NAVIGATING DETERRENCE: LAW, STRATEGY, AND SECURITY IN THE TWENTY-FIRST CENTURY

ZACHARY K. GOLDMAN

Deterrence, the dominant approach governing the security relationship between the United States and the Soviet Union during the Cold War, is both a set of theories and related strategies for the management of threats. At a theoretical level, deterrence, specifically employing nuclear weapons, helped shape the development of political science during the Cold War, and the applications of game theory and other structures to the study of international relations.[1] At the level of national security strategy, Cold War era deterrence studies helped policy-makers to understand better the role that nuclear weapons would play in the evolving post-World War II international security environment.[2] These academic engagements helped enhance understanding of the ways in which deterrence could be used to manage security relations in a dynamic environment, and to build appropriate force structures and military doctrines. It also helped policymakers to conceptualize the ways in which nuclear weapons and conventional arms could be thought of as part of a coherent approach to risk management. Mutually assured destruction was in some respects the apotheosis of the logic of deterrence, and after that concept was articulated early in the Cold War, significant advancements were made in the understanding of deterrence and in the weapons systems needed to implement it.[3]

Deterrence is the act of influencing an adversary's cost/benefit calculations to prevent him from doing something that you do not want him to do,[4] and as that deceptively simple definition suggests, it has a wide range of applications outside the nuclear strategy realm. As the Cold War ended, however,

[1] *See, e.g.*, THOMAS C. SCHELLING, THE STRATEGY OF CONFLICT (1960); HERMAN KAHN, ON THERMONUCLEAR WAR (1961).

[2] *See, e.g.*, Albert Wohlstetter, *The Delicate Balance of Terror*, 37 FOREIGN AFF. 211 (1959); HENRY KISSINGER, NUCLEAR WEAPONS AND FOREIGN POLICY (1957).

[3] LAWRENCE FREEDMAN, DETERRENCE (2004).

[4] *See* PHILIP BOBBITT, DEMOCRACY AND DETERRENCE: THE HISTORY AND FUTURE OF NUCLEAR STRATEGY 9 (1988).

scholars and practitioners questioned the continued relevance of the concept. And immediately after the terrorist attacks of 9/11, deterrence lost its salience as a principal component of the U.S. Government's security strategy, having been replaced in the 2002 National Security Strategy by paradigms of preemption and prevention.[5] But in the post-Cold War, post-9/11 world, ideas about the relevance of deterrence have been revived and revised.[6]

Deterrence, far from being a static and monolithic concept, is actually comprised of a cluster of related ideas that, together, determine whether and to what extent a defender can shape the cost/benefit calculations of a challenger. Key to the actualization of deterrence is the ability of a defender to communicate effectively a credible threat to deploy capabilities against a challenger to achieve an objective.[7] Concepts that are important to the operation of effective deterrence strategies include rationality.[8] And it is equally critical that

[5] THE WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 15 (2002) ("Traditional concepts of deterrence will not work against a terrorist enemy whose avowed tactics are wanton destruction and the targeting of innocents; whose so-called soldiers seek martyrdom in death and whose most potent protection is statelessness.").

[6] Kathleen H. Hicks, *The Case for Deterrence*, *in* CTR. FOR STRATEGIC & INT'L STUDIES, 2015 GLOBAL FORECAST 10, 11 (Craig Cohen & Josiane Gabel eds., 2014) ("In the coming year, deterrence will be an aspect of virtually all of our security dealings.").

[7] T.V. Paul, *Complex Deterrence: An Introduction*, *in* COMPLEX DETERRENCE 1, 2 (T.V. Paul et al. eds., 2009) [*hereinafter* T.V. Paul].

