Chapter 1

Cross-Domain Deterrence as a Practical Problem and a Theoretical Concept

Jon R. Lindsay and Erik Gartzke

[*Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Erik Gartzke and Jon Lindsay]

<1>Introduction

"When there is mutual fear," Thucydides observed, "men think twice before they make aggressions on one another."[1] Political leaders have used threats of war to defend their interests since antiquity, but deterrence as a precise theoretical concept and a paramount element of national security policy only emerged in the nuclear era. Throughout most of history the means of violence were inherently limited, so war remained a real option for settling disagreements when threats failed. In the aftermath of Hiroshima, however, warfighting became suicidal. Massive, mobile, and dispersed arsenals of intercontinental missiles, each capable of destroying entire cities, rendered defense all but futile, even as militaries sought ways to limit damage. Yet for the same reason, as Bernard Brodie famously pointed out, threats of nuclear war could be especially useful for keeping the peace. The superpowers developed weapons they dared not use but which they needed to discourage aggression, or for occasional blackmail. A vast literature developed to understand deterrence as a problem of high stakes bargaining between two states, to include specialized elaborations on the credibility of nuclear guarantees to allies, the incentives for conventional war in the shadow of nuclear deterrence, the reliability of nuclear command and control systems, and

[1] Benjamin Jowett, *Thucydides, Translated into English, to Which Is Prefixed an Essay on Inscriptions and a Note on the Geography of Thucydides*, 2nd ed. (Oxford: Clarendon Press, 1900), para. 4.62.

psychological and cultural deviations from the rationalist ideal. This work produced a general consensus on the logic, if not the practice, of deterrence.[2]

The complexity of the 21st century threat landscape contrasts markedly with the bilateral nuclear bargaining envisioned by classical deterrence theory. Nuclear and conventional arsenals continue to develop alongside newer threats of anti-satellite programs, autonomous robotics or drones, cyber warfare and pervasive surveillance, directed energy weapons, biotechnology, and innovations barely imagined. Some of these technologies may produce disruptive effects on par with weapons of mass destruction, but many of them open up options for low intensity or even nonlethal effects. Some of these technologies depend on rarified military capabilities, but many draw their aggressive potential from their utility and availability in the global economy. Various political actors may have the ability and motivation to exploit these capabilities in unexpected ways, from ambitious rising powers like China to dissatisfied regional powers like Russia or Iran, domestic factions of weak allies like Pakistan and Iraq, anarchist movements like Anonymous, terrorist groups like the so-called Islamic State, and the list goes on. It is possible, and widely feared, that weaker states and non-state actors might exploit the technologies of globalization to undermine the conventional military advantages of top powers like the United States; it is also

[2] Lawrence Freedman, *Deterrence* (Wiley, 2004), 117, notes "how complicated a theoretical tangle developed around deterrence even during the cold war, a period of unusual clarity and continuity in international affairs." Influential works include Bernard Brodie et al., *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace and Co., 1946); Albert Wohlstetter, "The Delicate Balance of Terror" (Santa Monica, CA: RAND Corporation, December 1958); Herman Kahn, *On Thermonuclear War* (Princeton University Press, 1960); Glenn H Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton, N.J.: Princeton University Press, 1961); Thomas C. Schelling, *Arms and Influence: With a New Preface and Afterword* (New Haven, CT: Yale University Press, 2008); Kenneth N Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley Pub. Co., 1979); Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca: Cornell University Press, 1989); Robert Powell, *Nuclear Deterrence Theory: The Search for Credibility* (Cambridge University Press, 1990). Insightful reviews of classical deterrence literature include Fred Kaplan, *The Wizards of Armageddon* (New York: Simon and Schuster, 1986); 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; Marc Trachtenberg, *History and Strategy* (Princeton University Press, 1991), chap. 1. For argument that Cold War nuclear policymaking departed significantly from strategic precepts see Francis J. Gavin, *Nuclear Statecraft: History and Strategy in America's Atomic Age* (Ithaca: Cornell University Press, 2012).

possible that strong and wealthy states are better poised to integrate emerging capabilities to augment and enhance their power. The considerable complexity of the 21st century need not necessarily result in higher levels of danger; on the contrary, complexity may provide the means for strategic actors to subtly revise the status quo without triggering war. Either way, complexity itself poses major problems for strategy.

The term *cross-domain deterrence* (CDD) emerged in the late 2000s as defense policymakers in the United States grappled with the vulnerability of space and cyberspace and the willingness of states like China and Russia to exploit it for asymmetric advantage. The Pentagon recognizes five operational environments or *domains*—land, sea, air, space, and cyberspace—and U.S. military power depends on carefully synchronized operations across them. Chinese strategists, among others, point out that the Achilles Heel of the American juggernaut is the network of sensors, computers, and datalinks that facilitate intelligence gathering and precision strikes; they argue that vital information infrastructure on Earth or in orbit can be disrupted via low-cost or deniable means to discourage or even defeat American intervention overseas.[3] The dangers were dramatized throughout the 2000s by the burgeoning of China's so-called Anti-Access/Area-Denial (A2/AD) capacity in the Western Pacific, as well as aggressive cyber intrusions linked to China, Russia, and the United States itself. Policymakers became concerned about the erosion of U.S. conventional and nuclear deterrence postures and worried that any military retaliation for space or cyber attacks might be too escalatory or totally misinterpreted by foreign governments, given the absence of common norms of appropriateness and proportionality in new domains. American mastery of cross-domain *operations* thus came at the price of more

[3] Jacqueline Newmyer, "The Revolution in Military Affairs with Chinese Characteristics," *Journal of Strategic Studies* 33, no. 4 (2010): 483–504; Kevin Pollpeter, "Controlling the Information Domain: Space, Cyber, and Electronic Warfare," in *Strategic Asia 2012-13: China's Military Challenge*, ed. Ashley J. Tellis and Travis Tanner (Seattle, WA: National Bureau of Asian Research, 2012).

complicated cross-domain *deterrence* for political and military leaders. At the same time, the potential advantages of doing CDD well, or at least better than an opponent, could be substantial.[4]

One might wonder whether CDD is just another Pentagon buzzword coined amid millennial concerns about space, cyberspace, and China. While the term CDD has a peculiar American provenance, the strategic problem appears more general. The Chinese concept of "Integrated Strategic Deterrence," for example, responds to similar challenges and opportunities created by the expanded diversity and interdependence across military technologies, stressing an imperative for coordinating nuclear, conventional, space, and cyber capabilities to achieve Chinese security objectives.[5] The goal of this book is to problematize CDD as an analytical concept, highlighting the complex relationships between the portfolio of coercive instruments available and the effectiveness of coercive policy. Are traditional deterrence concepts sufficient to explain why threats in or across novel domains succeed or fail, or does the very complexity of emerging threats require new strategic concepts?

In generalizing CDD we pay particular attention to the *means* of deterrence. Classical deterrence theory was agnostic about means because threats were assumed to be nuclear. Theorists thus focused on the political problems of interest and credibility rather than the choice of means, while empirical scholars debated the applicability and scope of the theory.[6] Much deterrence scholarship today still puts primary emphasis on nuclear weapons, which is reasonable enough

[4] Discussion of CDD by contemporaries include Shawn Brimley, "Promoting Security in Common Domains," *The Washington Quarterly* 33, no. 3 (July 1, 2010): 119–32; James A. Lewis, "Cross-Domain Deterrence and Credible Threats" (Washington, DC: Center for Strategic and International Studies, July 2010); 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); Madelyn R. Creedon, "Space and Cyber: Shared Challenges, Shared Opportunities," *Strategic Studies Quarterly*, no. Spring (2012): 3–8.
[5] Michael S. Chase and Arthur Chan, "China's Evolving Approach to 'Integrated Strategic Deterrence'" (Santa Monica, CA: RAND Corporation, 2016), http://www.rand.org/pubs/research_reports/RR1366.html.
[6] For a thorough review of theoretical and empirical deterrence scholarship see Shannon Carcelli, "Blast from the Past: Updating and Diversifying Deterrence Theory," Working Paper (La Jolla, CA, March 24, 2016).

