Cybersecurity and Cross-Domain Deterrence: The Consequences of Complexity

Jon Lindsay
University of Toronto
jon.lindsay@utoronto.ca

Erik Gartzke
University of California San Diego
egartzke@ucsd.edu

18 August 2016

In Damien T. Van Puyvelde and Aaron Brantley, eds., *National Security in Cyberspace* (Routledge, forthcoming)
[final copyedited text may differ] [1]

The authors wish to thank Damien Van Puyvelde, Tim Ridout, and Joshua Rovner for helpful comments.

Introduction

Cross-domain deterrence (CDD) is the use of threats of one type to discourage behavior of another type, for example promising economic sanctions or a military strike in response to a cyber attack. Increasing societal dependence on computing infrastructure, together with confusion about how to respond to serious cyber attacks, had prompted policymakers to look beyond cyberspace for tools to disarm or deter attackers. The May 2011 White House *International Strategy for Cyberspace* thus declared, "We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order

[1] Authors' Note:

to defend our Nation, our allies, our partners, and our interests." At the same time, cyberspace has expanded the palette of options threat actors can use to work around the deterrence policies of their adversaries. The United States used Stuxnet to attempt to disrupt Iran's nuclear program without starting a war, and Russia sought to influence the course of the 2016 U.S. presidential election without provoking an explicit confrontation. Computing networks, moreover, are increasingly essential for the command and control of military capabilities used for deterrence or defense on land, at sea, in the air, or in outer space; the security of the cyber domain thus affects all other domains.

Yet deterrence is only one aspect of cybersecurity. Indeed, many experts are skeptical of cyber deterrence and thus favor reliance on denial and resilience for network defense.[2] Similarly, not every use of deterrence relies on different means. Modern deterrence theory itself was built around the within-domain challenge of using nuclear weapons to prevent nuclear war.[3] Offensive and defensive cyber operations may play out completely within cyberspace, while CDD can deal with threats and responses beyond the cyber domain, exhibiting little operational interaction with the virtual world. Whereas cybersecurity is a relatively recent problem resulting from decades of economic and technological innovation, CDD has been practiced for millennia wherever actors have leveraged a diverse set of available strategic options, for instance relying on command of the

[2] Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Forces Quarterly*, 2015; David Elliott, "Deterring Strategic Cyberattack," *IEEE Security & Privacy*, 2011; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009); Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press, 2015). Cf., Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyber Attack," *Journal of Cybersecurity* 1, no. 1 (2015): 53–67.

[3] Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca: Cornell University Press, 1989); Lawrence Freedman, "The First Two Generations of Nuclear Strategists," in *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*, ed. Peter Paret (New York: Oxford, 1986), 735–78.

sea to deter land invasion. Thus, CDD occupies a niche in the broader cybersecurity policy debate, and cyberspace is one domain among many in a broader deterrence calculus.

Nevertheless, cybersecurity and CDD are closely entwined as defense policy issues. Cyberspace, a human-built information and control infrastructure, is not valuable just for its own sake but rather because it enables firms and governments to expand their control over commercial and political activities. The cyber domain is inherently cross-domain. Some aspects of cyberspace relative to traditional military operating environments, such as low barriers to entry, the secrecy of capabilities, and the attribution problem, appear to pose serious challenges for deterrence policy. Although the practice of CDD is nothing new, and may be as old as deterrence itself, cybersecurity catalyzed the concept of CDD as an explicit concern in the U.S. national security community. The vulnerability of industrial control systems and military command and control networks and their dependence on technology largely invented, owned, and operated by the private sector posed serious challenges to traditional notions of deterrence that assumed attacks would be easily attributed to nation states.

More fundamentally, CDD and cybersecurity are closely entwined theoretically. Both are symptomatic of increasing sociotechnical complexity in the modern world and the information problems created by greater diversity of actors, capabilities, and linkages between them. Cyberspace is literally built out of information technology, and cyber attacks rely on stealth and deception. Cybersecurity thus becomes a race between attackers exploiting pervasive information asymmetries and defenders patching the informational inefficiencies in cyberspace.[4] Deterrence is also an information problem as defenders seek to generate credible signals of resolve and intent

[4] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–48.

for challengers. The evolution of CDD is, likewise, a race between an expanding portfolio of means available to inflict harm on others, which tends to increase dangerous uncertainty, and the adaptation of policy to restore some clarity and credibility in coercive communication. Cybersecurity and CDD, conceptually separable though they may be, both directly confront with the information problems inherent in conflict, and in practice they both generate additional information problems that exacerbate conflict.

Modern computing systems, too complex to understand in formal detail, are rife with uncertainty. Policymakers also confront great uncertainty in trying to deter ambiguous threats posed by new technologies and actors. The rationalist bargaining theory of war, a workhorse in the field of security studies, highlights uncertainty and commitment problems as major causes of conflict.[5] Uncertainty emerges from objective complexity in the world, imperfections in subjective assessments, and deliberate secrecy and misrepresentation. The bargaining model of war can help to understand how the uncertainty inherent in cybersecurity and CDD affects conflict, but the implications are neither straightforward nor determined by technology alone. Explicit focus on the bargaining implications of increasing complexity, moreover, holds promise for both the development of deterrence theory and an improved understanding of cybersecurity.