[8] Rationality in this context is conceptualized as determinations about whether political decisionmakers can perceive communications from others and internalize them in decisionmaking processes. *See, e.g.*, PATRICK M. MORGAN, DETERRENCE (1977) (discussion in chapter 4); PATRICK M. MORGAN, DETERRENCE NOW (2003) (discussion in chapter 2). The problem in the Cold War context was captured by Keith Payne, who described the inability to have "confidence that challengers will reliably observe the nuclear balance, recognize and believe U.S. demonstrations of will, understand the situation, calculate rationally, and then be deterred, is . . . inadequate . . . , for even the most brilliantly presented deterrence threat may be discounted or misunderstood by a challenger." KEITH B. PAYNE, THE FALLACIES OF COLD WAR DETERRENCE AND A NEW DIRECTION 31 (2001). Janice Gross Stein and Richard N. Lebow also did pathbreaking work demonstrating that "existing theories of deterrence are incomplete and flawed . . . . Theories of deterrence do not consider the most important determinants of strategic choice. These determinants are outside of and at times contradictory to their fundamental as-

scholars and strategists keep clear the distinctions between deterrence and cognate influence strategies like compellance.[9]

As the articles in this volume demonstrate, deterrence and the core concepts of which it is comprised are as relevant as ever to the management of persistent security threats, even as the threats themselves have evolved from the bipolar nuclear standoff between the United States and the Soviet Union that animated the Cold War.[10]

Indeed, in the last several years, government officials faced with significant security threats consistently have spoken in the language of deterrence as they sought to mitigate the challenges posted by rogue states, humanitarian crises, and cyber threats, among others.

In March 2011, for example, President Obama said, in the face of significant violence against Libyan civilians, that "Moammar Qaddafi has a choice. . . . If Qaddafi does not comply with [UNSCR 1973] the resolution will be enforced through military action."[11] President Obama used the warning of military force to dissuade Qaddafi from committing a massacre that the Libyan dictator had threatened against the city of Benghazi. So too during Israel's last two conflicts in Gaza, in November 2012 and during the summer of 2014, did Israeli government officials speak about their objectives in terms of "restoring deterrence" vis a vis Hamas and other terrorist groups in Gaza.[12] The government's goal was to halt the

sumptions." Richard N. Lebow & Janice G. Stein, *Rational Deterrence Theory: I Think, Therefore I Deter*, 41 WORLD POLITICS 208, 208 (1989).

[9] Compellence is the use of threats or force to alter the status quo in some way. The classic discussion is found in THOMAS SCHELLING, ARMS AND INFLUENCE 70-73 (1966).

[10] *See generally* Richard K. Betts, *The Lost Logic of Deterrence*, 92 FOREIGN AFF. 87 (2013); Suzanne Nossel, *Obama Needs to Find His Inner Cold Warrior*, FOREIGN POLICY (June 25, 2014), http://www.foreignpolicy.com/articles/2014/06/25/obama_needs_to_find_his_inner_warmonger_iraq_syria_deterrence; CRAIG COHEN & JOSIANE GABEL, CTR. FOR STRATEGIC & INT'L STUDIES, 2015 GLOBAL FORECAST: CRISIS AND OPPORTUNITY (2015).

[11] President Barack Obama, Remarks by the President on the Situation in Libya (Mar. 18, 2011) (transcript available at http://www.whitehouse.gov/the-press-office/2011/03/18/remarks-president-situation-libya).

[12] Jonathan Ferziger, Gwen Ackerman & Elliott Gotkine, *Barak Says Israel to Hit Hamas Until Deterrence Restored*, BLOOMBERG (Nov. 13, 2012), http://www.bloomberg.com/news/articles/2012-11-13/barak-says-israel-will-hit-hamas-until-deterrence-is-restored; Haaretz, *LIVE UPDATES: Operation*

rocket fire from Hamas-controlled territory into Israel by raising the price for Hamas and others of repeated rocket attacks. And in Syria, President Obama famously said that "chemical weapons moving around or being utilized" was a "red line" that would change his calculus about American intervention in the civil war there, implying that if President Assad crossed that line, unacceptable consequences would follow.[13]

But even as deterrence currently forms a central part of the way that officials are thinking about managing a wide range of threats, it is clear that there have been difficulties in the translation of classical thinking about deterrence into practical strategies to manage contemporary security problems.