given the dangers of a putative "second nuclear age."[7] The literature on the interaction between nuclear and conventional forces offers some potentially useful insights for CDD, for instance the idea that nuclear stability can incentivize limited or proxy wars, or that limited conventional attacks might inadvertently escalate to nuclear war.[8] Recent scholarship has begun to tackle the complexity of modern deterrence by relaxing the classical focus on nuclear weapons, bilateral bargaining, and state actors to address problems of proliferation, terrorism, conventional war, and other forms of aggression.[9] There is a lacuna regarding the diversification of strategic instrumentalities in play, although there is a developing literature on the deterrence challenges in idiosyncratic domains like space and cyberspace.[10]

Policymakers and commanders today have a complicated portfolio of coercive means available to pursue their objectives. They may use air strikes to retaliate for terrorism, cyber operations to disable an attacker's military command and control, or targeted economic sanctions to punish a cyber intrusion. CDD posits that *how* actors choose to deter affects the quality of the deterrence they achieve. Deterrence in practice must deal with not only the fruits of the nuclear

---

[7] Inter alia, T. V. Paul, Richard J. Harknett, and James J. Wirtz, eds., *The Absolute Weapon Revisited: Nuclear Arms and the Emerging International Order* (University of Michigan Press, 2000); Avery Goldstein, *Deterrence and Security in the 21st Century: China, Britain, France, and the Enduring Legacy of the Nuclear Revolution* (Stanford University Press, 2000); George P. Shultz, Sidney D. Drell, and James E. Goodby, *Deterrence: Its Past and Future—Papers Presented at Hoover Institution, November 2010* (Stanford, CA: Hoover Institution, 2011); Toshi Yoshihara and James R Holmes, eds., *Strategy in the Second Nuclear Age: Power, Ambition, and the Ultimate Weapon* (Washington, DC: Georgetown University Press, 2012).

[8] Inter alia, Glenn H. Snyder, "The Balance of Power and the Balance of Terror," in *The Balance of Power*, ed. Paul Seabury (San Francisco, CA: Chandler, 1965); Jervis, *The Meaning of the Nuclear Revolution*; Barry R. Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Ithaca, N.Y.: Cornell University Press, 1991); Avery Goldstein, "First Things First: The Pressing Danger of Crisis Instability in U.S.-China Relations," *International Security* 37, no. 4 (2013): 49–89; Vipin Narang, *Nuclear Strategy in the Modern Era: Regional Powers and International Conflict* (Princeton University Press, 2014).

[9] Inter alia, Frank C. Zagare and D. Marc Kilgour, *Perfect Deterrence* (Cambridge University Press, 2000); Patrick M. Morgan, *Deterrence Now* (New York: Cambridge University Press, 2003); Timothy W. Crawford, *Pivotal Deterrence: Third-Party Statecraft and the Pursuit of Peace* (Cornell University Press, 2003); T. V. Paul, Patrick M. Morgan, and James J. Wirtz, eds., *Complex Deterrence: Strategy in the Global Age* (Chicago: University of Chicago Press, 2009); Jeffrey W. Knopf, "The Fourth Wave in Deterrence Research," *Contemporary Security Policy* 31, no. 1 (April 1, 2010): 1–33; Anne E. Sartori, *Deterrence by Diplomacy* (Princeton University Press, 2013).

[10] See the chapters in this volume by Bahney et al and Schneider on space and cyberspace, respectively.

revolution, but also manage a growing array of new technological "apples and oranges" that differ markedly from each other in their material, organizational, and political characteristics. *Cross-domain deterrence*, therefore, is the use of threats in one domain, or some combination of different threats, to prevent actions in another domain that would change the status quo. More simply, CDD is the use of unlike means for the political ends of deterrence.

The notion of a "domain," moreover, need not be limited to a discrete territory with clearly delineated boundaries. It might also describe a legal jurisdiction, the ownership of resources, a division of labor, or an area of technical expertise. Complex problems span domains. In this book we consider a *domain* to be any pathway or means for coercion that is different from other means in important respects so that one may compare interactions between actors according to how like confronts like and, increasingly, how unlike confronts unlike. This approach frees theory from an arbitrary restriction to geography and affords analysis of non-military means like economic sanctions or immigration policy. Nuclear and conventional weapons can thus be considered as different domains because of their profoundly different material and political characteristics, even as both types of forces are deployed in the land, sea, air, and space environments. Generalizing the concept of domain also expands the historical applicability of CDD.

The remainder of this chapter provides background on why CDD emerged as a defense policy problem when it did, summarizes each chapter's contribution to the assessment of CDD as an analytical concept, and concludes with reflections on the implications for deterrence theory.

<1>The Historical Context of CDD

At the end of the Cold War, the United States found itself in an unrivaled position of global military superiority, or hegemony. Throughout the 1970s and 80s, in the face of preponderant Soviet

conventional forces in Central Europe, the U.S. military attempted to substitute quality for quantity by investing heavily in battlefield surveillance networks, long-range precision weapons, electronic warfare, and a highly-skilled Joint Force. Many described the result as a Revolution in Military Affairs (RMA). Freed from the geopolitical constraints of the Cold War, the RMA produced lopsided combat victories for the United States in the 1991 Gulf War, 1999 Kosovo War, and 2003 invasion of Iraq; moreover, even in the protracted counterinsurgencies in Afghanistan and Iraq, the U.S. military proved adept at adapting RMA technologies to target individual insurgents. However, the American RMA was expensive, thinly stretched, and exceedingly dependent on information technologies. A modernizing China or a resurgent Russia might exploit these factors to erode U.S. military hegemony and undermine the credibility of its security guarantees.[11]

Concern about CDD in the United States was motivated mainly by the strategic conundrums of space and cyberspace in the context of challenges to U.S. hegemony in the Western Pacific, even as the scope of CDD as a strategic concept was not limited to these developments. The potency of offensive methods relative to the efficacy of defense appeared to be especially challenging in cyberspace—the one domain that connects all others—even as attribution and ambiguity problems appeared to undercut the reliability of deterrence.

<2>The Cyber Domain

Four of the Pentagon's domains are physical places, but the fifth is constructed, according to the official definition, from "interdependent networks of information technology infrastructures and

[11] The seminal description of the RMA is Office of Net Assessment, *The Military-Technical Revolution: A Preliminary Assessment*, ed. Andrew F Krepinevich (Washington, DC: Center for Strategic and Budgetary Assessments, 2002). For review of the contentious RMA debate see Tim Benbow, *The Magic Bullet? Understanding the Revolution in Military Affairs* (Brassey's, 2004). On the performance of the RMA in Iraq see 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; Keith L Shimko, *The Iraq Wars and America's Military Revolution* (New York, NY: Cambridge University Press, 2010).

resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[12] There is nothing inevitable about this categorization, however, as the use of the term "domain" for a military operating environment gained currency only around the turn of the millennium. *Joint Vision 2010*, an RMA manifesto issued in 1996 by the Chairman of the Joint Chiefs of Staff, did not use the word "domain" even though it envisioned "widely dispersed joint air, land, sea, and space forces" working together to realize "full spectrum dominance" and other RMA ideals.[13] Yet the word figured prominently in the 2000 update of *JV2010*, entitled *Joint Vision 2020*: "U.S. forces are able to conduct prompt, sustained, and synchronized operations with combinations of forces tailored to specific situations and with access to and freedom to operate in all domains—land, sea, air, space, and information."[14] *JV2020* gave special emphasis to the "information domain" due to its vital importance to other domains and vulnerability to exploitation by "asymmetric" adversaries: "The United States itself and U.S. forces around the world are subject to information attacks on a continuous basis regardless of the level and degree of engagement in other domains of operation."[15]

Indeed, the rise of "domain" terminology is inextricably linked to the rise of cyberspace as a national security concern for the United States and a bureaucratic opportunity for its military services.[16] Throughout the 1990s and 2000s, members of the nascent U.S. information warfare

