original location (if we can assume this was the objective of the attacks). Furthermore, many states choose to employ cyber proxies to conduct cyber operations because they may not have the means to conduct the operation themselves or desire plausible deniability. Proxies may not act in the way a government desires depending on the proxy's incentives for participating in the attack and a government's ability to incentivize good behavior.[82] Furthermore, once the attack tool is released, it may be exceedingly difficult to stop. For instance, the Stuxnet computer virus was presumably never intended to propagate beyond Iranian nuclear centrifuges, but it infected over 100,000 computers worldwide before it could be stopped.[83] Due to the technical complexities of cyber capabilities and the collective action issues that may surround command and control of a cyber attack, a rational actor would be wise to second guess a reassurance that an assault will stop in exchange for submission.

A unique paradox occurs as an implication of this analysis. The ideal means to reassure a target is to engage in a disruptive cyber attack. Disruptive attacks are easily reversible and can, therefore, be credibly revoked if a target complies with a coercer's demands. However, disruptive attacks are not particularly costly and, therefore, are less credible than a destructive attack. A destructive attack can deliver an immediate effect, and it also generates irreversible costs to the target that can increase over time. Together, this implies that a coercive cyber attack that both reassures and maximizes costs for the target may be unachievable.

Assessing Warfighting Strategies in Cyberspace[84]

As the above discussion illustrates, cyber power is not an ideal independent tool of coercion. Nevertheless, governments may still choose to use cyber power to pursue warfighting strategies aimed at eroding a target's ability or willingness to resist due to the perceived ease or cost effectiveness of conducting cyber operations as opposed to conventional ones, particularly under conditions of conventional asymmetry—as well as their destructive nature in many cases.[85] In this section, we

---

[81] Andreas Schmidt, "The Estonian Cyberattacks," in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, ed. Jason Healey (Vienna, VA: Cyber Conflict Studies Association, 2013), 182.
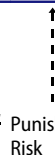
[82] For further reference, see Erica D. Borghard and Shawn W. Lonergan, "Can States Calculate the Risks of Using Cyber Proxies?" *Orbis* 60, no. 3 (Summer 2016): 395–416.

[83] Kim Zetter, "Report: Obama Ordered Stuxnet to Continue After Bug Caused It to Spread Wildly," *Wired*, 1 June 2012.

[84] For further discussion of the likely impact of cyber on strategy in general, see Joseph S. Nye, Jr., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* (Winter 2011): 18–36.

[85] Anti-Access/Area-Denial strategies currently pursed by states to thwart the movement and maneuver of conventionally superior militaries in a theater of operations typically contain a strong element of cyber power. See, for example, Erica D. Borghard and Shawn W. Lonergan, "Will Air-Sea Battle Be 'Sunk' by Cyberwarriors?" *National Interest*, 8 December 2014.

Table 1. Assessing warfighting strategies in cyberspace.[86]

	Viable	Nonviable
Effective	Attrition Denial Decapitation ← - - - -	↑ ⁝ ⁝
Ineffective	Intimidation ← -	Punishment Risk

analyze the viability and effectiveness of the six most prominent warfighting strategies that have been explored in the coercion literature and apply them to the cyber domain: attrition, denial, decapitation, intimidation, punishment, and risk. In particular, we discuss the extent to which these strategies are viable based on the current state of the field, as well as the extent to which they can generate sufficient costs to be theoretically effective.[87] We define viability in terms of whether the strategy is technically feasible based on known, existing capabilities.[88] We define effectiveness in terms of whether the strategy can generate sufficient costs to change state behavior. This is conditional on several things: on the target side, whether a target's systems are vulnerable, whether the systems themselves have resiliency, and whether the target as a whole has resiliency beyond the affected system(s) (that is, how dependent the target is on a particular set of cyber-enabled services or capabilities); and on the coercer's side, how costly the attack is to conduct in material, personnel, and political terms. Together, two dimensions of viability and effectiveness form a 2×2 matrix according to which the six strategies can be assessed, as depicted in Table 1.