Indeed, in the cases cited above, political leaders did not implement military strategies that were able to effectuate their stated objectives of deterring undesirable conduct. In Libya, for example, what began as an effort to deter Qaddafi from committing a massacre quickly evolved into a military operation that unseated the regime and led to his death. The United Nations also referred the situation in Libya to the International Criminal Court.[14] The net effect of these actions was not to change Qaddafi's cost/benefit calculations and convince him to abandon his objectives. Rather they potentially convinced him that he had no choice but fight to the end or to capitulate unconditionally to the international coalition, violating Thomas Schelling's cardinal principle, "To be coercive, violence has to be anticipated. And it has to be avoidable by accommodation. The power to hurt is bargaining power. To exploit it is diplomacy."[15]

If the primary goal of the international community's intervention had been to deter Qaddafi from perpetrating atrocities against civilians, it would have needed to leave space for him to accommodate its demands while avoiding the imposition of consequences—an outcome that likely would have required the international community to be satisfied with Qad-

Protective Edge, Day 26, HAARETZ (Aug. 3, 2014), http://www.haaretz.com/news/diplomacy-defense/1.608426.

[13] Mark Landler, *Obama Threatens Force Against Syria*, N.Y. TIMES, Aug. 20, 2012, http://www.nytimes.com/2012/08/21/world/middleeast/obama-threatens-force-against-syria.html?_r=0.

[14] S.C. Res. 1970, ¶ 4, U.N. Doc. S/RES/1970 (Feb. 26, 2011).

[15] SCHELLING, *supra* note 9, at 2.

dafi's continued rule. Instead, however, objectives other than deterrence dictated the scope and goals of the military campaign. The scope of the intervention ultimately was defined by the relevant U.N. Security Council Resolutions, which limited the goals that the international community was able to pursue to the "protection of civilians." Targets that Qaddafi valued most highly that might have been held at risk if the primary goal had been to deter him were, therefore, likely excluded from the political or legal bounds of the intervention.

In the circumstances of the Libya case Qaddafi's use of violence against the Libyan people foreclosed any outcome that would have accommodated his continuation in power, and thus, any effort to deter him was unlikely to be successful. As President Obama said two weeks before the military campaign in Libya began, "Muammar Qaddafi has lost the legitimacy to lead, and he must leave," because of his "appalling violence against the Libyan people."[16] Indeed, it is important to note as a general matter that strategies of preemption or regime change might make "deterrence failure more likely."[17] The political/military strategy that the international community pursued, therefore, while initially framed as an exercise in deterring the commission of crimes against civilians, was implemented as something altogether different.

So too, when the United States contemplated intervening in Syria in the fall of 2013 in response to Bashar al-Assad's use of chemical weapons, did it speak about different goals. Some senior officials spoke clearly about deterrence, as when General Martin Dempsey testified, "The task I've been given is to develop military options to deter—that is to say, change the regime's calculus about the use of chemical weapons and degrade his ability to do so."[18] Other officials seemed to mix deterrence of the future use of chemical weapons with other goals—upholding international norms, and more thorough degradation of his capacity to conduct future chemical strikes

[16] Mark Landler, *Obama Tells Qaddafi to Quit and Authorizes Refugee Airlifts*, N.Y. TIMES, Mar. 3, 2011, http://www.nytimes.com/2011/03/04/world/africa/04president.html.

[17] Jeffrey W. Knopf, *The Fourth Wave in Deterrence Research*, 31 CONTEMP. SECURITY POL'Y 1, 7 (2010).

[18] Carol Lee, Janet Hook & Julian Barnes, *Support Builds in Congress for U.S. Strike Against Syria*, WALL ST. J. (Sept. 4, 2013), http://www.wsj.com/articles/SB10001424127887324432404579053344262636248.