The coevolution of cybersecurity and CDD

Deterrence is an ancient phenomenon. Many animals produce dramatic threat displays to warn away competitors, and some prey animals mimic the patterning of poisonous species to fool predators. Threats to invade and conquer are commonplace in human history, but so is war itself

[5] James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (1995): 379–414; Robert Powell, *In the Shadow of Power: States and Strategies in International Politics* (Princeton, NJ: Princeton University Press, 1999); Charles L. Glaser, *Rational Theory of International Politics: The Logic of Competition and Cooperation* (Princeton, NJ: Princeton University Press, 2010).

because threats are often miscommunicated or doubted. The nuclear revolution brought deterrence to the forefront of strategy because, as Bernard Brodie stressed, the horrendous cost of nuclear war for the first time exceeded any conceivable benefit of victory.[6] As defense against large numbers of ballistic missiles from hidden or inaccessible launch points appeared futile or prohibitively expensive, deterrence appeared to be the only option for preventing Armageddon. The strategy of deterrence had always been available, but now it had to be explicitly conceptualized to guide defense policy. The point is worth stressing: innovation in a particular technological means forced a conceptual reconsideration of the strategic difference between deterrence and defense, or in Thomas Schelling's terms, between contests of resolve and contests of strength.[7] Both strategies have always existed and have usually intermingled, but nuclear weapons led strategists to bring to the forefront the logic of deterrence in an effort to ensure that they were never used.[8]

Cross-domain deterrence follows a similar evolution. Policymakers and commanders have always employed a diversity of means to pursue their ends and to work around the strategies of their opponents, but they didn't need a special term to describe what they were doing. Sparta tried to deter Athens with its formidable army while Athens tried to deter Sparta with its unequaled navy; deterrence failed to prevent a war but, ironically, succeeded in prolonging it.[9] The British Royal Navy has long posed a powerful deterrent to invasion by superior continental armies. In 1940 Germany responded with an air campaign intended to defeat the Royal Air Force in order to expose the Royal Navy, but superior defense in the Battle of Britain convinced Germany to

[6] Bernard Brodie et al., *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace and Co., 1946).
[7] Thomas C. Schelling, *Arms and Influence: With a New Preface and Afterword* (New Haven, CT: Yale University Press, 2008).
[8] Shannon Carcelli and Erik Gartzke, "Blast from the Past: Revitalizing and Diversifying Deterrence Theory," Working Paper (La Jolla, CA, March 24, 2016).
[9] Joshua Rovner, "New Concepts for Ancient Wars: Cross-Domain Deterrence in the Peloponnesian War," in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, edited by Erik Gartzke and Jon R. Lindsay,(forthcoming).

abandon its invasion plans.[10] Germany later turned to the undersea domain to design around the Royal Navy and enjoyed some success until the Allies managed to cobble together a viable system of intelligence collection and anti-submarine warfare. Each side played a form of 'rock, paper, scissors' to coerce in one domain or work around coercion in another. Likewise during the Cold War, NATO and the Soviet Union fielded sophisticated nuclear and conventional capabilities on land, in the skies, on and under the sea, and in orbit around the Earth, as well as irregular proxy forces. The complicated set of options in the Cold War strategic portfolio enabled states to think the unthinkable, to continue to compete over practical geopolitical objectives in the shadow of nuclear conflagration. Historically states have also used nonmilitary means, such as economic sanctions and immigration policy, to attempt to shape the target's behavior in the security realm. Where even conventional military conflict was deemed prohibitively costly or risky—and thus mutual deterrence existed—adversaries shifted their threats or actions to domains where aggression could more safely be contemplated. There seems to be no upper bound on the evolving heterogeneity of coercive tools and methods.

Whereas innovation in a single technology—nuclear weapons—raised the problem of deterrence to the fore, innovation across a range of technologies makes CDD an explicitly pressing problem. There has always been diversity in the methods for inflicting harm, but the entire portfolio has never been so extensive, and thus complex. The proliferation of dual-use threat technologies (e.g., largescale data networks, automated robotics, additive manufacturing, synthetic biology, and the list goes on), their interaction in the global economy, and their use across bureaucratic jurisdictions pose a series of challenges for deterrence. Who is the target if attribution is uncertain? What is the cost of punishment if a capability is untested? What is a credible signal

[10] Jon R. Lindsay, *Shifting the Fog of War: Information Technology and the Politics of Control* (forthcoming), ch 4.

if the means of punishment must be kept secret? Yet one technology looms above others for contemporary CDD, precisely because it increasingly connects and controls all other technologies. Information technology is vital for nearly all engineering and administrative functions in the 21st century globalized environment and thus offers a vector for potential influence over any other type of capability or activity. The ambiguity and accessibility of cyber weapons thus appears, some would argue, to undermine deterrence as surely as nuclear weapons undermined defense.