Viable and Effective Strategies

Currently, we argue that there are three warfighting strategies that are likely to succeed using cyber power: attrition, denial, and decapitation. We claim that governments are most likely to achieve desired objectives using these strategies because the technical requirements and capabilities for carrying out these operations in cyberspace exist and because they can generate sufficient costs (in theory) to force a target government to concede. However, it is imperative to note that this discussion remains theoretical and its efficacy in practice is highly context dependent—whether a given government will concede to the demands of a coercing state will depend on the particular cost–benefit calculus it makes for a specific situation. While attrition, denial, and decapitation have different logics, what unites them is their discrete military application—these strategies are generally employed against military targets—and they are most likely to be successful when coupled with

---

[86]As is the case with conventional coercion, these capabilities may vary tremendously across states. In fact, this is especially likely in an emergent domain.
[87]Given the relative newness of these strategies, much of this discussion remains theoretical rather than applied.
[88]Of course, this is liable to change as the state of technology changes.

conventional military operations and/or diplomacy. In other words, the use of cyber power to undermine a government's ability or willingness to resist is not as effective in isolation from other instruments of state power.

Attrition

Attrition strategies seek to erode the adversary's military capability such that the target can no longer resist. Within the cyber domain, this strategy could include attacks that both degrade and destroy government or private networks and systems, depending on the latter's military utility. In cyberspace, the successful application of an attrition strategy would force a target to abandon a network or system through destroying it or building up a user's mistrust in it such that the target is forced to abandon its operation. A notable attribute of attrition strategies is that they seek to exhaust a target state's resources as it is forced to dedicate assets to protect or replicate capabilities in different and more secure manners. In particular, cyber raiding—targeting an enemy in its weakest areas—is a common tactic of attrition, where data is the equivalent of an enemy's provisions. Conventionally, raiding refers to stealing or destroying an enemy's provisions or equipment. These forays are commonly conducted behind an adversary's lines and are directed against their supply convoys and depots. In cyberspace, destroying or corrupting servers that handle military plans, air or ship tasking orders, or even defense developmental efforts, can prevent certain actions from occurring at the time they are urgently needed. More importantly, if they persist they will eventually erode a state's confidence in its networks and the data resident on them. It is difficult, if not impossible, to destroy a state's militarily capabilities through the exercise of cyber power alone. However, it is theoretically possible to force a state to suffer the gradual erosion of its capabilities—especially of its confidence in them—as vulnerable targets are attacked and as governments are forced to divert considerable resources to investigating and repairing them until the cost of continued resistance becomes unbearable.

Denial

A denial strategy involves increasing the costs to an adversary such that achieving a military objective—such as taking a piece of territory—becomes prohibitive or impossible.[89] As such, it could involve both a defensive component (increasing one's own defenses such that an adversary cannot go on the offense without incurring significant costs), as well as an offensive one (actively taking out enemy capabilities to deny the adversary the ability to achieve an objective).[90] In cyberspace, the targets of denial strategies mirror those of traditional domains of warfare, except that the effect achieved is delivered via a cyber operation. An adversary's

---

[89]Robert Pape defines coercion by denial as "using military means to prevent the target from attaining its political objectives or territorial goals." *Bombing to Win*, 13.
[90]Byman and Waxman, *Dynamics of Coercion*, 78–82.

Integrated Air Defense Systems (IADS), command and control apparatuses, and air traffic control systems are all examples of legitimate targets for a state pursuing a denial strategy. An example of using cyber means (coupled, in this case, with conventional military power) to target an adversary's air defense systems is the alleged 2007 Israeli air attack against Syria's nuclear facilities.[91] Unlike conventional approaches to denial, in cyberspace, due to the increasing reliance of embedded technology in many modern battlefield systems, the surface from which these systems can be attacked has significantly increased. For instance, in conventional warfare the only way to remove tanks from a battlefield is to destroy them piecemeal from the air or ground. However, theoretically, it may be possible in the not too distant future (if not already) to use a cyber attack to render entire fleets of weapon systems inert at a critical moment. This concern has already been realized by many policymakers and is evident in the discussion over Chinese cyber espionage of the research and development of the Joint Strike Fighter.[92] On the other hand, the length of the timeframe under consideration could affect assessments of the potential costliness of denial strategies in cyberspace. For instance, cyber instruments could be used to disable, rather than destroy, an adversary's weapons systems or command and control, rendering an attack costly in the short term but less costly than the ostensibly permanent destruction of those systems through conventional means.[93]