(as opposed to altering his cost/benefit calculations about whether or not to do so).[19]

While these goals are not mutually exclusive, they do suggest different military and targeting strategies. If the primary purpose of the intervention would have been to deter the future use of WMD, military planners would have focused on identifying and targeting assets that Assad valued highly in order to raise the costs to him of the contemplated future use of WMD. While this target set likely would have comprised the units or equipment employed to use chemical weapons (if not the chemical weapons themselves), it also could have included a broader set of targets that Assad valued highly, and which would have altered his cost/benefit calculations if held at risk by the United States and its allies. An example of such a target is the Hezbollah units that reportedly constitute some of the Syrian regime's most skilled fighters, but who are not necessarily connected directly to the WMD program.[20] Attempts to hold at risk targets that Assad holds dear might also have included the Iranian sources of support for the regime. If, however, the military objective would have been only to punish Assad for the use of chemical weapons, or to prevent him from using them in the future, the rationale for limiting any military intervention to targets linked in some way to WMD would have been much stronger.

These examples illustrate some of the difficulties involved in applying traditional deterrence thinking to the types of threats that predominate today, as opposed to a potential nuclear exchange between superpowers. These include threats in cyberspace;[21] the threats posed by crimes against humanity and rogue behavior; threats from terrorist groups; the threat posed by regional nuclear powers;[22] and even questions about

[19] George Stephanopoulos, *'This Week' Transcript: Secretary of State John Kerry*, ABC NEWS (Sept. 1, 2013), http://abcnews.go.com/ThisWeek/week-transcript-secretary-state-john-kerry/story?id=20123604&singlePage=true.

[20] Jim Michaels, *Assad Regime Relying on Foreign Militias, Fighters*, USA TODAY, Apr. 1, 2014, http://www.usatoday.com/story/news/world/2014/04/01/assad-regime-local-militias-foreign-fighters/7116509/.

[21] MARTIN LIBICKI, CYBERDETERRENCE AND CYBERWAR (RAND Corp. 2009).

[22] VIPIN NARANG, NUCLEAR STRATEGY IN THE MODERN ERA: REGIONAL POWERS AND INTERNATIONAL CONFLICT (Princeton Univ. Press 2014).

the continued efficacy of the U.S. nuclear force,[23] among others. The Cold War saw, over time, an extensive body of academic literature and strategic plans developed to avoid superpower conflict. But as the types of conflict, and the actors involved in them, have changed in the post-Cold War world, "there have only been a handful of book-length studies on [deterrence] . . . undertaken by international relations scholars who explored the theory and practice of deterrence beyond a bipolar setting."[24]

More to the point, there are challenges in applying the core elements of deterrence—the communication of threats to parties that can receive and act upon them—to the types of threats that are the primary concern of policy-makers today. This is in part because the threats themselves have changed significantly from the bipolar world of the Cold War,[25] and in part because deterrence, with the demise of the Soviet Union, seemed more to be an "occasional stratagem rather than a constant, all-purpose stance,"[26] as the discussions of the approaches to Libya and Syria above demonstrate.

As a result of these changes, a "Fourth Wave" in deterrence research has developed in the last several years, the primary characteristics of which are "a change from a focus on relatively symmetrical situations of mutual deterrence to a greater concern with what have come to be called asymmetric threats" and "a broader concept of deterrence that is not exclusively military in nature."[27] Two of the richest areas of research in the more recent deterrence scholarship focus on deterrence in counterterrorism and in cyberspace, which have been identified by policymakers as key areas of strategic concern in the post-9/11 era.[28]

In counterterrorism, significant progress has been made since the immediate aftermath of the 9/11 attacks, when classic concepts of deterrence were thought to be very difficult to

[23] Keir A. Lieber & Darryl G. Press, *The New Era of Nuclear Weapons, Deterrence, and Conflict*, 7 STRATEGIC STUD. Q. 3 (2013).

[24] T.V. Paul, *supra* note 7, at 20.