[12] http://www.dtic.mil/doctrine/dod_dictionary/data/c/10160.html accessed 14 May 2016
[13] Chairman of the Joint Chiefs of Staff, "Joint Vision 2010" (U.S. Department of Defense, 1996), 20, http://www.dtic.mil/jv2010/jv2010.pdf.
[14] Chairman of the Joint Chiefs of Staff, "Joint Vision 2020: America's Military-Preparing for Tomorrow," *Joint Forces Quarterly*, 2000, 61.
[15] 72
[16] By the end of the 1990s, writers grappling with the national security implications of malicious software tools and ubiquitous internet connectivity had begun to explicitly write about the "cyber domain." E.g., Fred Cohen, "Managing Network Security: Returning Fire," *Network Security* 1999, no. 2 (February 1999): 11–15. This coinage followed naturally within the computer science milieu given the prevalence of the "Domain Name System" and similar nomenclature, but it also became attractive to military organizations in the business of dominating their rivals. Around the same time, the U.S. Navy began to use the term "Maritime Domain Awareness" to describe

community worked to gain acceptance for the idea of cyberspace as a warfighting domain as well as material support and legal authority to man, train, and equip forces to fight within it.[17] Similar to the way in which strategic bombing doctrine aided the champions of an independent air force in the 1930s and 1940s, the notion of a new fifth domain had important institutional implications. A September 2006 briefing by the director of the U.S. Air Force (USAF) Cyberspace Task Force promoted the new religion with "The Cyber Creed," which states, "Cyber is a war-fighting domain. The electromagnetic spectrum is the maneuver space. Cyber is the United States' Center of Gravity—the hub of all power and movement, upon which everything else depends. It is the Nation's neural network. Cyber superiority is the prerequisite to effective operations across all strategic and operational domains—securing freedom from attack and freedom to attack."[18] The same briefing noted that "Cross-Domain Dominance = Sovereign Options," a variation on the RMA theme of better fighting through Joint synergy, tinged with the classic airpower idea that advanced technology creates strategic or "sovereign" alternatives to traditional fighting. By no coincidence the USAF aimed to position itself as the leader in three of the five domains, as reflected in its mission statement "to fly, fight and win...in air, space and cyberspace." If cyberspace could be rhetorically differentiated from and considered coequal to the environments dominated by traditional services, then the new domain would also need service-like budgets and authorities.

---

electronic ocean surveillance and data fusion, activities which had been a naval preoccupation throughout the Cold War but which gained new urgency with the proliferation of data sources and complexity.

[17] For accounts of these efforts see Gregory J Rattray, *Strategic Warfare in Cyberspace* (Cambridge, Mass.: MIT Press, 2001), chap. 5; Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* 27, no. 5 (2012): 781–99; Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Washington, DC: Cyber Conflict Studies Association, 2013), chap. 1.

[18] Lani Kass, "A Warfighting Domain" (Headquarters U.S. Air Force, AF Cyberspace Task Force, Washington, DC, September 26, 2006), http://www.au.af.mil/info-ops/usaf/cyberspace_taskforce_sep06.pdf.

The colloquial term "domain" has both jurisdictional and functional connotations, meaning either "An area of territory owned or controlled by a ruler or government" or "A specified sphere of activity or knowledge."[19] It is quite misleading to think of cyberspace as a separate territorial space in the first sense. All information infrastructure exists somewhere—servers on land, submarine cables, communications satellites, radio waves in the air, *etc*.—and most of it is owned and operated by private firms or public utilities in some state's territory; governments can and do intervene to control content and devices in their jurisdiction.[20] Furthermore, the idea that cyberspace is some sort of global commons like the high seas or international airspace is a categorical mistake; from an economic perspective, access to data on the internet (e.g., Google searches and Twitter tweets) and critical internet resources (e.g., bandwidth and reliable addressing) are better described as club goods or common pool resources rather than pure public goods.[21]

Nevertheless, cyberspace can be considered as a domain in the second, functional, sense. Any tank, ship, aircraft, or satellite relies on communication and computation to do anything in its environment whatsoever, and computer network operations in turn require a skilled workforce and organizational support. The bureaucratic prize of the cyber "domain" is domination of the resources and authorities associated with this expertise. The USAF was the first service to establish a major cyber warfare command, followed by smaller analogs in the Navy and Army cobbled together from personnel from intelligence, cryptology, information operations, and computer

[19] http://www.oxforddictionaries.com/us/definition/american_english/domain accessed 14 May 2016. In the computer science usage—"A distinct subset of the Internet with addresses sharing a common suffix or under the control of a particular organization or individual"—the jurisdictional connotation of "domain" remains salient.
[20] Jack L Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press, 2006).
[21] Mark Raymond, "Puncturing the Myth of the Internet as a Commons," *Georgetown Journal of International Affairs*, 2013, 53–64; Laura DeNardis, *The Global War for Internet Governance* (New Haven: Yale University Press, 2014); Jesse Horton Sowell, II, "Finding Order in a Contentious Internet" (Ph.D. Dissertation, Engineering Systems Division, Massachusetts Institute of Technology, 2015).

administration backgrounds. The Pentagon consolidated these efforts under U.S. Cyber Command (CYBERCOM) in May 2010 as a sub-unified command under U.S. Strategic Command (STRATCOM). CYBERCOM was collocated with the National Security Agency (NSA) to take advantage of its technical expertise, and General Keith Alexander, Director of the NSA, became its first commander. The acceptance by senior Defense leadership of cyberspace as a domain "just as critical to military operations as land, sea, air, and space"[22] gave the fledgling CYBERCOM—and its comparatively geeky warfighters by traditional military standards—a legitimacy and influence it might not otherwise have enjoyed.

The origins of CYBERCOM within the USAF and STRATCOM also contributed to a focus on the strategic potential of the new domain, and by extension, awareness of the problem of CDD. STRATCOM, with its Cold War heritage in USAF Strategic Air Command and operational control of the nation's nuclear forces, is an important locus of deterrence thinking in the U.S. Department of Defense (DoD). Furthermore, Secretary Donald Rumsfeld's 2002 Unified Command Plan reorganization gave STRATCOM responsibility for the capabilities that ultimately morphed into CYBERCOM and also merged U.S. Space Command with STRATCOM. According to the official history, "Technological advances were outpacing doctrine, particularly in global information operations, and a new STRATCOM could direct integrated global planning and execution to link strategic capabilities and the space domain."[23] Like the USAF Cyberspace Task Force, STRATCOM emphasized the strategic potency of attacks on vital information infrastructure. Attacks on satellite constellations or the control systems for electrical power delivery, air traffic control, industrial manufacturing, global finance, or military communications might cripple a

[22] William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, 2010.
[23] Edward J. Drea et al., *History of the Unified Command Plan, 1946–2012* (Washington, DC: Joint History Office, Office of the Chairman of the Joint Chiefs of Staf, 2013), 85.

nation as sure as weapons of mass destruction. If the notion of "Cross-Domain Dominance" articulated by the USAF envisioned a quantum leap in warfighting effectiveness via cyberspace synergy, it was not a far leap to "Cross-Domain Deterrence," which sought to dissuade others from taking that leap. The consolidation under the STRATCOM umbrella of all U.S. nuclear, cyber, and space forces provided an institutional locus of concern for the strategic interaction of these quite different but exceptionally vital capabilities.[24]

Journalists report that STRATCOM played a key role, together with the NSA, in the development and testing of the cyber attack on Iranian nuclear enrichment infrastructure that was disclosed in the summer of 2010. Dubbed 'Stuxnet' by private cybersecurity experts, this unprecedented malware was allegedly part of a U.S. covert action program directed at Iran known as *Olympic Games*.[25] Although its material impact on Iran's nuclear program was negligible, Stuxnet demonstrated that cyber-physical attack on industrial machinery was a real option. Stuxnet was also a landmark case of CDD, being a cyber substitute for an airstrike against Iranian nuclear targets and an effort to persuade Israel not to strike out on its own, which would have probably resulted in terrorist retaliation from Iran or worse. Importantly, Stuxnet was meant to remain both covert and clandestine (unattributed and undiscovered), but its complexity resulted in mission compromise and unintended consequences, suggesting that operational weaponization can impose

[24] STRATCOM's enduring focus on the severity of CDD is reflected in recent comments by its commander: "as we look back on the events of 2014, and the early part of 2015, we can see that today's threat environment is more diverse, complex and uncertain than it's ever been, against a backdrop of global security environment latent with multiple actors, operating across multiple domains. From under the sea to geosynchronous orbit, you have your Strategic Command focused on addressing existential threats and preserving our democratic values and way of life." Cecil Haney, "Department of Defense Press Briefing by Adm. Haney in the Pentagon Briefing Room" (U.S. Department of Defense, March 24, 2015), http://www.defense.gov/News/News-Transcripts/Transcript-View/Article/607027.