Throughout the 2000s, the U.S. government became increasingly worried about the threats (and opportunities) of ubiquitous cyberspace. The internet catalyzed economic growth but also connected together systems that had never been designed with network security in mind. Russia's service denial attacks in Estonia in 2007 and Georgia in 2008 demonstrated that governments or 'patriotic hackers' might use the internet to inflict costs on the civilian economy or support a military invasion.[11] The Stuxnet attack on Iranian nuclear enrichment infrastructure, inadvertently revealed in late 2010, demonstrated that cyber-physical disruption was not just science fiction.[12] Chinese military modernization throughout the decade stressed the pursuit of "informatization," loosely modeled on U.S. network-centric warfare with particular emphasis on the use of cyber attack as a rapid, long-range, low-cost, high-impact countermeasure against American power projection.[13] Wide-ranging Chinese espionage against government, commercial, and civil society targets during the same period underlined the scope and severity of the emerging cyber threat. A number of reorganizations of cyber authorities within the U.S. Department of Defense culminated in the May 2010 launch of U.S. Cyber Command (CYBERCOM), collocated with the National

[11] Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Washington, DC: Cyber Conflict Studies Association, 2013).
[12] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365–404.
[13] Kevin Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S Reveron (New York: Oxford University Press, 2015).

Security Agency and commanded by its director, as a sub-unified Command under U.S. Strategic Command (STRATCOM). After years of terminological debate the DoD formally recognized cyberspace as a manmade 'domain' of military operations alongside the traditional physical domains of land, sea, air, and outer space.[14]

Space assets and cyber networks together form a global information infrastructure that is vital for U.S. economic and military performance. Notably, almost all of the important services provided by satellites in orbit are informational in nature (i.e., intelligence collection, communications, early warning, timing and navigation, etc.), and control of satellites is utterly dependent on electronic datalinks. Loss or degradation of critical space-based capabilities could imperil American ability to project power or even to secure domestic facilities and infrastructure. While China was by no means the first to develop space weapons (both superpowers experimented with them in the Cold War), the vulnerability of space infrastructure was dramatically demonstrated in 2007 by the Chinese test of a direct ascent antisatellite weapon that created a large debris cloud in low earth orbit.[15] The space and cyber warfare ambitions (if not yet capabilities) of China in particular were perceived by U.S. officials as key pillars in an 'anti-access, area-denial' (A2/AD) strategy, which also included an emerging arsenal of capabilities in other domains, including land based ballistic missiles, fast naval patrol craft, and advanced fighters, all aimed at contesting American 'command of the commons.'[16]

[14] William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, 2010.
[15] In addition to exoatmospheric nuclear tests in the early Cold War, the Soviet Union tested ASAT weapons in the 1970s and 80s, and the United States tested an ASAT weapon in 1985 (ASM-135) and demonstrated a capability again in 2008 with an unconventional use of a RIM-161 Standard Mk 3.
[16] Evan Braden Montgomery, "Contested Primacy in the Western Pacific," *International Security* 38, no. 4 (April 1, 2014): 115–49, doi:10.1162/ISEC_a_00160.

Upon taking office the Obama administration reorganized the Office of the Secretary of Defense, establishing the Assistant Secretary of Defense for Global Strategic Affairs (ASD-GSA) to consolidate policy for nuclear forces, ballistic missile defense, space, and cyberspace. The combination of these diverse activities under one tent suggested that space and cyber threats were seen to pose strategic problems on par with nuclear weapons. Unsurprisingly, the term CDD appears to have emerged around this same time within STRATCOM, an agency historically focused on existential threats. Yet the impetus for change was not only functional but also regional. The ability of the U.S. to deter Chinese aggression in the East or South China Seas appeared to be systematically eroding as A2/AD capabilities improved and China engaged in provocative actions well below the threshold of U.S. military retaliation (e.g., aggressive merchant vessel maneuvers, island reclamation, and cyber campaigns). Space and cyber warfare thus seemed to pose immediate threats to the freedom of U.S. military operations, while relentless human and cyber espionage posed a long term competitive threat. While China continues to exhibit difficulties in the absorption of certain types of military innovation, the illicit transfer of sensitive technology promises to enhance PRC capabilities in every domain. Russia and Iran posed different but related difficulties as they mobilized tailored capabilities in different domains to undermine various aspects of the U.S. deterrent posture. The proliferation of novel capabilities to terrorist and other seemingly non-deterrable non-state actors was another variation on the theme.[17]

[17] Madelyn R. Creedon, "Space and Cyber: Shared Challenges, Shared Opportunities," *Strategic Studies Quarterly*, no. Spring (2012): 3–8; James A. Lewis, "Cross-Domain Deterrence and Credible Threats" (Washington, DC: Center for Strategic and International Studies, July 2010); Shawn Brimley, "Promoting Security in Common Domains," *The Washington Quarterly* 33, no. 3 (July 1, 2010): 119–32; Vincent Manzo, "Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?," Strategic Forum (Washington, DC: Institute for National Strategic Studies, National Defense University, December 2011). It is not clear that terrorists and others are as often non-deterreable as presumed. The basic problem with the call to action in response to "non-deterrable" terrorists is that kinetic or other responses, if successful, should themselves generate deterrence. The problem may more accurately be described as uncertainty about the true cost or effectiveness of counter-terrorist actions.