[25] Knopf, *supra* note 17, at 2.

[26] FREEDMAN, *supra* note 3, at 76.

[27] Knopf, *supra* note 17, at 1.

[28] *Worldwide Threat Assessment of the US Intelligence Community before the Senate Armed Serv. Comm.*, 113th Cong. (2014) (statement of James R. Clapper, Director of National Intelligence).

apply to counterterrorism.[29] How, it was asked in the early post-9/11 period, can you manipulate the cost/benefit calculations of people who were prepared to give up their lives in order to conduct an attack? At that time, and for several years afterwards, "deterrence . . .[was] a poorly understood and underutilized element of U.S. counterterrorism strategy," and of counterterrorism research more broadly.[30]

Over a decade after the attacks, scholars and practitioners substantially have advanced their understanding of this and related questions.[31] They have done so by focusing on different ways of manipulating the cost/benefit calculations of targets, including deterrence by denial, in which a challenger is deterred from a course of action when a defender employs measures that make a successful attack less likely. These deterrence strategies received comparatively less attention in Cold War studies of the discipline.[32] But scholars also have developed new approaches to deterrence like "deterrence by delegitimization,"[33] the objective of which "is to reduce the challenger's probability of achieving his goals by attacking the legitimacy of the beliefs that inform his behavior."[34] This approach recognizes the different types of objectives that Islamist terrorist groups seek, and potential ways of raising the costs to them of pursuing those objectives.

A core insight in the adaptation of deterrence to counterterrorism is that terrorist networks are comprised of

[29] PAUL K. DAVIS & BRIAN MICHAEL JENKINS, DETERRENCE & INFLUENCE IN COUNTERTERRORISM: A COMPONENT IN THE WAR ON AL QAEDA (RAND Corp. 2002).

[30] Matthew Kroenig & Barry Pavel, *How to Deter Terrorism*, 33 THE WASHINGTON Q. 21, 22 (2012).

[31] *See, e.g.*, Robert F. Trager & Dessislava P. Zagorcheva, *Deterring Terrorism: It Can be Done*, *in* CONTENDING WITH TERRORISM: ROOTS, STRATEGIES, AND RESPONSES 229 (Michael E. Brown et al. eds., The MIT Press 2010); *Deterring Terrorism: Theory and Practice* (Andreas Wenger et al. eds., Stanford Univ. Press 2012).

[32] John Gearson, *Deterring Conventional Terrorism: From Punishment to Denial and Resilience*, 33 CONTEMP. SECURITY POL'Y 171, 193(2012).

[33] Alex S. Wilner, *Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism*, 34 J. OF STRATEGIC STUD. 3, 26 (2011); *see also* Marisa L. Porges, *Getting Deradicalization Right*, Letter to the Editor, 89 FOREIGN AFF. 155 (2010); Jessica Stern, *Mind Over Martyr: How to Deradicalize Islamist Extremists*, 89 FOREIGN AFF. 95 (2010).

[34] Wilner, *supra* note 33, at 26.

different components, some of which may be more deterrable than others (i.e., that financiers, many of whom have "legitimate" businesses and who are sensitive to reputation might be more deterrable than suicide bombers).[35] This disaggregation of terrorist networks into those for whom coercion can be effective and those for whom only strategies of prevention and disruption will work made its way into national security strategy at the highest levels. During the campaigns in Iraq and Afghanistan, for example, General David Petraeus often spoke of the distinctions between insurgents that were "reconcilable," and who could be dissuaded from participating in violent activities,[36] and the "irreconcilables . . . foremost among [whom] are al-Qaida Iraq and their affiliates" who must be "tenaciously and relentlessly" pursued.[37]

So too in cybersecurity have there been challenges as scholars and practitioners struggle to adapt well-established Cold War theories to a new "domain" of conflict. The first challenge in developing effective strategies for deterrence in cyberspace is conceptual: What exactly are the harms that we are trying to deter? The possibility of cyber war, in the sense of cyber activities that cause significant physical destruction and/or loss of life, exists, to be sure. An act of "cyber war" is what former Secretary of Defense Leon Panetta meant when he spoke of the potential for a "cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability."[38]

It is often argued, however, that there has only been one "possibly violent cyber attack to have taken place in the wild—Stuxnet[,]" the cyber attack on Iranian centrifuges,[39] and that

[35] Davis & Jenkins, *supra* note 29, at 14.

