ARTICLES

COUNTERTERRORISM AND NEW DETERRENCE

SAMUEL J. RASCOFF*

It has been widely assumed that deterrence has little or no role to play in counterterrorism on the grounds that the threat of punishment is powerless to dissuade ideologically inspired terrorists. But an emerging literature in strategic studies argues, and aspects of contemporary American national security practice confirm, that this account misunderstands the capacity of deterrence to address current threats. In fact, a great deal of American counterterrorism is predicated on what I call "new deterrence," a cluster of refinements to traditional deterrence theory that speaks to a world of asymmetric threats. Yet the emergence of new deterrence has been largely lost on lawyers, judges, and legal academics, resulting in significant gaps between the practice of national security in this area and the legal architecture ostensibly designed to undergird and oversee it. In particular, the legal framework of counterterrorism has not adequately incorporated or addressed new deterrence's implications for scale, secrecy, and psychology, both at the level of doctrine and institutional design. This absence is striking given the prominence of deterrence theory in American strategy and criminology—precisely the two fields thought to converge in counterterrorism. In this Article, I debut in legal scholarship a sustained analysis of new deterrence and highlight its consequences for national security law, thus ushering in a serious reckoning for jurists with counterterrorism deterrence.

 Associate Professor of Law, Faculty Director, Center on Law and Security, New York University School of Law. Thanks to participants in the NYU Law Faculty Workshop, the Columbia Summer Workshop on National Security Law, and the March 2013 conference on New Models of Expertise and Democratic Participation in Policing at the Humboldt University in Berlin. Special thanks to Rush Atkinson, Bobby Chesney, Bridge Colby, Nick Colten, Sharon Dolovich, David Garland, Zachary Goldman, Stephen Holmes, Aziz Huq, Jim Jacobs, Jon Michaels, Trevor Morrison, David Pozen, Jackie Ross, Adam Samaha, Stephen Schulhofer, and Matt Waxman for extraordinarily helpful comments. Gretchen Feltes was superb at library assistance. Kirti Datla, Michael Hotz, Nishi Kumar, Zander Li, Daniel Schwartz, Matthew Simon, and Madeline Snider provided excellent research assistance. For their hospitality, I thank Dean Marty Katz and Professor Fred Cheever of the Sturm College of Law at the University of Denver.

INTRODUCTION

For all the strides that legal scholarship has made in analyzing the enormous range of issues presented by contemporary counterterrorism, there is a striking dearth of analysis of the role that deterrence plays.[1] Terrorism, it is generally agreed, stands in an intermediate position along a spectrum defined by traditional warfare on one end and violent crime on the other. Similarly, counterterrorism itself lies on a continuum between warfare and crime control.[2] One would therefore expect deterrence—the theoretical framework that motivated American national security for the better part of the post–World War II era[3] and, in a different but related form, supplied one of the core foundations of American criminology in that same

[1] Deterrence literature often struggles with whether deterrence is best described as an account of the world or a science of decisionmaking. *See* Frank C. Zagare, *Deterrence Is Dead. Long Live Deterrence*, 23 CONFLICT MGMT. & PEACE SCI. 115, 115–16 (2006) (discussing the two approaches to deterrence); *see also* Richard Ned Lebow, Deterrence 2 (May 2008) (unpublished manuscript), *available at* http://www.dartmouth.edu/~nedlebow/recent_articles.html ("In analytical terms, theories of deterrence must be distinguished from the strategy of deterrence. The former address the logical postulates of deterrence and the political and psychological assumptions on which they are based, the latter the application of the theory in practice.").

[2] *See, e.g.*, Robert Chesney & Jack Goldsmith, *Terrorism and the Convergence of Criminal and Military Detention Models*, 60 STAN. L. REV. 1079, 1100–20 (2008) (detailing how formerly distinct military and criminal detention paradigms have evolved and grown closer post-9/11).

The strategic and criminological literatures on deterrence are, of course, motivated by very different goals and implicate very different institutional, cultural, and conceptual repertoires. Furthermore, the criminological literature is informed by millions of data points (crimes everywhere committed every day) rather than a handful (the maintenance or breakdown of regional or international order over years or decades). Nonetheless, there is more than a family resemblance between these two senses of deterrence theory.