[25] Fred Kaplan, "Who Leaked the Stuxnet Virus Story?," *Slate*, June 28, 2013; Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishing Group, 2014). For further analysis of this case see the chapter by Nacht et al in this volume and Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365–404.

real constraints on CDD. Stuxnet raised the specter that the same methods might be used to work around U.S. deterrence as well, unless the U.S. could devise some sort of new and credible policy.

Russian cyber operations provided further impetus for worrying about CDD. Russian hackers penetrated Pentagon systems in operations dubbed Moonlight Maze and Buckshot Yankee, raising concerns that the same techniques used for intelligence collection might also be employed for disruptive attack. More dramatic was the wave of distributed denial of service (DDoS) attacks that hit Estonia in 2007, resulting in millions of dollars in lost productivity and remediation costs. As the newest member of the North Atlantic Treaty Organization's (NATO), Estonia considered invoking Article V, the treaty's collective defense clause, but as the Estonian defense minister observed, "Not a single NATO defence minister would define a cyber-attack as a clear military action at present."[26] Moreover, Moscow's culpability was never demonstrated beyond a reasonable doubt, although it had an obvious motive to protest Tallinn's removal of a Soviet stature.[27] The attacks created much consternation within NATO about whether and how to deter such ambiguous provocations in the future. A year later, Georgia was hit with a similar barrage of DDoS attacks of ambiguous provenance, this time coinciding with a Russian land invasion of South Ossetia and naval blockade of Abkhazia.[28] Georgia was not a NATO member, so there could be little expectation of a deterrent response, but the apparent success of Russia's cross-domain operation nevertheless created more pessimism about CDD. If an attacker exploited the cyber domain to avoid the undesirable consequences of acting somewhere else, it could inflict some amount of harm yet fly below the threshold of retaliation. These cases also highlighted an

[26] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 17, 2007, http://www.theguardian.com/world/2007/may/17/topstories3.russia.
[27] Andreas Schmidt, "The Estonian Cyberattacks," in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, ed. Jason Healey (Washington, DC: Cyber Conflict Studies Association, 2013), 174–93.
[28] Deibert R.J, Rohozinski R, and Crete-Nishihata M, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War," *Security Dialogue* 43, no. 1 (2012): 3–24.

apparent paradox of CDD, namely that failure to deter action at one level in one domain may in fact be evidence of successful deterrence of more serious attacks elsewhere. CDD might even be characterized somewhat facetiously, if accurately, as the art of using new means to get your way when you don't care enough to use the old ways. This logic recalls the stability-instability paradox of the Cold War, whereby mutual nuclear deterrence may have prevented nuclear war, but also led to extensive peripheral conventional aggression where nuclear threats were not credible.[29]

Russian cyber activity in the 2000s paled by comparison with Chinese campaigns, in volume if not sophistication. Chinese cyber espionage had increased to epidemic levels by 2011, motivated mainly, but not exclusively, by non-military objectives such as economic espionage and political censorship. While the Chinese "advanced persistent threat" (APT) focused initially, and continually, on Western government and defense industry targets, the traditional focus of state intelligence services, Chinese APTs increasingly targeted commercial firms and non-governmental organizations that had little expectation of government protection. While China was perhaps deterred from direct military confrontation with the United States, cyberspace enabled it to design around the deterrent. A gradual "death by a thousand cuts" via the erosion of U.S. military and economic competitiveness thus emerged as a real alternative to the "digital Pearl Harbor" often invoked by cyber futurists (and ridiculed by skeptics). Moreover, defense planners could not rule out a catastrophic Chinese cyber attack on Western targets, in part because strategists in the People's Liberation Army (PLA) wrote enthusiastically about just such an eventuality. Chinese concepts of "unrestricted warfare" and "integrated network electronic warfare" elaborated on RMA ideas about the potency of the information revolution and extolled the asymmetric, low-cost,

[29] Jon R. Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," in *The Power to Hurt*, ed. Kelly M. Greenhill and Peter J. P. Krause (Under review, n.d.).

offense-dominant, and decisive potency of network warfare. The accumulating evidence of pervasive Chinese cyber espionage lent some credibility to the PLA's fanciful aspirations; furthermore, in the context of Chinese military modernization across *all* domains, Chinese doctrine regarding "limited war under conditions of informatization" imparted considerable urgency to the problem of CDD.[30]

<2>Contesting Common Domains

U.S. military hegemony, according to Barry Posen, is founded on "command of the commons," the ability to use the Earth's oceans, atmosphere, and outer space for military advantage while preventing opponents from doing the same.[31] Two years after Posen's seminal article appeared, the *2005 National Defense Strategy* (NDS) asserted that "operating in the global commons" was one of America's "key operational capabilities" and "critical to the direct defense of the United States and its partners."[32] Yet in terrestrial and littoral "contested zones," Posen cautions that the balance of cost or resolve begins to tilt against the United States. Abundant small arms, indigenous nationalism, and marginal American interests combine to turn most U.S. military adventures on foreign soil into costly quagmires. Likewise, China's A2/AD envelope extends ever further offshore through a combination of advanced surface-to-air missiles, fifth-generation fighters, long-range anti-ship missiles, fast patrol craft, quiet diesel submarines, and space and counter-space capabilities, together with institutional reform of the PLA. The balance of power still strongly favors the United States over China in every domain for most conceivable scenarios (e.g., a

[30] On Chinese cyber operations and policy see Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (New York: Oxford University Press, 2015).
[31] Barry R. Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security* 28, no. 1 (2003): 5–46.
[32] "The National Defense Strategy of the United States of America" (U.S. Department of Defense, March 2005), 15–16.

Taiwanese movement toward independence or a clash over the Spratley Islands), but the relative gap has been closing steadily. The expanding contested zone in the Western Pacific was, and remains, a major stimulus for thinking about CDD.[33]

Although "domain" terminology predates Posen's article by a few years, it resonates strongly with the idea of the global commons and the struggle to dominate them. Revealingly, the phrase "land domain"—the one environment that is anything but a commons insofar as everything but Antarctica is someone's sovereign soil—does *not* appear in the official DoD dictionary as of this writing (unlike the other four domains). In traditional legal vernacular the terms "maritime domain" and "land domain" usually referred to the extent of national sovereignty; where a state's maritime domain or territorial waters ended, international waters or the maritime commons began.[34] A domain is owned and the owner claims a right of exclusion. A government might claim eminent domain over its citizens' property rights. The British Empire ruled over its Dominions. A commons, by contrast, is "land or resources belonging to or affecting the whole of a community."[35] Only a military hegemon able to project power at a global scale could imagine conflating a global commons with a military domain extending around the entire Earth. Command of the seas, in the Mahanian sense, precludes an enemy fleet from interfering with sea lines of communications, in effect imposing exclusionary control on a previously open commons. If the naval hegemon is a

[33] On A2/AD see Evan Braden Montgomery, "Contested Primacy in the Western Pacific: China's Rise and the Future of U.S. Power Projection," *International Security* 38, no. 4 (2014): 115–49; Eric Heginbotham et al., *The U.S.-China Military Scorecard* (Santa Monica, CA: RAND Corporation, 2015). On the absence of A2/AD or the purportedly Chinese term "counter-intervention" in Chinese doctrine see M. Taylor Fravel and Christopher P. Twomey, "Projecting Strategy: The Myth of Chinese Counter-Intervention," *The Washington Quarterly* 37, no. 4 (2015): 171–87. On CDD, escalation, and China see Forrest E. Morgan et al., *Dangerous Thresholds* (Santa Monica, CA: RAND Corporation, 2008); James Scouras, Edward Smyth, and Thomas G. Mahnken, "Cross Domain Deterrence in U.S.-China Strategy," Workshop Report (Laurel, MD: Johns Hopkins Applied Physics Laboratory, 2014).