[36] Ernesto Londono & Thomas E. Ricks, *Petraeus Says Boost in Troops May Be Needed Past Summer*, Wash. Post Mar. 9, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/03/08/AR2007030802015.html.

[37] *Petraeus Lauds Iraq Violence Fall*, BBC News (Dec. 21, 2007), http://news.bbc.co.uk/2/hi/middle_east/7155628.stm?MobileOptOut=1.

[38] Leon E. Panetta, U.S. Secretary of Defense, Keynote Address to the Business Executives for National Security: "Defending the Nation from Cyber Attack" (Oct. 11, 2012).

[39] Thomas Rid, Cyber War Will Not Take Place 32 (2013). For an extensive discussion of the Stuxnet operation, see David Sanger, Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power (2012).

the vast majority of malicious cyber activity can be conceived of as something else—in Thomas Rid's framing, a combination of espionage, sabotage, or subversion.[40] While all three types of cyber activities are common, it is in fact financially-motivated cyber theft (or, more accurately, cyber-enabled theft) that constitutes perhaps the most prevalent type of cyber incident.[41]

Is this kind of criminal activity deterrable? Is the less prevalent but still potential act of cyber war deterrable? A persistent problem in the deterrence of cyber attacks is the "attribution problem," that is, the difficulty of knowing with confidence who is the actual perpetrator of an attack given how easy it is to mask one's physical location when conducting cyber operations. If one does not know who is actually conducting the attacks, then it will be difficult to tailor responses to them that can actually affect the cost/benefit calculations of the perpetrators. An additional challenge inheres in the large range of parties that are the actual or potential victims of cyber attacks—entities that range from government intelligence agencies to some of the largest defense contractors, and from large national retail companies, to small businesses all over the United States.

A further issue complicating the ability to establish effective deterrence relationships in cyber space pertains to secrecy. As noted above, deterrence is grounded in the ability effectively to communicate threats to challengers so that they can re-calibrate their cost/benefit calculations with respect to contemplated action. Secrecy in cyber activities poses a dual

[40] RID, *supra* note 39, at 32.

[41] See, for example, VERIZON ENTERPRISE SOLUTIONS, 2014 DATA BREACH INVESTIGATIONS REPORT 9 (2014), for one of the most authoritative reports on the scope, features, and motivations of cybersecurity incidents. For reports of specific breaches, see Jia Lynn Yang & Amrita Jayakumar, *Target Says Up to 70 Million More Customers Were Hit by December Data Breach*, WASH. POST, Jan. 10, 2014, http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html; Jessica Silver-Greenberg, Matthew Goldstein & Nicole Perlroth, *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES, Oct. 2, 2014, http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_r=0; Robin Sidel, *Home Depot's 56 Million Card Breach Bigger Than Target's*, WALL ST. J., Sept. 18, 2014, http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.

threat to that paradigm. First, states have generally tended to cloak their capabilities for the development of cyber intrusion tools behind a mantle of extreme secrecy. This inhibits the ability of a defender to communicate to potential challengers the nature of the consequences that may be visited upon them if the challenger proceeds with a course of action. But there is a second sense in which secrecy is important in cyber strategy, related to the computer vulnerabilities whose exploitation is the avenue for a complex cyber operation.[42]

Specifically, the ability to compromise an adversary's system depends upon a vulnerability in that system that is unknown to the adversary, and which the adversary has not patched. There is an active ongoing debate about whether the U.S. government, when it learns of vulnerabilities, should have a policy of disclosing that flaw to the software or hardware manufacturer so it can be patched.[43]