Decapitation

Decapitation strategies seek to achieve strategic paralysis by targeting command and control centers, leadership, critical economic nodes, and key weapons systems.[94] Currently, it is technically possible to use cyber attacks to shut down a command and control node. However, given that most states employ secondary and tertiary redundant systems (for example, analogue or even courier-based communication), as well as separate communication networks (for example, multiple classified and unclassified networks), the impact of this type of operation could be short lived. Nevertheless, successfully targeting a critical command and control node, such as the US government's Secure Internet Protocol Router Network (SIPRNET) or Joint Worldwide Intelligence Communications System (JWICS), would have immediate and significant material and psychological effects. Therefore, governments should either take into account temporal limitations when targeting command and control networks, or ensure that they also target all additional means of adversary communication. Conventional military operations that target command and control facilities can wipe out entire communications networks, for example, through dropping ordnance on a facility. In contrast, cyber

---

[91]Clarke and Knake, *Cyber War*, 1–8.
[92]David E. Sanger, "With Spy Charges, U.S. Draws a Line That Few Others Recognize," *New York Times*, 19 May 2014.
[93]The authors are grateful to Robert Jervis for pointing this out.
[94]Pape, *Bombing to Win*, 79.

operations can typically target a single or limited number of communications nodes or networks due to the compartmentalized nature of each network. This would therefore require multiple distinct cyber operations to achieve near-complete command and control paralysis. Furthermore, even if cyber attacks could be used to successfully target a government's primary communications networks, backup systems would likely need to be defeated through traditional forms of electronic warfare or conventional operations (for example, jamming transmissions, capturing curriers, or cutting telephone lines or undersea cables). Altogether, this analysis implies that one is more likely to observe decapitation strategies employed at lower echelons of command, such as troops in the field, where there are typically fewer redundant systems, or against less-capable state adversaries.

Viable and Ineffective Strategies

Warfighting strategies in cyberspace can be technically viable but ineffective because they cannot force the adversary to incur sufficiently high costs to prompt a change in her behavior. Much of the activity that currently occurs in cyberspace falls into this category—actors can harass, annoy, or otherwise inconvenience each other. Indeed, those who claim that the threat of a cyber Armageddon is exaggerated focus on these kinds of cyber attacks.[95]

Intimidation

An intimidation strategy is designed to directly address a state's domestic audiences and sometimes, national policymakers. Actions as part of an intimidation strategy do not cause significant damage and are typically tailored to undermine a government's legitimacy or convince domestic audiences that the government is powerless, prompting a loss of confidence by the public.[96] In cyberspace, intimidation typically takes the form of website defacement and email spamming campaigns. While these operations are technically easy to conduct because they involve fewer resources and a lower skill set compared to other types of operations, they cause minimal cost to the recipient. The effect these attacks produce is typically perceived as an annoyance, rather than a strategic message, because these types of attacks are fairly common and easy from which to recover. Therefore, they are unlikely to be sufficiently costly to force targeted governments to change their behavior. Indeed, observed intimidation strategies, such as the 2008 defacements of Georgian government websites portraying President Mikheil Saakashvili as Adolf Hitler, have had no real effect.[97]

---

[95]Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013), xiv–xv.

[96]Andrew H. Kydd, and Barbara F. Walter, "The Strategies of Terrorism," *International Security* 31, no. 1 (Summer 2006): 66.

[97]Jeffrey Carr, *Inside Cyber Warfare*, 2nd ed. (Sebastopol, CA: O'Reilly, 2012), 183–84. Andreas Hagen, "The Russo-Georgian War 2008," *A Fierce Domain*, ed. Healy. Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete–Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," *Security Dialogue* 43, no. 1 (February 2012): 3–24.

Nonviable and Ineffective Strategies

The two paradigmatic strategies of traditional coercion that currently have the least utility in cyberspace are punishment and risk. While there has been considerable brou-haha in public and even government spheres regarding the potentially dire consequences of a "World War 3.0" or a "cyber Pearl Harbor," these are largely unrealistic given the current state of the domain.[98] However, as we will describe below, changes in modern societies' interconnectivity and reliance on automated systems, as well as advances in military cyber technologies, could change the value of these strategies.[99]

Punishment

Originally stemming from the work of Giulio Douhet, an Italian general and early proponent of the strategic use of air power, punishment strategies are designed to inflict sudden, large-sale pain and devastation on an adversary's civilian population until the panic-stricken citizenry demands an end to the war.[100] Indeed, Douhet envisioned that a single successful air raid on an enemy's population center could" … spread terror through the nation and quickly break down [a state's] material and moral resistance."[101] This concept was further refined by Schelling and modern coercion theorists, who applied it to the strategic use of nuclear weapons; holding an adversary's population at risk of extreme destruction is the foundation of modern deterrence theory.[102]