[3] *See, e.g.*, AUSTIN LONG, RAND CORP., DETERRENCE: FROM COLD WAR TO LONG WAR 5 (2008), *available at* http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG636.pdf (discussing the history of deterrence theory, including the "paramount place" deterrence held during the Cold War).

time frame[4]—to figure prominently in counterterrorism, especially in its treatment by lawyers. It doesn't. Rather, the legal analysis and application of deterrence thinking in counterterrorism has been, and continues to be, sparse.

Skepticism of the capacity of deterrence to address terrorist threats was widespread in the immediate aftermath of 9/11.[5] Emblematic of this outlook was President George W. Bush's 2002 National Security Strategy, which stated that "[t]raditional 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] But this skeptical posture was relatively short-lived. Deterrence began to make a small but palpable comeback in the discourse of some security officials and commentators,[7] partly because the effectiveness of alternative approaches, like preemption,[8] had begun to be called into question. Thus, the Obama Administration's 2011 Counterterrorism Strategy identified certain mechanisms for deterring terrorist activity, including prosecutions and

---

[4] *See* Raymond Paternoster, *How Much Do We Really Know About Criminal Deterrence?*, 100 J. CRIM. L. & CRIMINOLOGY 765, 777–80 (2010) (discussing the revival of deterrence theory among criminologists in the 1960s).

[5] *See* LAWRENCE FREEDMAN, DETERRENCE 2 (2004) (arguing that the shift during the Bush administration from deterrence toward a policy of preemption was because "[t]here were some threats that could not be deterred and must be dealt with before they could be realized"). Some commentators have tried to merge the discussion of deterrence with other strategies. *See, e.g.*, David B. Rivkin, Jr., *The Virtues of Preemptive Deterrence*, 29 HARV. J.L. & PUB. POL'Y 85, 93–94 (2005) (arguing that the Bush doctrine of preemption "dispel[s] an impression of American weakness," helping the United States regain a "credible deterrence posture").

[6] WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 15 (2002), *available at* http://www.state.gov/documents/organization/63562.pdf. Some empirical data suggest terrorist decisionmaking does not conform to Bayesian rationality. *See* Max Abrahms, *What Terrorists Really Want: Terrorist Motives and Counterterrorism Strategy*, 32 INT'L SECURITY 78, 93–95 (2008) (noting evidence which suggests terrorist activity is motivated by social solidarity rather than likelihood of successful political outcomes). *See generally* SHARON BERTSCH MCGRAYNE, THE THEORY THAT WOULD NOT DIE: HOW BAYES' RULE CRACKED THE ENIGMA CODE, HUNTED DOWN RUSSIAN SUBMARINES & EMERGED TRIUMPHANT FROM TWO CENTURIES OF CONTROVERSY (2011) (discussing the history of the reception and applications of Bayesian theory).

[7] *See* ERIC SCHMITT & THOM SHANKER, COUNTERSTRIKE: THE UNTOLD STORY OF AMERICA'S SECRET CAMPAIGN AGAINST AL QAEDA 56 (2011) (discussing the approval of language referring to a strategy of deterrence in the March 2006 National Security Presidential Directive 46 as evidence of an emerging willingness to view terrorists and terrorist organizations as susceptible to deterrence).

[8] *See* ALAN M. DERSHOWITZ, PREEMPTION: A KNIFE THAT CUTS BOTH WAYS 2 (2006) (observing a conceptual shift away from deterrence and toward preemption).

target hardening.[9] Meanwhile a new body of deterrence scholarship has taken shape,[10] drawing attention to deterrence theory's relevance to the design and implementation of effective counterterrorism programs.

However, legal scholarship and analysis have not kept pace with these developments. This may be due, in part, to something as simple as terminological confusion. Unlike the traditional paradigm, which emphasizes the role of backward-looking punishment and cost imposition as sources of deterrence,[11] the emerging strategic studies literature has a more thoroughly forward-looking, preventative orientation. Professor Balkin reveals this conceptual rift in arguing that "[g]overnance in the National Surveillance State is increasingly statistically oriented, *ex ante* and preventative, rather than focused on deterrence and *ex post* prosecution of individual wrongdoing."[12] Furthermore, lawyers tend to frame counterterrorism issues in narrow, incapacitationist terms, emphasizing the legal issues surrounding efforts to eliminate or neutralize a particular threat (for example, through detention, targeted killing, or arrest) rather than deterrence-based accounts that tend to focus on preventing threats

---

[9] *See* WHITE HOUSE, NATIONAL STRATEGY FOR COUNTERTERRORISM 6, 8 (2011), *available at* http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf ("The successful prosecution of terrorists will . . . deter terrorist activity . . . . [Target hardening] can deter [terrorists] from attacking particular targets or persuade them that their efforts are unlikely to succeed."). For a definition and description of "target hardening," see *infra* Subpart I.C.