ASD-GSA convened a 'Cross-Domain Deterrence Initiative' (CDDI) working group in 2010 to discuss these issues. The CDDI invited senior academic scholars and industry experts specializing in deterrence strategy and particular regional and technological threats to the Pentagon and provided them with classified briefings on alarming developments in each area. Ensuing discussion in the CDDI highlighted a number of serious challenges to implementing effective deterrence policy. Foremost was the uncertainty inherent in the use of complex technologies, let alone subtle combinations of them, in a signaling role across domains and across cultures. Without an observable history of use or common norms regarding the intent, appropriateness, and proportionality of moves with novel capabilities, the attempt of one side to deescalate could trigger preemption from an adversary. Cyberspace (including its space-based infrastructure) loomed large in the discussion because of its global reach, low barriers to entry, and pervasive ambiguity about the extent and intention of an intrusion (the same methods support intelligence collection and infrastructure disruption) and the identity of the responsible actor (who might even be a non-state entity). How is it possible to deter attacks that have no return address? Conversely, how is it possible to credibly threaten military retaliation for cyber attacks that turn out to be mere nuisances? How should government declaratory policy protect civilian technology it does not control without distorting competition and responsible risk taking in markets that brought that technology into being? Does complexity itself doom deterrence?[18]

[18] Michael Nacht, et al., "Cross Domain Deterrence in American Foreign Policy," in *Cross-Domain Deterrence: Strategy in an era of Complexity* (forthcoming). See also "A New Look at the 21st Century Cross- Domain Deterrence Initiative: Summary of a Workshop, May 19-20, 2016 At The George Washington University," (La Jolla, 16 September 2016), http://deterrence.ucsd.edu/_files/CDDI2-Workshop-Summary-080916.pdf

Deterrence by other means

The answer is no, or at least, not always. The same complexity that creates the impetus to pursue deterrence across domains also provides an opportunity to revisit the assumptions of deterrence theory. Success in policy and conflict is not about an ideal of perfection, but of relative capabilities, foresight or acumen. Complexity, faced by adversaries on both sides, can be an advantage to the faction that is most skilled in addressing and exploiting its challenges. In an increasingly complex world, victory goes not to the bold *per se*, but to the better informed.

Moreover, complexity in strategic affairs is, counterintuitively, a reaction to the efficacy of deterrence. When deterrence works in one respect a challenger has incentives to 'design around' the barrier in another.[19] As a nation, American security problems seem terribly difficult today because we have the luxury of attending to them, confident that the bigger problems of yesterday are under control. Urban terrorism and ubiquitous surveillance are 'first world problems' that become salient when a society's existential concerns are attenuated, the risk of major power war receding in probability. In some situations, however, the risk of serious war may increase when technology creates new `moves' that are not countenanced under an existing declaratory policy, forcing policymakers to improvise and, potentially, to miscalculate. Consternation about the potential for deterrence failure as a result of complexity usually reflects a desire to extend the success of deterrence to cover new provocations in the "gray zone," not the categorical failure of deterrence.

With apologies to Raymond Carver we must ask, what do we talk about when we talk about deterrence? Several things, it turns out. Intuitively, deterrence uses the threat of some future

[19] Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (Columbia University Press, 1974), 399.

penalty to dissuade an opponent from acting to realize a benefit—"don't come any closer or I'll shoot." Deterrence is often contrasted with compellence, which uses threats to persuade an opponent to act in ways it otherwise would not—"give me your wallet or I'll shoot." The distinction is often muddied in practice, as when an offensive action to compel change includes measures to deter preemption—"stay back and toss over your wallet or I'll shoot." China may view A2/AD as a means of deterring U.S. intervention in its local or even internal affairs (i.e. Taiwan), while the United States may view the same action as a means of compelling America to accept a Chinese fait accompli intended to revise the status quo. For tactical, normative or psychological reasons, actors tend to represent their intentions as defensive even when they are acting aggressively. The difference between deterrence and compellence may thus be in the eye of the beholder. Both forms of coercion, in Schelling's formulation, rely on credible communication about "the power to hurt" in the future rather than "brute force" in the present.[20] One of the key challenges of CDD turns on ambiguity about the credibility of such threats—the magnitude of potential harm, the meaning of force—and on a blurring of the distinction between threatening in the future and using force in the present. A second challenge has to do with the complexity of threats or actions in a world posing an increasing number of options. The actors themselves may not know what they plan to do in response to aggressive measures by an adversary. Actors cannot threaten credibly if they do not yet understand their own options or intentions. Nevertheless, we can make some analytical progress by disaggregating the capabilities that affect disparate dimensions of deterrence.

The U.S. military defines deterrence as "The prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the

[20] Schelling, *Arms and Influence*.

perceived benefits."[21] There are several different ideas at work in this definition. Deterrence is about "prevention of action" or preserving one's favored distribution of benefits, the status quo. The parts about "credible threat" and "belief" point to the mind of the target, who must decide if a given threat (a signal implied or articulated) is really expositive of the defender's intent, or just a bluff. Finally the target must decide that "the cost of action outweighs the perceived benefits." The definition is ambiguous about whether costs result from "unacceptable counteraction" or some other source, such as the target's private concerns about blowback, collateral damage, or mission failure that might produce 'self-deterrence.' The other side of the cost equation—the defender's costs for carrying through on the threat—is not explicit in the Pentagon definition, but the usual assumption is that successful deterrence without a fight is preferable to failed deterrence with a fight. Threatening to fight is usually cheaper than fighting, which is of course why deterrence poses a credibility problem; anyone can make 'cheap talk.' It is, however, possible that an actor might, in some cases, prefer to fight rather than make a threat at all, especially if the costs of "prevention of action" by other means are somehow less than making a truly "credible threat."[22]