While this debate is important from the perspective of computer security more broadly, scholars like Martin Libicki have pointed out the implications of this discussion for the ability to deter potential adversaries through the brandishment of cyber capabilities. Defenders generally cannot reveal the specific nature of their cyber capabilities because to do so would enable potential challengers to patch vulnerable systems, rendering the defenders' capabilities ineffective. But, neverthelesss, the knowledge by challengers that potential defenders have such sophisticated capabilities may be sufficient to cloud with uncertainty and doubt the challengers' own confidence in the integrity and availability of their weapons systems to refrain from attacking.[44] Such novel conceptions of

[42] MARTIN C. LIBICKI, BRANDISHING CYBERATTACK CAPABILITIES 22 (RAND Corp. 2013).

[43] Jack Goldsmith, *Cyber Paradox: Every Offensive Weapon Is a (Potential) Chink in Our Defense—and Vice Versa*, LAWFARE, Apr. 12, 2014, http://www.lawfareblog.com/2014/04/cyber-paradox-every-offensive-weapon-is-a-potential-chink-in-our-defense-and-vice-versa/; Andrea Peterson, *Why Everyone is Left Less Secure When the NSA Doesn't Help Fix Security Flaws*, WASH. POST, Oct. 4, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/04/why-everyone-is-left-less-secure-when-the-nsa-doesnt-help-fix-security-flaws/; Bruce Schneier, *Should U.S. Hackers Fix Cybersecurity Holes or Exploit Them?*, THE ATLANTIC, May 19, 2014, http://www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploit-them/371197/.

[44] LIBICKI, *supra* note 42, at 8.

the way deterrence might operate, as well as a renewed focus on the parameters of deterrence by denial,[45] will likely form the basis for a cyber deterrence strategy moving forward. So too will the United States and its allies be able more effectively to deter financially motivated malicious cyber activities, which may be more susceptible to cost/benefit manipulations.

***

These are the debates into which the articles in this volume wade, as they are each focused on the ways in which traditional understandings of the theory and practice of deterrence are being adapted to new security environments.

Austin Long problematizes many of the assumptions that govern the juxtaposition of the "classical" era of Cold War deterrence with the new approach to the problem. He argues, most importantly, that the fundamental view of the Soviet Union as a "risk averse" and "status quo" power, embedded in Cold War deterrence thinking, was in fact contested during the period. Long points out that the Cold War status quo was in important respects negotiated between the two superpowers, and also critiques the idea that mutually assured destruction was accepted by both sides as the stable (or even desirable) basis for the status quo. Finally, Long turns his attention to two issues—the importance of credibility in deterrence thinking, and the ways in which clandestine capabilities affect the ability of defenders to deter threats. Long's essay prompts modern deterrence thinkers to consider the ways in which some of the core components of deterrence as a threat management strategy might need to be rethought in response to newly-uncovered evidence regarding the ways in which the U.S. government actually understood Soviet behavior during the Cold War.

The next three essays in the volume analyze different aspects of deterrence in the context of counterterrorism.

Alex Wilner's contribution builds on the substantial work he has already done on new ways to understand the requirements for effective deterrence in counterterrorism.[46] Wilner's

[45] David Elliott, *Deterring Strategic Cyberattack*, 9 IEEE SECURITY & PRIVACY 36 (2011).

[46] WENGER, *supra* note 31.

essay aims to situate deterrence in the counterterrorism context within the broader renaissance in deterrence thinking experienced in the last several years, and to "highlight both the promises and pitfalls of deterring terrorism while commenting more broadly on the manner in which deterrence theory has been re-imagined and repackaged in recent decades."[47] Wilner first calls attention to the fact that attempts to reorient deterrence to address counterterrorism challenges generally embrace a broader definition of the term than was prevalent during the Cold War. This is consistent with the broader range of actors and activities that have been implicated in the project of deterring terrorist groups, and the broader range of interests on which defenders have focused in their attempts to dissuade terrorist groups from attacking. Those focused on deterring terrorism have also disaggregated the relevant groups into their constituent parts, and have tailored their energies differently to different components of terrorist networks. As a consequence of broadening both our understanding of deterrence and the targets of deterrent efforts, Wilner notes that the scholarly and policy communities also have derived a broader range of "coercive processes" to apply to terrorism threats. He also points out some of the problems with the current approach, such as the elision of conceptual distinctions between deterrence, and related concepts like military victory.