[10] *See, e.g.*, DETERRING TERRORISM: THEORY AND PRACTICE (Andreas Wenger & Alex Wilner eds., 2012) (collecting articles that apply deterrence theory to counterterrorism effects); Matthew Kroenig & Barry Pavel, *How to Deter Terrorism*, 35 WASH. Q. 21, 21–22 (2012) (explaining how, with a change in focus and scope, deterrence is applicable to terrorism as it was to the U.S.S.R.); Alex S. Wilner, *Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism*, 34 J. STRATEGIC STUD. 3, 3–4 (2011) (discussing the use of new and traditional methods to deter terrorists). Some commentators refer to this body of work as the "fourth wave" of deterrence research. *See* Jeffrey W. Knopf, *The Fourth Wave in Deterrence Research*, 31 CONTEMP. SECURITY POL'Y 1, 3 (2010) (noting that the three prior waves of deterrence research dealt with aspects of the symmetrical threat posed by the U.S.S.R., while the new wave is characterized by the asymmetric threat posed by terrorists). As discussed below, "new deterrence" literature in strategic studies overlaps with and tends to be reinforced by a separate body of literature in criminology that focuses on situational crime prevention. *Compare* RONALD V. CLARKE & GRAEME R. NEWMAN, OUTSMARTING THE TERRORISTS 1 (2006) ("[W]e must identify and remove the opportunities that terrorists exploit to mount their attacks."), *with* Laura Dugan et al., *Testing a Rational Choice Model of Airline Hijackings*, 43 CRIMINOLOGY 1031, 1056–57 (2005) (concluding that deterrence by punishment and deterrence by denial reduce the risk of hijackings undertaken by nonterrorist criminals).

[11] *See* Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 176–77 (1968) (discussing criminals' cost-benefit calculus).

[12] Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 10–11 (2008).

from arising in the first place.[13] In addition, and in contrast to at least one theory about the nature of discourse in relation to crime control,[14] legal analysis of security issues has typically eschewed cost-benefit framing in favor of more full-throated normative contestation of counterterrorism practices.[15] Finally, national security law scholarship generally has not paid sufficient attention to the amenability of the terrorist threat to strategic response.[16]

This Article demonstrates how a focus on aspects of contemporary deterrence theory can help refine our understanding of certain critical issues in the law of national security.[17] The structure is as follows. In Part I, I describe developments in the strategic studies literature on deterrence motivated by post-9/11 terrorism, which I refer to cumulatively as "new deterrence." I emphasize three elements of new deterrence: tailoring, layering, and denying. I also draw attention to conceptually overlapping developments in criminology (most

---

[13] Criminal law literature often treats incapacitation as that which becomes necessary when deterrence fails. *See* Richard A. Posner, *An Economic Theory of the Criminal Law*, 85 COLUM. L. REV. 1193, 1223 (1985) ("The fact that certain criminals may not be deterrable argues for greater emphasis on their incapacitation, which implies long prison terms."); *see also* Isaac Ehrlich, *On the Usefulness of Controlling Individuals: An Economic Analysis of Rehabilitation, Incapacitation, and Deterrence*, 71 AM. ECON. REV. 307, 318 (1981) ("An optimal policy would not exempt [offenders unresponsive to deterrence-oriented sanctions] from punishment, but punish them through incapacitative penalties.").

[14] *See* Dan M. Kahan, *The Secret Ambition of Deterrence*, 113 HARV. L. REV. 413, 435 (1999) (arguing that deterrence talk in criminal law obfuscates more full-throated political and normative contestation).