[34] E.g., George Grafton Wilson, "Territorial Waters," *Proceedings of the American Society of International Law at Its Annual Meeting (1921-1969)* 22 (1928): 93–108.

[35] http://www.oxforddictionaries.com/us/definition/american_english/commons accessed 14 May 2016

liberal trading state, however, then its command of the sea is also meant to protect the free flow of trade, which can benefit others too.

By similar logic, proponents of a more proactive U.S. grand strategy often construe any military challenge to U.S. dominance (especially Chinese A2/AD) as an illegitimate attempt to contest the global commons safeguarded by the United States.[36] As the U.S. Chief of Naval Operations and the Air Force Chief of Staff wrote in 2012, "Free access to the ungoverned 'commons' of air, maritime, cyberspace and space is the foundation of the global marketplace….But this interconnectedness also makes the global economy more susceptible to disruption. The fragility of chokepoints in air, space, cyberspace and on the sea enable an increasing number of entities, states and non-state actors alike to disrupt the global economy with small numbers of well-placed, precise attacks." Admiral Greenert and General Schwartz continue with a barely disguised reference to China: "Autocratic states and groups seeking to subvert the prevailing political and economic order are already leveraging their geographic advantages to employ armed coercion and political action to counter American presence and power projection, as well as to disrupt free access to key areas in the air and maritime commons. As these revisionist strategies advance, America's friends will increasingly seek the security and stability provided by comprehensive U.S. national power."[37] Cross-domain operational concepts like "Air-Sea Battle" and freedom of navigation operations by the U.S. Navy assert access to common areas while denial of them constitutes a revisionist provocation. China, on the other side, protests American

[36] E.g., Abraham M. Denmark and James Mulvenon, eds., *Contested Commons: The Future of American Power in a Multipolar World* (Washington, DC: Center for a New American Security, 2010); Scott Jasper, ed., *Securing Freedom in the Global Commons* (Stanford, CA: Stanford University Press, 2010). Pursuit of liberal primacy in the face of threats to command of the commons is, ironically, the opposite of the implication drawn by Posen, who counsels restraint in contested zones.

[37] Jonathan W. Greenert and Norton A. Schwartz, "Air-Sea Battle," *The American Interest*, February 20, 2012, http://www.the-american-interest.com/2012/02/20/air-sea-battle/. "Comprehensive national power" is the usual translation of the Chinese concept of 综合国力.

intervention in its expanding littoral domain as an aggressive interference in its sovereign interests. The commons remain open, ironically, only as long as they are the domains of a liberal military hegemon.

Cyberspace is often included (e.g., in the 2005 NDS) alongside the sea, air, and space commons that Posen describes. Yet "command of the commons" would be particularly complicated in cyberspace, not least because cyberspace is not really a commons, as noted above. The complex structure of property rights over cyber resources and the voluntary nature of connection to them creates many new opportunities for deception and malicious behavior, complicates traditional governance schemes, and raises difficult strategic questions. Yet almost all cyber exploitation depends on the unwitting cooperation of the victim of deception, which incentivizes a degree of restraint.[38] The limits to domination in the cyber domain are still not well understood, which may be either a source of frustration or consolation for CDD efforts.

Space is another intellectually and pragmatically challenging domain. Space and cyberspace are often mentioned in the same breath and managed by the same bureaucratic policy shops. Cyberspace relies on space assets such as communication satellites that broadcast content and relay data and the Global Positioning System (GPS) used by most commercial mapping applications. Space relies on cyberspace insofar as satellites are computers in orbit networked to ground stations and to each other via radio links, and the primary utility of space is informational, providing remote imaging, intelligence collection, communication relay, and position, navigation, and timing services (e.g., GPS). Information infrastructure on Earth or in orbit is not useful in and of itself but because of its ability to command and control other things, which makes space and

[38] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–48; Jon R. Lindsay, *Shifting the Fog of War: Information Technology and the Politics of Control* (Book Manuscript, n.d.), chap. 7.

cyberspace inherently cross-domain. For the United States in particular and increasingly for other nations as well, the two domains provide the global nervous system that makes military operations in the other three domains possible. The leverage and sensitivity of global command and control systems also subjects space and cyber operations to extreme secrecy.

The Bush Administration's 2005 NDS noted that "as the nation's reliance on space-based systems continues to grow, we will guard against new vulnerabilities. Key goals, therefore, are to ensure our access to and use of space, and to deny hostile exploitation of space to adversaries."[39] The August 2006 U.S. National Space Policy maintained this provocative tone, stating that "Freedom of action in space is as important to the United States as air power and sea power" and directing the Pentagon to "Develop capabilities, plans, and options to ensure freedom of action in space, and, if directed, deny such freedom of action to adversaries." This policy was put to the test in January 2007 when China tested a direct ascent anti-satellite (ASAT) kill vehicle, destroying its own *Fengyun-1C* satellite in low earth orbit (LEO) and creating the largest orbiting debris cloud in history; it remains ambiguous whether this was an uncoordinated scientific test or a deliberate political signal. Nonetheless, this incident highlighted not only the vulnerability of spacecraft—especially those in LEO such as U.S. intelligence collection platforms—and the tremendous collateral damage potential of space warfare, but also the specter of differing national opinions regarding the escalatory nature of ASATs. In February 2008, just weeks after China and Russia began advocating at the United Nations (UN) for a ban on space weapons, the United States launched a RIM-161 Standard Missile 3 (SM-3) missile from the *USS Lake Erie*, a *Ticonderoga* class cruiser, in the central Pacific. Designed as a ballistic missile interceptor but suitable as an ASAT weapon, the SM-3 intercepted and destroyed a non-functional U.S. satellite. *Operation*

[39] "2005 NDS," 16.

Burnt Frost was ostensibly intended to prevent the spillage of toxic hydrazine fuel from the deorbiting spacecraft, but it prompted considerable speculation that it was also a deterrent signal from Washington to Beijing and Moscow. China conducted additional ASAT tests in the following years, this time designed to minimize the generation of debris. The Obama administration significantly toned down the rhetoric in its June 2010 *National Space Policy*, emphasizing goals like "Expand international cooperation," "Strengthen stability in space," and "Increase assurance and resilience of mission-essential functions." All the same, the vulnerability of vital space assets and the ambiguity of space signaling was and remains a serious CDD challenge and an essential consideration in any militarized crisis scenario involving the United States and China.[40]

Although space and cyberspace are often discussed together, they are radically different in many ways. Space is a harsh physical environment while cyberspace is constructed of arbitrary technical protocols. Heavy lift and satellite operations are extremely expensive, although barriers are falling with the advent of commercial space flight; while there are only a handful of spacefaring nations as a result, millions of individuals can own and design portions of cyberspace. Damaged or derelict satellites may take millions of dollars and many years to replace, but cyber infrastructure is continuously upgraded (the pace of change in cyberspace is notoriously rapid). These differences may simply highlight the incoherence of treating "cyberspace" per se as a commons or an independent domain, as noted previously, given the radically different material and economic qualities of the sociotechnical components that provide information services on land, under water,

[40] Michael Krepon and Julia Thompson, eds., *Anti-Satellite Weapons, Deterrence and Sino-American Space Relations* (Washington, D.C: Stimson Center, 2013); Brian Weeden, "Through a Glass, Darkly: Chinese, American, and Russian Anti-Satellite Testing in Space" (Secure World Foundation, March 2014), http://www.thespacereview.com/article/2473/1.

through the air, or in space. In any case, CDD must account for the strategically salient similarities and differences across these domains.