The next two essays, by Janice Gross Stein and Ron Levi, and by Jackie Ross, combine modes of reasoning about deterrence from criminal law with insights from political science, to arrive at new understandings about deterrence in counterterrorism. This is particularly important as the units of analysis of deterrence thinking in political science shift from their predominant focus on nation-states to individuals and small groups. It is also important because criminology has access to substantially more empirical data about the impact of different deterrence strategies available to it than political science, and also a series of natural experiments that can be derived from observing the results of different policing strategies adopted by otherwise similar jurisdictions.

[47] Alex Wilner, *Contemporary Deterrence Theory and Counterterrorism: A Bridge Too Far?*, 47 N.Y.U. J. Int'l L. & Pol. 439, 442 (2015).

Stein and Levi focus on deterrence by denial as a distinct strategy for mitigating the risk of terrorist attacks, identifying both the underlying logic of deterrence by denial as well as some of the challenges inherent in a shift to deterrence by denial as an approach to counterterrorism. In doing so, they also draw on criminological literature to identify the factors that contribute to effective deterrent strategies. Particularly important for Stein and Levi are the social, procedural justice, and other community-based factors that reduce the rewards accruing to those who participate in terrorism as an essential component in understanding how to deter terrorism.

Jackie Ross devotes her attention to a comparative analysis of European and American approaches to undercover policing and the implications that these differences have for the ability to infiltrate and deter terrorist groups. Ross argues that concerns about entrapment, which limit investigatory options in Europe to a greater degree than in the United States, might limit the extent to which law enforcement and intelligence services will be able to use those operations to disrupt terrorism. Such undercover operations are often a part of strategic efforts to deter terrorist groups, injecting doubt into potential recruits as to whether they are in discussions with genuine members of terrorist groups or rather members of a law enforcement agency. The fate of this practice may, then, shape the availability of a traditionally important tool for deterring terrorism.

Finally, Paul Davis focuses on the complex and important discussion about the possibilities—and limits—of adapting deterrence theory to govern risk and operations in cyberspace. Davis first identifies deterrence an element—but only an element—of broader strategic approaches to strategic planning and decision-making in crisis and non-crisis environments. He then disaggregates the similarities and differences between "classic" deterrence and its application to cyberspace, and outlines how fears about escalation through the use of cyber capabilities might actually play out, coupled with a model for decision-making in situations of crisis.

In focusing the volume on deterrence, the objective was to enhance the analytical tools available for managing an increasingly crowded threat landscape. The threats posed by ISIS and other globally networked terrorist groups, cyber attacks, and regional nuclear powers might be new, but the frameworks needed to understand them, and manage the risks they pose, are not. Deterrence as an analytical framework has been part of the Western canon since the Bible. And while the threat landscape might be as diverse as it has ever been in the last fifty years,[48] the conceptual distinctions between the different means of threat management—between defeat, deterrence, and compellance, among others—remain constants. The work of adapting these ideas to specific threats will continue, with the contributions of those authors with whom we were lucky enough to work for this edition of JILP.

[48] James R. Clapper, Director of National Intelligence, Remarks as delivered by The Honorable James R. Clapper, Director of National Intelligence, IATA – AVSEC World, Oct. 27, 2014, *available at* http://www.dni.gov/index.php/newsroom/speeches-and-interviews/202-speeches-interviews-2014/1127-remarks-as-delivered-by-the-honorable-james-r-clapper-director-of-national-intelligence.