In theory, inflicting punishment in cyberspace would involve the use of cyber power to cause virtual and physical damage to civilian infrastructure and population centers. This could entail attacks against essential services, such as water treatment facilities, transportation, air traffic control systems, nuclear power plants, electrical grids, food safety systems, waste management systems, etc. However, in practice, there are two critical elements of punishment that cannot be sustained given the current nature of the cyber domain: first, the immediate and sudden nature of an attack; and second, the scale and scope of the pain. Put simply, governments cannot kill a lot of people in a very short period of time using cyber weapons; the magnitude of the pain states are currently capable of inflicting via the cyber domain alone is hardly comparable to the devastation wrought by conventional or nuclear attacks against cities. Access requirements and the customized nature of cyber capabilities render it nearly impossible to launch a time-dependent, highly coordinated cyber campaign of the scale required to inflict severe costs on enemy populations. The scope is also nearly impossible to achieve because it would require an extraordinarily

---

[98]See Michael Joseph Gross, "World War 3.0," *Vanity Fair*, 30 March 2012; Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall 2013): 41–73.

[99]The utility of punishment or risk strategies in general is beyond the scope of this discussion.

[100]Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (New York: Coward-McCann, 1942), 57–58.

[101]Ibid., 57.

[102]Beyond Schelling, see, for instance, Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills, CA: Sage Publications, 1977); Robert Powell, *Nuclear Deterrence Theory: The Search for Credibility* (Cambridge: Cambridge University Press, 1990); Kahn, *On Thermonuclear War*.

large number of discrete and distinct cyber attacks. As discussed in prior sections, there is limited universal lethality of cyber weapons, which means that governments would have to develop unique accesses and distinct tools for each targeted system. Moreover, there is no guarantee that an effect can be delivered as planned. Additionally, it is difficult to envision a government entity being able to sustain a cyber assault against multiple key pieces of infrastructure in order to push a society to a breaking point before the target moves to mitigate the onslaught through preestablished redundant mechanisms and/or cyber or kinetic military operations.

Manipulation of Risk

Punishment and risk are fundamentally related—both involve targeting an adversary's population centers to force the government to concede to the coercer's demands. However, unlike punishment strategies that call for immediate and decisive destruction, risk strategies entail gradually escalating the intensity and scope of attacks against civilian targets.[103] There is a critical psychological element to the manipulation of risk in that what drives concessions is the threat and prospect of future pain. This requires that the coercing state can sustain and ratchet up an assault over time.

Like punishment, the manipulation of risk does not translate well into cyberspace. Carrying out a comprehensive, tiered cyber campaign plan to create the ratcheting effect of punishment that Schelling proscribes is exceedingly difficult for reasons already articulated. To wit, this would require a significant planning effort and mandate a costly access and capability development program. Furthermore, risk strategies do not rely upon the sudden and intense destruction that are envisioned by punishment strategies, but instead are designed to be employed over time. In order to be effective, the attack would have to be maintained against an adversary that would likely be active in trying to stop or mitigate the effects of the onslaught. Presumably, if a state is at the technical level where it is susceptible to large-scale cyber attacks, it also has the wherewithal to defend against them over time. Finally, the effective employment of a risk strategy in cyberspace would require an impossibly high level of control by the coercing government over the cyber tools it would employ against an adversary. According to Schelling, risk is most likely to succeed when an action, "once initiated, causes minimal harm if compliance is forthcoming and great harm if compliance is not forthcoming, is consistent with the time schedule of feasible compliance, is beyond recall once initiated, and cannot be stopped by the party that started it but *automatically* stops upon compliance, with all this fully understood by the adversary."[104] Indeed, the risks of using cyber power—effects getting beyond the control of the initiating state in unanticipated and potentially undesirable ways—are precisely the opposite of the calibrated manipulation of risk Schelling envisions.

---

[103]Schelling, *Arms and Influence*, 3. Also see Pape's discussion of manipulation of risk in *Bombing to Win*, 66–69.
[104]Schelling, *Arms and Influence*, 89. Italics in the original.