The Bush administration initiated, and the Obama administration continued, a number of different studies of the problem of CDD within the intelligence community, national nuclear weapons laboratories, STRATCOM, and the Office of the Secretary of Defense. One particularly noteworthy study in the context of this book was the *21st Century Cross Domain Deterrence Initiative* (CDDI), which was organized in early 2010 by Michael Nacht, lead author of chapter two in this volume, in his capacity then as Assistant Secretary of Defense for Global Strategic Affairs (ASD-GSA). ASD-GSA consolidated policymaking for U.S. nuclear forces, ballistic missile defense, space, and cyberspace. The CDDI invited a number of eminent scholars and experts from outside the DoD to reflect on the strategic challenges running through this diverse policy portfolio. Nacht's chapter summarizes some of the insights that emerged. The CDDI and similar efforts produced greater appreciation for the urgency and complexity of CDD, but a new strategic consensus regarding the best way forward remained elusive. As Shawn Brimley, a staff member in the office of Under Secretary of Defense for Policy Michèle Flournoy, observed in a 2010 article, "cross-domain deterrence dynamics will constitute a core analytic issue for the U.S. defense, diplomatic, and intelligence community, particularly as shifts in the actual or perceived balance of power in sea, air, space, and cyberspace become more opaque."[41]

[41] Brimley, "Promoting Security in Common Domains," 129.

<1>Exploring the Analytical Potential of CDD

If Brimley is right, then we have a major opportunity (and challenge) to reevaluate the foundations of strategic thought. This volume probes whether there is more to CDD than the fashion trends of Pentagon jargon or American paranoia about space, cyberspace, and China.

We posit that increasing sociotechnical complexity is the very problem which gives rise to CDD. The long-term growth of industrialization unlocks new resources but also requires more complicated institutions to coordinate social activity.[42] Military affairs have likewise undergone a competitive ratcheting up of complexity in recent centuries. Computer networks and autonomous robotics that improve warfighting are not sudden disruptions, but rather the most recent manifestations of a long-term trend toward more sophisticated sociotechnical control. Political actors have a growing number of ways and means for influence, with more emerging over time, yet because they act in a political system of other actors with similar opportunities, they also face increasingly complicated constraints on their choices. Strategic complexity, moreover, is as much political as it is technological. Unfortunately, most of the discussion of CDD and associated challenges in cyberspace, space or elsewhere tends to focus on the technological "cross-domain" problem rather than on the political "deterrence" problem. The literature on military innovation has reached a consensus that technological innovation by itself does not determine strategic or even tactical outcomes without the development of complementary doctrines and organizations to

[42] James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, MA: Harvard University Press, 1986); Douglass C North, *Institutions, Institutional Change, and Economic Performance* (Cambridge; New York: Cambridge University Press, 1990); Joel Mokyr, *The Gifts of Athena: Historical Origins of the Knowledge Economy* (Princeton University Press, 2002).

employ it. CDD thus cannot overlook the institutional circumstances of the policymakers and commanders who choose technological means to advance political ends.[43]

This book is, accordingly, divided into two substantive sections. The first focuses on the technological and the second on the political complexities of deterrence, but all of the chapters are suffused with concerns for both. Chapter contributors include scholars and practitioners with deep expertise in particular technologies, international relations, or defense policy. Indeed, an interdisciplinary approach is required to understand whether and how different technologies affect coercion in theory and practice. The conversation among them has been evolving for a couple of years under the auspices of the "Deterring Complex Threats" project, a five-year research program sponsored by the DoD Minerva Initiative to improve understanding of CDD, led by the editors of this book and Michael Nacht, former ASD-GSA, with the collaboration of experts at the Lawrence Livermore and Los Alamos National Laboratories. Many of the authors presented early drafts of their chapters at an academic conference held in November 2014 at the University of California San Diego. A subsequent workshop in May 2016 at the George Washington University reconvened many of the original participants in the aforementioned CDDI (hosted in 2010 by ASD-GSA), including some of the most eminent scholars of deterrence such as Thomas Schelling, George Quester, Morton Halperin, Robert Jervis, and Richard Betts, among others. The intent of this book is not to provide a finished theory of CDD, but rather to explore whether the concept provides any analytical traction in contemporary and historical cases or whether CDD helps to reveal any novel insights that a more general theory of means-based deterrence might incorporate.

---

[43] On military innovation see MacGregor Knox and Williamson Murray, *The Dynamics of Military Revolution, 1300-2050* (New York: Cambridge University Press, 2001); Adam Grissom, "The Future of Military Innovation Studies," *Journal of Strategic Studies* 29, no. 5 (October 1, 2006): 905–34. On the fallacy of technological determinism in general see Langdon Winner, *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought* (Cambridge, MA: MIT Press, 1977); Merritt Roe Smith and Leo Marx, eds., *Does Technology Drive History? The Dilemma of Technological Determinism* (Cambridge, MA: MIT Press, 1994)..

One important theme that spans this volume is that the emergence of CDD as a term postdates considerably the use of CDD in practice. The following chapter by Michael Nacht, Patricia Schuster, and Eva Uribe, "Cross-Domain Deterrence in American Foreign Policy," shows that CDD is not new, even if our awareness of it is. Prominent cases from the Cold War, such as the Korean War and the Cuban Missile Crisis, can be interpreted through a CDD lens and fruitfully compared with more contemporary cases like Stuxnet. These cases illustrate the variation across domains by the adversary and the U.S. responses. The authors find the United States generally responded to these crises by initially limiting itself to the domain where a crisis started and only later expanding into other domains. The United States. has generally been cautious when shifting domains and has tried to escalate in ways that would not produce adversarial retaliation.

Moving into the section on technological complexity, the next two chapters explore the inherently cross-domain problems of cyber and space warfare, the primary motivations for the policy articulation of CDD. "Deterrence in and through Cyberspace" by Jacquelyn Schneider argues that most of the discussion of cyber deterrence has been "riddled with ambiguity, uncertainty, and a lack of empirical precedent, which has trickled down to policies that remain largely unformed or partially implemented." Schneider reviews debates about the definition of cyber operations and cyber deterrence, distinguishing the use of cyberspace to support deterrence in other domains and the deterrence of actions within cyberspace itself. She finds that uncertainty is a resounding theme in this literature, which poses both challenges and opportunities for CDD. Cyber enabled military capabilities may both bolster U.S. deterrence policies and incentivize attack in a difficult paradox of capability and vulnerability.

"Anti-Satellite Weapons and the Instability of Deterrence" by Ben Bahney, Jonathan Pearl, and Michael Markey, all from the Lawrence Livermore National Laboratory, articulates a

logic of space control, emphasizing security competition between global and regional powers. U.S. military power projection is utterly dependent on space assets for command, control, communications, intelligence, and targeting, but they are increasingly vulnerable to ASAT capabilities including not only direct attacks on satellites but also indirect cyber and electronic warfare interference. Facing military confrontation with the United States, states would have strong incentives to use ASATs preemptively. Several cross-domain options are available for both deterrence by denial (the threat of effective defense) and by punishment (the threat of retaliation). Unfortunately, the lack of shared norms regarding space warfare has uncertain consequences for escalation dynamics. Similar to the cyber domain as described by Schneider, space deterrence faces challenging issues of credibility and attribution.