Deterrence is thus not a single integrated activity but a bundle of different objectives and policy options, each of which pose military and/or policy tradeoffs in terms of one another. At its most basic, deterrence is the attempt to get your way, without a fight, at low cost. There may be many other objectives as well in any particular case—ensuring the legitimacy of one's behavior, satisfying a domestic interest group, cultivating a reputation for resolve, redirecting investment toward butter over guns, maintaining open trade in the midst of rising international tensions, etc. We will use the terms *winning* and *warning* to capture two of the most fundamental goals in any

[21] U.S. Joint Chiefs of Staff, "Deterrence," in Joint Publication (JP) 3-0: Joint Operations, 11 August 2011. http://www.dtic.mil/doctrine/dod_dictionary/data/d/3763.html

[22] Certain types of military action are particularly dependent on surprise or secrecy. Threats that leave too little to chance can be undermined as a target adjusts its defensive posture to counter action anticipated in a deterrent claim.

coercive interaction (these two alone generate complex tradeoffs and are thus useful for making headway into an understanding of CDD). Getting one's way ("winning") requires challenging or defending the status quo. If the disposition of politics or policy as an objective is particularly important, then capabilities and the resolve to fight will be needed to prevail if deterrence fails. Avoiding a fight ("warning"), in contrast, means ensuring that both sides clarify their interests, capabilities and intentions to one another so that mutually acceptable diplomatic bargains can be worked out, obviating the need for war. Warnings must be made as clear and credible as possible, so that the target understands just where redlines are drawn and where the risk of escalation becomes unacceptable. This will often mean making some compromises, either in negotiations or in the nature and expectations of threats. Deterrence fails when the target of a deterrent threat is asked to concede too much, or when demands appear unlikely to be acted on; everyday examples abound—"if you make me go to bed, I will hold my breath until I turn blue." Military capabilities have this dual role of changing the balance of power (winning in war) and communicating interests (warning in politics).

We focus on these two distinct goals because they follow readily from the basic bargaining model of war. Adversaries can either make a deal to keep or revise some division of the disputed good, or they can participate in a costly lottery (war), which destroys some of the surplus they could have divided. A deal enables both sides to avoid the costs of conflict even if one or the other has to give way on their preferred distribution of benefits. Yet each side has incentives to misrepresent costs and power, either by bluffing to get a better deal in the *ex ante* bargain ing or by concealing capabilities to improve performance in the *ex post* fighting. Capabilities that improve military (or intelligence) performance alter the relative balance of power, and thus the probability of doing well in a contest of strength if bargaining fails. By contrast, capabilities that

send credible signals help to reduce uncertainty about the true balance of power and the costs of conflict.

CDD emerges when different types of capabilities differentially affect winning or warning. Airpower is very useful for attacking land forces maneuvering in the open because of its great mobility and firepower. Yet this same maneuverability means that air forces can be quickly withdrawn or revectored, raising questions about whether this kind of military capability will actually be engaged when needed. Ground forces, by contrast, might suffer higher costs in attempting to repel an invasion should it occur, but since it is hard to move them out of the way of an attack, with limited mobility and logistic impedimenta, they provide a more credible signal of intent to become involved, should active combat occur. By this logic the U.S. deployment of ground forces in Europe during the Cold War and in Korea to this day acted as commitment mechanisms to ensure the U.S. would go to war if this tripwire was tripped. Naval forces face similar tradeoffs, providing power projection and influence to keep disputes further from the home power's shores, but their very mobility across the seas makes their deployment in the event of a distant crisis much more uncertain. At the same time, the costs of losing a warship, measured in hundreds if not thousands of souls, can be used to signal commitment if the signaler can somehow avoid redeploying warships out of the danger zone. Many variations are possible. Forward basing of aircraft with investment in supply and facilities may improve the credible threat to use them when needed. An adversary that equips ground forces with advanced air defenses may deter the use of aircraft altogether. Ground forces that rely on special operations and proxies sacrifice their signaling role by relying on secrecy and stratagem.

In many arenas it is possible to use different capabilities to reinforce one another. In combined arms warfare, for example, the firepower of artillery, the mobility of armor, and the

ability of infantry to identify and report on threats work as complements; the strengths of one capability cover weaknesses of the other, together enhancing the combat power of the group. Coordination of different specialized military capabilities increase the probability of winning in battle.[23] Combined arms teams can also pose a formidable deterrent, provided that elements operate together effectively (no easy task) and assuming that potential adversaries know of their effectiveness, either from the outcomes of previous contests or because they have been observed in exercises. For all the shortfalls and controversy regarding the ideology of the 'network-centric' revolution in military affairs, U.S. mastery of this mode of fighting provides a powerful deterrent against risking conventional military combat against the United States.[24]

However, winning and warning are sometimes incompatible. Nowhere is this more apparent than in the combination of cyber operations and nuclear weapons. These two capabilities are nearly perfect complements, with opposite bargaining characteristics. The fundamental utility of nuclear forces is in signaling vital national interests, not in winning a war. The nuclear domain is stable for actors armed with a secure second strike (or maybe even something less) because mutual warnings are clear and credible for all parties. By contrast, the fundamental utility of cyber operations is for changing the distribution of power by enhancing intelligence advantage or supporting the application of military force, not for signaling.[25] The revelation of a cyber exploit or an active intrusion facilitates effective defense against it through system reconfiguration or