Future Trends in Viability and Effectiveness

The negligible utility of punishment and risk strategies rests on the current state of technology and the dependence (and, therefore, vulnerability) of modern societies on cyber-enabled essential services. Changes along either of these dimensions—technical viability and/or the costs that can be imposed on civilian populations—would alter the feasibility and effectiveness of these strategies. For instance, the dawn of the "Internet of Things" (a concept that depicts a not-too-distant future where everything from an individual's toaster and refrigerator to a city's garbage collection and other essential services are automated and connected to the Internet) could make it possible for governments to impose high and devastating costs on society through cyber means.[105] Moreover, it is conceivable that, as societies remove human redundancy through increased automation and become more dependent on interconnected networks of services, punishment and risk strategies could become more effective as the attack surface expands and more targets become vulnerable to a cyber attack.

Additionally, punishment and risk strategies could become more viable due to better investment in human capital, decreasing costs of planning and conducting large-scale cyber campaigns, increased government spending on developing cyber capabilities, and gaining and maintaining accesses to potential target sets, and the unknown unknowns of potentially disruptive technological innovations that make these attacks easier.

Strategic Implications of the Coercive Use of Cyber Power

This analysis explores the applicability of traditional theories of coercion to the cyber domain. We identify four key elements of coercion—communication, cost–benefit calculus, credibility, and reassurance—and assess how each manifests itself in cyberspace. We then analyze the utility of various warfighting strategies that seek to undermine an adversary's ability and/or willingness to resist and find that, based on the current state of the field, only three—attrition, denial, and decapitation—are likely to be useful for aspiring coercers in cyberspace. However, even these strategies are most useful in conjunction with conventional instruments of power and/or diplomacy; cyber power is rarely, if ever, independently decisive. For policymakers, this suggests that, especially if a coercing state has an asymmetrical advantage in other elements of national power, using cyber power to enable espionage, sabotage, and other shaping operations to support a cross-domain coercive strategy may be a more effective use of cyber capabilities than employing it as an independent instrument of state power.

This framework also highlights the importance of indices and developing an understanding of another state's intentions in cyberspace due to the high risk of misperception, which can lead to unintended outcomes and inadvertent escalation.

---

[105]Jayavardhana Gubbi et al., "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems* 29, no. 4 (September 2013): 1645–60.

A policy implication of this is that states should focus intelligence-collection efforts on developing an advanced understanding of the cyber capabilities and aspirations of potential adversaries. In addition to indices, states may also send signals through the use of cyber attacks. However, since neither of these signaling mechanisms is inherently clear, the most likely way to convey the intent behind an action in cyberspace is to ensure attribution and couple the event with a diplomatic message or place it within the context of a conventional military operation. Furthermore, for cyber power to be an effective coercive tool, the target needs to believe that an attack will cease once she complies with the coercer's demands. This would require assurances that would have to come via established means that often do not yet exist. Providing a credible reassurance is difficult because many types of cyber attacks, such as DDoS attacks, can come from numerous users and make it difficult for the threatening state to credibly demonstrate it exerts control over a decentralized network of attackers. This leads to a paradox in which the type of cyber attack that is most likely to aid in reassuring a victim may also not be able to generate the punishment that would be necessary for capitulation.

Cyber power can be used as a coercive instrument of state power but, once the theory of coercion meets the reality of cyber operations, many attractive targets may become too costly and out of reach for a state to attack in a timely manner. Therefore, governments are more likely to pursue coercive strategies that allow for a wide variety of targets that are more easily accessible than hardened critical infrastructure. In other words, long development timelines and access constraints often mean that policymakers cannot attack their ideal target(s) in a timely manner and, therefore, are more likely to pursue warfighting strategies that do not necessitate sudden and intense devastation but, rather, inflict costs against vulnerable public and private interests. Given current levels of dependency on technology, this type of attack would provide damaging, but limited, effects. This has unique and potentially troubling implications. Since the end of the Second World War, many states have sought to limit their coercive attacks to key pieces of government and military infrastructure out of ethical and legal concerns surrounding targeting civilian infrastructure (and due to the domestic and international political costs of doing so). However, given that in cyberspace much of the vulnerable infrastructure is owned by private industry, policymakers may reevaluate norms against targeting these systems as they pursue attrition, denial, or decapitation strategies. Cyber warfighting strategies that intentionally target civilian infrastructure, such as punishment and risk, are currently nonviable and ineffective. However, as technology evolves and the Internet of Things makes societies both more interconnected and vulnerable, states may find strategies that explicitly aim to wreak havoc on civilian populations more effective. Together, this suggests that, at the domestic level, governments should strive to continue to build resiliency into civilian networks and, at the international level, norms governing appropriate targeting in the cyber domain are urgently needed.

Acknowledgments

Funding