"Deterrence in War—Air Power Versus Ground Forces" by Phil Haun, Professor and Dean of Academics at the U.S. Naval War College and a former A-10 Thunderbolt II (a.k.a., "Warthog") pilot, identifies the conditions where air power is most lethal and therefore has the greatest effect on deterring ground forces. Haun thereby relaxes two major assumptions of classical deterrence theory. First, deterrence concepts were developed to prevent nuclear war, for obvious reasons, and thus tend to focus on high-stakes crisis bargaining, or "chicken" games. With additional means available, however, it is likely that deterrence may operate in many different games and with repeated interactions. This is especially the case in war itself, where many different platforms can be combined to constrain the battlefield choices of the enemy over the course of a campaign. Deterrence can operate at the tactical level even when a state is defending or attacking at the strategic level. Second, deterrence theorists usually emphasize the protection of the status quo, reserving the term compellence for revision. However, deterrence can be used as part of a broader compellent strategy, just as a shield supports the sword. Drawing on a number of historical

examples, Haun argues that command of the air over the battlefield deters ground forces from massing and maneuvering, which can support both offensive and defensive operations. The degree to which an air force can deter depends upon operational and environmental factors, including the degree of air superiority achieved over the battlefield; the capability of an air force to locate, identify, target, and assess air strikes against ground forces; the composition of enemy ground forces; and the presence and capability of friendly ground forces.

Many CDD technologies, notably in space and cyberspace, rely on secrecy to be effective, but secrecy can undermine the effectiveness of deterrent signals. “Signaling with Secrets—Evidence on Soviet Perceptions and Counterforce Developments in the Late Cold War” by Brendan Rittenhouse Green and Austin Long examine the problems of clandestine deterrence in the Cold War. They demonstrate that widespread strategic interaction across different domains with challenging secrecy constraints is not a new phenomenon. During the late Cold War, nuclear forces deterred conventional attack, theater nuclear forces deterred strategic nuclear escalation, and conventional threats to nuclear capabilities deterred conventional attack. Some of these capabilities, particularly intelligence collection and electronic datalinks, depended on sensitive tactics and technologies that could not be revealed lest the enemy develop countermeasures. This increased uncertainty about the true balance of power, which should have made conflict more likely according to rationalist theory. Green and Long show, however, that the United States was able to use several mechanisms to communicate its capabilities to the Soviet Union without totally compromising the ability to use them. Leveraging evidence from senior Soviet leadership, they argue that American counterforce nuclear strategy influenced Soviet perceptions and affected its policy across a variety of military and political domains.

Although the concept of CDD emerged as response to American concerns about Chinese A2/AD developments, Vladimir Putin's Russia subsequently emerged as one of its most adept practitioners. "Cross-Domain Coercion—The Current Russian Art of Strategy" by Dima Adamsky leverages Russian primary sources to explain how "Moscow incorporates non-military, informational, cyber, nuclear, conventional, and sub-conventional tools of strategic influence in an orchestrated campaign." Adamsky uses the term "cross-domain coercion" to emphasize, like Haun, that CDD can be used for revision as well as defense of the status quo; furthermore, Adamsky points out that the difference between the two is often in the eye of the beholder and misperception of an adversary's intentions remains a problem for CDD as much as, if not more than, traditional deterrence. Adamsky identifies a distinctly Russian approach to CDD that views nuclear weapons as an integral part of Russian operational art, emphasizes the integration of information operations with both nuclear and non-nuclear operations, "waged simultaneously on the digital-technological and on the cognitive-psychological fronts." The unconventional war in Ukraine which began in 2014 has provided a dramatic example of the challenges and opportunities of CDD for NATO and Russia. The recent crisis in Ukraine, especially the annexation of Crimea, offered Russia the most favorable conditions possible for cross-domain coercion because the balance of resolve strongly favored Russia over Western Europe. This suggests that the use of CDD for revisionist purposes may be affected by important scope conditions.

The book next transitions to an emphasis on the political complexity of CDD. As a segue, the first chapter in this section treats the "domains" of hoplites and triremes to underscore the point that CDD is not just about advanced 21st century technology. "New Concepts for Ancient Conflicts—Cross-Domain Deterrence in the Peloponnesian War" by Joshua Rovner asks whether the concept of CDD can shed any new light on one of the most famous wars in all of international

relations. Athens enjoyed unquestioned maritime superiority, Sparta was the dominant land power in ancient Greece, and both sides played to their competitive advantage. Rovner finds that CDD failed when both sides wanted it to succeed, but succeeded when both sides wanted it to fail. During the prewar crisis the two sides believed they could overcome their asymmetric disadvantages through alliances and arms racing. The disastrous first few years of the war proved these beliefs to be wrong, and both sides grudgingly admitted that cross-domain asymmetries were facts of life. Yet because neither side was willing to challenge the other on its favored domain, a decisive battlefield victory became impossible. Athens repeatedly tried to lure Sparta into fleet-on-fleet engagements, and Sparta repeatedly tried to bait Athens into pitched land battle. Neither side was able to engineer a decisive confrontation in its preferred domain that might have forced the other to capitulate. This novel interpretation of a classic case challenges an existing consensus of CDD as rapid, dynamic and destabilizing. Similar disparities at sea and on the continent in Asia for example, could ensure that any conflict between China and the United States is longer, more costly and less decisive than either side perhaps expects.

Taking a more radical view of the notion of a domain, some coercive means need not be military or technological at all and may have important advantages for precisely those reasons. "Asymmetric Advantage—Weaponizing People as Non-Military Instruments of Cross-Domain Coercion" by Kelly Greenhill discusses coerced migration as an alternative to military influence employed by some actors against more powerful democracies. The aims of coercively engineered migration vary tremendously and usually include political, military, and economic goals. A widely held belief in deterrence theory, first articulated by Thomas Schelling, is that compellence is harder than deterrence. Greenhill finds, however, that weak actors have often been able to successfully use coercive migration to compel stronger states to alter their policies. Initiators can use the

strategy of "capacity swamping", manipulating the target's physical ability to deal with the migration, or "political agitation" to change the behavior of the target by stoking and exploiting politics of the target state. Greenhill finds that liberal democracies are most vulnerable to this particular means of coercion, even as they have important advantages in other arenas. This non-traditional example of CDD shows convincingly that a difference in means in the right context can have a differential effect on the success or failure of coercion.

Deterrence depends, among other things, on the clear communication of a credible threat, which in turn assumes that the sender and the receiver speak the same language, so to speak. "International Law and the Common Knowledge Demands of Cross-Domain Deterrence" by James Morrow argues that the complexity of CDD is major barrier to establishing coordinated expectations about violations and consequences. For a system of CDD to work, actors must understand what actions will trigger a response, what the response might be, and how willing the responding actors are to actually respond. Any such system is likely to be less robust than Cold War nuclear deterrence because of the number of domains involved, constraints on revealing secret capabilities (which Green and Long demonstrate is challenging but not impossible), or even the identity of the challenger, and the availability of provocations that fall below the established threshold of response. Morrow recommends using an analogy to the law of war rather than nuclear deterrence to understand the possibilities of setting up a workable CDD regime. Morrow's analysis helps to explain why debate about norms for cyberspace and space has become such a hot topic in recent years.

An essential component in the implementation of any deterrence policy is the assurance of both allies and adversaries that one will indeed act as promised when a threshold is crossed, but assurance has received comparatively little attention in theory. "Extended Deterrence and

Assurance in Multiple Domains" by Rupal Mehta examines how the proliferation of domains might affect commitments to allies. Mehta draws on the precedent of the U.S. nuclear triad, where the advent of intercontinental and submarine-launched ballistic missiles dramatically altered U.S. deterrence commitments in East Asia and Western Europe. She is more pessimistic, however, about the plethora of capabilities emerging in the 21st century which enable allies and adversaries alike to engage in risky behavior while undermining American willingness to intervene overseas. Mehta concludes with policy implications for the United States and its alliance policies as well as the general evolution of extended deterrence strategies in an increasingly cross-domain system.