[23] Stephen D Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, N.J.: Princeton University Press, 2004).
[24] Jon R. Lindsay, "Reinventing the Revolution: Technological Visions, Counterinsurgent Criticism, and the Rise of Special Operations," *Journal of Strategic Studies* 36, no. 3 (2013): 422–53; Michael Fortmann and Stefanie von Hlatky, "The Revoluition in Military Affairs: Impact of Emerging Technologies on Deterrence," in *Complex Deterrence: Strategy in the Global Age*, ed. T. V. Paul, Patrick M. Morgan, and James J. Wirtz (Chicago: University of Chicago Press, 2009), 304–20.
[25] Lindsay, "Tipping the Scales."

patching, while vague threats of hacking are far less credible.[26] The cyber domain is notoriously unstable as actors are constantly probing, exploiting, defending, and adapting their networks in the face of great uncertainty about the concurrent activities of the other side. What happens when these complements combine? On one hand, the stability of the nuclear domain provides an upper bound on cyber aggression, strongly discouraging any catastrophic infrastructure attack for fear that this might trigger unacceptable retaliation. On the other hand, the instability of the cyber domain can be a worrisome destabilizer of nuclear relationships, since one side can compromise the reliability of the other side's nuclear forces but cannot reveal this coup without undermining success. This inadvertently leads the other side to run risks in false confidence that its deterrent remains credible. Cyber attacks against a nation's nuclear deterrent can take many forms, interdicting the complex chain of events involved in nuclear deterrent capabilities anywhere from satellite sensing of enemy ballistic missile launch, to command and control systems, to the actual missile launch, guidance and warhead detonation. In each case, the critical factor is an attacker's incentives to conceal successes from the target of attack, to exercise advantages in future (nuclear) battles, rather than to exercise military successes in cyberspace in the form of diplomatic leverage. If the prospect of inadvertent escalation in the nuclear domain seems undesirable and effective warning thus desirable, then it becomes important to sacrifice some capability for winning in the cyber domain (or at least that corner of it that innervates nuclear command and control).[27]

Deterrence has always included multiple objectives. What has changed are the many means now available to pursue them. Since different means may differentially affect the pursuit of different ends, a full theory of deterrence must account for how choices among means influence

[26] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (2013): 41–73.
[27] For additional exploration and justification of these arguments, please see Erik Gartzke & Jon R. Lindsay, "Thermonuclear Cyberwar," (under review)

the quality of deterrence produced with them. CDD is not a different kind of deterrence, but rather a more general account of how deterrence works. Deterrence within a domain, matching threats of one type to capabilities of the same type (i.e., apples versus apples), is simply the special case of a much more general phenomenon. Classical deterrence theory focused on using nuclear weapons to prevent nuclear war and did not emphasize choice among means as a decisive act. Now that there are more means that are far less hurtful or provocative than nuclear war—some of which do not even rise to the level of force—the question for policy makers and careful observers is why and how choices are made to threaten or exercise one implement of power as opposed to others. Indeed, the increase in the diversity of means tends to fill out the lower end of the conflict spectrum, where policies for credible warning do not yet exist. Deterrence becomes more complex where uncertainty about the effects of threats and provocations is greater and the resolve to employ or counter them is more in doubt. Thus, not only does deterrence in the cyber domain suffer from an ambiguity of novelty (policy makers and practitioners are uncertain about the effects of cyber conflict), but it also struggles with an ambiguity of interaction (policy makers and practitioners do not know how conflict in the cyber domain substitutes for or complements the potential to hurt in other dimensions).

Information and Complexity

In our sketch of the logic of CDD we have discussed cyberspace as merely one domain among many. Cyber means become particularly attractive as a non-kinetic or non-intrusive way of tweaking the balance of power, even as their signaling utility is low. Yet there is a deeper relationship between cyberspace and CDD stemming from the essential role of information in economics and politics. Information becomes more salient as systems become more complex.

'Information' has a number of contradictory colloquial connotations: meaningless bits of data or the meaningful content of data; something that provides knowledge or something distinct from it; something universal or something peculiarly human.[28] Formal 'information theory,' developed simultaneously by Claude Shannon and Norbert Weiner with some influence by John Von Neumann, provides a better-defined set of concepts; these ideas underlie modern communications and electronics engineering, robotic and vehicle control, cryptology and cryptography, and game theory.[29] Information here is a measure of the probability of receiving a particular message given the variety of values a message can take. The larger the variety of possible states, the lower the probability of receiving any particular message, and thus the more informative it is to receive it. Generally, a particular message is informative about something when the state of the message is correlated with the true state of that thing and is distinguishable from what would have appeared by chance in the message. In engineering a reliable communication circuit the task is to devise encodings and error-correction schemes that faithfully transmit signals from a source to a receiver in the presence of noise in the channel. Bandwidth and storage capacity measured in bits describe the overall entropy of the system, so more bits enables to transmission and storage of more information. In cryptography the task is to devise encodings that appear like random noise for an interloper but can readily be identified as a deliberate signal by the intended receiver through the use of one or more decoding keys. Increasing the entropy of the encoded message (the number of possible states) makes it harder to guess the true state without the key. These and other applications of information theory are foundational in computer science.