If new and different means have a differential effect on the political ends of deterrence, then one might also expect variation in political ends to highlight newly salient features of existing means. "Linkage Politics—Managing the End of the Cold War" by Joshua R. Itzkowitz Shifrinson asks whether shifts in a state's desired ends and available means carry different strategic risks. Political leaders often attempt to link different issues to offset bargaining weaknesses in any one of them alone, but what happens when their goals change? Shifrinson draws on newly available archival evidence to examine this problem in the case of American efforts to deter Soviet repression in Poland and East Germany at the end of the Cold War. In both cases U.S. policymakers used diplomatic reassurance and threats of isolation to shape Soviet policy as the United States pressed its newfound political interests in Eastern Europe rather than its traditional preoccupation with military affairs. Shifrinson finds that the very ambiguity of cross-domain actions, which Morrow and others highlight as a problem for deterrence, can in some situations enable actors to probe intentions and assess risks to avoid a more confrontational meeting engagement, playing for time to clarify one's own interests to better choose the means best suited for one's goals. A broader

diplomatic conception of CDD, moreover, highlights the potential of using financial, institutional, or other political moves to render military moves less attractive.

CDD concerns arise against the background of 21st century globalization, and while many stress the vulnerability and instability of interconnected infrastructure in space and cyberspace, by contrast a long tradition of theorizing in international relations highlights the stabilizing features of political and economic interdependence. "Globalization and the Multidimensionality of International Relations in East Asia" by Chin-Hao Huang and David Kang argue that, in some circumstances, it may be prudent to be aware of the multiplicity of domains in which a state interacts with another state. Situating the security domain alongside economic and social domains of interaction among countries is important for creating a full analysis of a state's priorities in a particular region, or with any particular other state. For example, the U.S. policy of "pivoting to Asia" showcases both the multidimensionality of U.S. preferences regarding China and the risk that priorities will be widely misunderstood. The pivot itself emphasized diplomacy first, followed by economic relations in the region and lifting pressure on the military dimension. However, the pivot is increasingly viewed as a purely military response to China's rise. Yet data on East Asian defense spending over twenty-five years appears to present a puzzle: by many measures, East Asian military expenditures have declined fairly significantly over the past quarter century. This finding appears starkly at odds with the conventional wisdom that Chinese bellicosity, its expenditure on A2/AD, and the U.S. reallocation of forces are driving up tension in the region.

The book concludes with reflections on the notion of CDD by two men with deep expertise in the practice and theory of deterrence, respectively. In "Simplicity and Complexity in the Nth Nuclear Era," Ron Lehman draws on his diverse experience in senior positions in the U.S. DoD, Department of State, White House, and Lawrence Livermore National Laboratory to compare,

contrast, and synthesize deterrence issues related to the emergence of new military technologies, with particular focus on the complex geometries of escalation. In "The Past and Future of Deterrence Theory," Patrick Morgan draws on decades of influential scholarship on deterrence, including several book projects examining the problems of complex deterrence after the Cold War, to evaluate the promises and pitfalls of CDD in the context of the historical evolution of deterrence theory.

A basic challenge for this new era of deterrence research is to render the increasing complexity of CDD analytically tractable, even for domains that have yet to be invented or imagined. The chapters in this book suggest both that CDD will continue to be an important defense policy problem in the 21st century, and that analytical insights gleaned from CDD have the potential to clarify and provide impetus to future thinking about deterrence and military strategy.

<1>Conclusion

Deterrence was not a new phenomenon at the dawn of the nuclear age, but the demand for theory about it was new. CDD is also not new, but its relevance is increasing. Strategic actors have long combined capabilities or shifted domains to make coercive threats or design around them. The stalemate of symmetric confrontation outside the gates of Troy ended with the asymmetric ruse of the Trojan Horse. Sun Tzu recognized that deception and misdirection was essential to the art of war long before Chinese hackers began sending phishing emails to American defense contractors. The British sank the French fleet in the Battle of the Nile rather than attempting to directly confront Napoleon's formidable army on land in Egypt. The United States deployed a naval blockade and used the threat of nuclear escalation to force the Soviet Union to reconsider its deployment of missiles to Cuba. Just as deterrence was simply an intuitive policy practice before the advent of

nuclear weapons, the choice of deterrent means has long been seen as either sufficiently intuitive in practice or so dense in its abstraction that there was no perceived need or willingness to articulate an explicit theory. Intuition may no longer be sufficient, however, given that technological development has increased available options and multiplied their interactions. Nor can CDD be treated as a purely technical question involving military expertise. Just as Clausewitz pointed out two centuries ago that war is politics by other means, the increase in the number of means complicates and integrates political issues with the military art. Nuclear weapons produced a radical historical change in the upper bound of political violence, prompted strategists to articulate novel theory for deterrence and further cementing military operations to national policy and politics. Increasing complexity in the entire portfolio of means now available now appears to necessitate the refinement of deterrence as both a military and political process. As the proliferating options available for coercion create more uncertainty and complexity, understanding CDD becomes a limiting factor for national security strategy.

The ability to manage complexity has become increasingly critical in military affairs with each passing decade of the modern era. The emergence of modern combined arms warfare in the First World War enabled military organizations to restore movement to an increasingly lethal battlefield.[44] Combined arms warfare works by using the advantages of one category of force to cover the weaknesses of another. Armor can provide fires and protection, even as it is vulnerable to other arms such as artillery and tactical aviation. As effective as this method of force employment is in battle, however, mastering the inherent complexity and accumulating the human and organizational capital required is beyond the reach of many states. Engineering systems

[44] Stephen D Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, N.J.: Princeton University Press, 2004).

integration is another complementary form of complexity management. Both work together to field the panoply of weapons and organizations that nations and even non-state actors need for "command of the commons." This brings us back to the problem with which CDD began, namely whether American cross-domain prowess is being undermined by developments in space, cyberspace, and other arenas and whether other American advantages might be brought to bear to compensate. One way to think about CDD is by analogy to the problem of combined arms warfare, but applied to the level of political strategy. Mastering combined arms operations assigned "winners" in combat in the twentieth century and allowed the United States to wield an effective form of dominance as hegemon. In the same way, making sense of the different political properties of different coercive instruments and their combinations may allow actors who master CDD to exercise increased influence in the future and restore the credibility of deterrent policies undermined by technological innovation. There will be technological changes that create new threats in the future that are hard to imagine now; instead of reacting piecemeal to each new threat or capability, a strategic policy designed explicitly to confront the problem of continuously increasing socio-technical complexity would make it easier to accommodate, even anticipate, novel threats. The question is to what extent that level of policy sophistication can be achieved through deductive intuition or requires greater experience.

As with classical deterrence, a theory of CDD should link the technical ability to harm with the political utility of aggression. CDD can and should look to familiar deterrence principles. What differs is the technological and political context of bargaining. Traditional deterrence theory is agnostic about means (usually assuming the means are nuclear), but choice among means is essential for CDD. Deterrence theory, furthermore, rests on the notion of political bargaining between broadly rational actors, and it is desirable to retain this paradigm to first capture the logic

of optimal choice before later examining non-rational deviations. The basic bricks and mortar for a theoretical perspective on CDD are in reach by conceiving of social institutions as a type of bargaining equilibrium between agents in a political system and war as a type of bargaining failure.[45] There are countless institutions that regulate social behavior in any system, some formal and some informal. When novel technological and political developments alter participants' bargaining power, beneficiaries may be tempted to renegotiate while others resist change as disadvantageous. Disagreements about the effects of change can lead to war. The disruptive technologies of CDD which differentially affect various capabilities, linkages, and actors are precisely the kinds of developments destined to prompt bargaining failures.

A basic question underlying these efforts is whether CDD—and sociotechnical complexity more generally—is fundamentally destabilizing. Many people certainly think so. Emerging technologies seem, by some accounts, to advantage opportunistic attackers, weaker actors, and challenges to the status quo. Interdependent infrastructures create grave vulnerabilities for all, especially strongest and wealthiest states. The growing number of potential threats from ever more state and non-state actors complicates the choice of strategy. However, the opposite might be the case. Some asymmetric capabilities reinforce the status quo, while economic interdependence, a form of complexity common in recent times, is generally thought to be pacifying. More and more actors have a stake in the current global system. Better theory and policy approaches should aim to resolve or at least clarify these controversies.

[45] James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (1995): 379–414; R. Harrison Wagner, *War and the State: The Theory of International Politics* (University of Michigan Press, 2010).