[28] John Seely Brown and Paul Duguid, *The Social Life of Information* (Cambridge, MA: Harvard Business Press, 2000); Paul Davies and Niels Henrik Gregersen, eds., *Information and the Nature of Reality: From Physics to Metaphysics* (New York: Cambridge University Press, 2010).
[29] Ronald R. Kline, *The Cybernetics Moment: Or Why We Call Our Age the Information Age* (Johns Hopkins University Press, 2015).

The same information theory underlies the modern bargaining theory of war and the capacity for deterrent signaling. In non-cooperative game theory the task is for one player to discriminate the true preferences or type of the other on the basis of observable behavior. A signal is informative when it reduces uncertainty *for the receiver* about the true state of the source, not simply when the source assumes some given state. So-called cheap talk is not informative because a reliable person and a liar would say the same thing: the signal is effectively random. By contrast, costly signaling (i.e., tying hands or burning bridges) is informative because only the true type would be willing to display such behavior: the signal is anything but random. Politicians sometimes describe their desire to 'send a signal,' but the receiver's ability to discriminate likely from unlikely signals ultimately determines whether any meaningful signal is received. Deterrence depends on credible signaling that enables the challenger to infer that the defender is willing and able to punish any transgression.

A system with a greater variety of possible outcomes can be described as more complex. Such a system requires more information to describe its state. A system in a highly improbable state can be said to be more organized or less random. Economic development increases the complexity of society by rearranging the material world into less probable states. The same minerals that have always been in the Earth have been rearranged, over a long span of evolutionary and historical development, into quite improbable groupings of cities, airplanes, rockets, and the internet. It thus takes more information to describe the present state of the Earth because there are more types of things on, under, over, and around it than ever before, and there are more ways to combine them in productive and destructive activities. To coordinate and control things in the practice of government or commerce, actors need information about what state those things are in. Any measurement process that encodes and transmits information about the state of a system

(usually through some combination of information technologies, administrative organization, and human interpretation) has the potential to reduce uncertainty for an observer of that system, in effect making the system more predictable. Better information then enables an observer to select from a variety of actions those that are appropriate to the state of the system and more likely to bring about an intentional goal, or maximize utility. For example, an electronic representation of a train schedule enables a passenger to leave her house on time to catch a train and visit her friend. Information about the world and decisions to act make intended states of the world more likely and less random. More complex action that moves the world into an even less probably state (many friends visiting at the same time) requires even more information.

The evolution of information technologies makes more complex control possible. All information technology from the Rosetta Stone to the world wide web has co-evolved historically along with other human institutions to improve measurement, coordination, and enforcement in collective action. Bureaucracies rely on standardized files and statistic techniques to extend the scope of its control because their agents have limited cognitive capacities and may leave for new jobs.[30] Telecommunications and timetables can make transportation more predictable. Intelligence and surveillance systems may allow a military to know more about the state of the enemy and to strike with greater precision. The evolution of a system toward greater complexity also requires an evolution in the information technology that improves predictability and controllability in that system. The illustration of this truth is in the exceptions, when information technology does not improve quickly enough to maintain control over complexity. The Battle of Jutland provides a classic example. Innovations in government finance, propulsion, explosives, high-grade steel, and

[30] James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (New Haven, CT: Yale University Press, 1998).

fuses out-paced communications technology as signal flags were hard to see and radio was in its infancy; battleships could thus destroy each other quickly at great distance, requiring the battlespace to expand dramatically, but Admiral Jellicoe lost track of his fleet and could not communicate effectively with his ship captains.

The increase in sociotechnical complexity is a long-term historical and co-evolutionary process. Economic competition fosters a division of labor that improves the efficiency of production but also expands the scope of competition, since there are more actors and resources brought into the market. Control improvements for one competitor become a threat to the other, who will seek to disrupt enemy control systems and/or improve their own control. Military competition on a historical scale deepens the division of labor within forces and weapons systems by a similar logic. Competition becomes more nuanced as the systems that regulate it become more sophisticated. Conflict within cyberspace is exemplary in this regard because it exploits imperfections in the most complex systems human beings have ever built, relying on deception and guile rather than brute force. 'Cyber' comes from a Greek word meaning control, a root shared by 'government.' Thus 'cyberspace' as such is symptomatic of the expanding complexity and scope of control in every sector of human activity—science, commerce, entertainment, administration, and warfare—which all depend on ever more sophisticated means for representing and communicating the dynamic state of the world.[31] There is more information in the world because governments, firms, and individuals enjoy more control over their affairs, and vice versa. This also creates control contests where their increased potential for control comes into conflict.

[31] Thomas Rid, *Rise of the Machines: A Cybernetic History* (New York: W. W. Norton & Company, 2016).

Information technology improves human control over flows of labor and capital, as well as control over the controls (bureaucracy and information technology).[32]

Herein lies the basic irony of both cybersecurity and CDD: there appears to be more uncertainty and conflict variety in the world precisely because there is more information and control in the modern globalized world. Because there are more types of capabilities, linkages, and actors, more information is required to describe the state of the world, and thus there is a lot more uncertainty in detail. With more uncertainty there is more scope for confusion and deception, and these information imperfections make conflict more likely. Yet the condition for the possibility of this complexity is a system that has moved, through a long evolutionary process, into a highly organized and historically improbable state. Perfect information is not available, but pretty good information often is available. Thus many states have no reason to resort to violence to renegotiate their bargains because they understand the likely costly consequences. The bargains that are uncertain and thus liable for renegotiation are for smaller stakes. Greater complexity creates more things to argue about by settling the big arguments. Put another way, disruptions are more frequent but less intense.[33]

Cybersecurity and CDD are both symptomatic of increasing sociotechnical complexity, and they both deal with threats that exploit the additional information required to fully describe the state of the complex world. Threats to the security of cyberspace and the stability of deterrence are quite literally working at the margins of the system, exploiting and predicated upon the

[32] James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, MA: Harvard University Press, 1986); Joel Mokyr, *The Gifts of Athena: Historical Origins of the Knowledge Economy* (Princeton University Press, 2002).
[33] Jon R. Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," in *The Power to Hurt: Coercion in Theory and in Practice*, ed. Kelly M. Greenhill and Peter J. P. Krause (New York: Oxford University Press, Forthcoming).

existence of predictable exchange relationships. Because people place more trust than ever before in cyberspace, there is more scope than ever for subtle subversion of the means of control. Because states have better information than ever before about the balance of power and likely costs of great power war, there is more scope than ever before for provocative moves in the 'gray zone' below the threshold of retaliatory response. Vertical moves that inflict clear and obvious harms risk serious punishment, but horizontal moves into new domains that are not clearly proscribed by a credible deterrent policy offer some promise of gain. Deterrence 'fails' in low-intensity and especially non-violent disputes because it 'succeeds' everywhere else.

Conclusion

Although it is possible and sometimes necessary to talk about cybersecurity and cross-domain deterrence separately, there is an intimate historical and conceptual connection between them. Cyberspace may be one domain among many, but all of the other domains depend on some sort of information technology for command and control. As a military operational environment, furthermore, it is notable that civilians largely invent, own, and operate much of the constitutive architecture; as a result, cyberspace is largely out of military control. Deterrence, in practice if not in theory, has leveraged many means since long before the information age, yet its success and failure has always been a problem of what one knows or perceives, and what one can convey. Even commitment problems under supposedly perfect information still depend on information about the range of states that actors might assume in the future. It is no accident that these two policy problems have appeared together, or that a complex information technology should complicate the information challenges of strategic interaction. They are symptoms of the same underlying cause: historically increasing economic, political, and technological complexity. Exchange and conflict

are two related mechanisms that ratchet up the complexity of human interaction by incentivizing an increase in variety.

This chapter has sketched an argument that is embedded in a larger research agenda on CDD.[34] We have noted the ways in which our previous work on cybersecurity has both inspired and benefitted from our research on deterrence. Further work remains to be done to clarify the formal logic and empirical implications and to test key implications of the insights that result. Doing so is difficult because of the same complexity that is the subject matter of this research. Yet in posing the problem of complexity as primarily an issue of uncertainty and the management of information, there is real potential to make new progress in both the micro and macro logic of deterrence, a topic that appeared filled out, well understood, and even stagnant to many scholars. Winning differs from warning. The fact that they have been conflated in traditional discussions of deterrence made it difficult to understand the tradeoffs involved in emphasizing one or the other, and made it impossible to consider how new means might differ in accomplishing either objective.

The historical origins of information theory may point out a way in which deterrence theory can develop. Shannon's seminal 1948 article on communication examined the challenges of encoding a signal to get it *through* a noisy channel.[35] This work was an outgrowth of Shannon's wartime work in Bell Labs on encryption, described in a classified 1945 article on the challenges of disguising an encoded signal *as* noise.[36] The mathematics of obfuscated information and reliable communication are one and the same endeavor. So too deterrence has a dual aspect, which we have described in terms of winning and warning. Warning is the problem of clear and reliable

[34] See http://deterrence.ucsd.edu
[35] Claude E. Shannon, "A Mathematical Theory of Communication," *The Bell System Technical Journal* 27 (October 1948): 379–423, 623–56.
[36] Claude E. Shannon, "A Mathematical Theory of Cryptography," Technical Report (Bell Labs, September 1, 1945).

signaling, which clarifies cost and power and makes war less likely. Winning is the problem of ensuring that power is sufficient to get a favored outcome in conflict, and it often relies on capabilities that must be hidden to be effective. The element of surprise is an important, but variable, complement to the possession and exercise of different capabilities. Maneuver warfare attempts to present the adversary with more problems than it can handle, tipping the relative balance of friction in one's favor. Cyber deception, like a magician's sleight of hand, exploits degrees of freedom that deterministic machines cannot detect. Whereas signaling attempts to reduce uncertainty, warfighting (and intelligence) attempts to increase it.

Shannon's unified view of clear communication and unreadable encryption suggests that winning and warning, apparently so different, need to be understood in a common framework. Warning attempts to credibly communicate through the noise, while winning attempts to prevail more effectively by masquerading as noise. Strategy must combine them both. The logic of encryption, moreover, may ultimately be more appropriate for the complex intelligence-counterintelligence contests that characterize modern strategic problems from cybersecurity to counterterrorism. Deterrence is no longer simply a game of chicken with the survival of civilization in the balance, if it ever was, but rather an ongoing tapestry of moves and countermoves at different timescales and levels of analysis. These intertwined and iterated games both exploit and generate systemic complexity. Classical deterrence theory provides the invaluable distinction between contests of strength and contests of resolve. A more general deterrence theory must include contests of deception as well.