[15] *See infra* notes 229–34 and accompanying text (proposing cost-benefit analysis as particularly appropriate in assessing deterrence strategies); *cf.* Darryl K. Brown, *Cost-Benefit Analysis in Criminal Law*, 92 CALIF. L. REV. 325, 363–64 (2004) (noting that the prevalence of retributivist logic in criminal law has served as an obstacle to the penetration of cost-benefit norms rooted in consequentialist theory). Professors Zimring and Hawkins have argued that jurists insufficiently scrutinize the costs and benefits of incapacitation-based rationales for imprisonment. *See* FRANKLIN E. ZIMRING & GORDON HAWKINS, INCAPACITATION: PENAL CONFINEMENT AND THE RESTRAINT OF CRIME 11 (1995) ("[P]articipants on both sides of the ideological debate on crime control accept[ ] some form of incapacitation as a residual rationale for imprisonment . . . .").

[16] That is not to say that the scholarship is entirely bereft of analyses of the developing nature of the terrorist threat. *See* Robert M. Chesney, *Beyond the Battlefield, Beyond al Qaeda: The Destabilizing Legal Architecture of Counterterrorism*, 112 MICH. L. REV. 163, 190–98 (2013) (discussing the implications of the franchise-like expansion of al-Qaeda into new regions). More generally, certain scholars have emphasized the tight connection between law and strategy. *See, e.g.*, PHILIP BOBBITT, TERROR AND CONSENT: THE WARS FOR THE TWENTY-FIRST CENTURY (2008); STEPHEN HOLMES, THE MATADOR'S CAPE: AMERICA'S RECKLESS RESPONSE TO TERROR 5–6 (2007) (arguing that law creates institutions within which strategy can be implemented).

[17] This Article is not intended as a contribution to the empirical study of deterrence in counterterrorism. As such, I do not hazard an assessment as to whether current practices (or some hypothetical set of alternative practices) are strategically necessary or normatively attractive.

notably Situational Crime Prevention), some of which have been expressly leveraged in understanding and implementing counterterrorism policies.

In Part II, I identify three core insights into contemporary counterterrorism policy and law that are brought out by new deterrence, illustrating each by reference to a concrete example. First, I contend that new deterrence argues for an appreciation of the "scale" of counterterrorism.[18] Recent legal scholarship emphasizes the manner in which counterterrorism, unlike traditional warfare, places a premium on the individual combatant, as opposed to large armies.[19] And law practice (especially within the executive branch) tends to emphasize the issues surrounding particular tactical-level, counterterrorism interventions. While these insights are significant, I show that they have to be understood against the backdrop of counterterrorism's strong programmatic dimension. I illustrate counterterrorism at scale by reference to airport security measures.

Second, I address how new deterrence upends much of the conventional wisdom regarding secrecy in national security. Deterrence entails communicating a threat, which cannot be done in secret. I situate this insight in the context of FBI counterterrorism sting operations and the criminal prosecutions to which they give rise.

Third, I show how new deterrence necessarily restores the role of fear and distrust (and psychology more generally) in the conversation about counterterrorism.[20] New deterrence depends in part on official signals of invulnerability, even of government omniscience and omnipotence, with an eye to frustrating and demoralizing the adversary. I illustrate by reference to the drone program, the purposes of which are not limited to incapacitating particular threats.

In Part III I identify two kinds of barriers to the effective incorporation of new-deterrence–based thinking into the legal archi-

---

[18] Kenneth Waltz introduced the concept of scale to war analysis by assessing the causes of war on three levels: the individual, the institutional, and the strategic. KENNETH N. WALTZ, MAN, THE STATE AND WAR 12 (1959). While contemporary legal scholarship on counterterrorism tends to privilege the first dimension, I aim to restore the centrality of the latter two.

[19] *See* Samuel Issacharoff & Richard H. Pildes, *Targeted Warfare: Individuating Enemy Responsibility*, 88 N.Y.U. L. REV. 1521 (2013) (observing that in contemporary counterterrorism, justifications for individual targeting or detention decisions are demanded); *see also* Gabriella Blum, *The Individualization of War: From War to Policing in the Regulation of Armed Conflicts*, *in* LAW AND WAR 48 (Austin Sarat et al. eds., 2014) (observing that because of the transition to individualization "wartime regulation is increasingly aspiring to make war look more like a policing operation").

[20] This is perhaps linguistically inevitable given that the Latin root of deterrence, "deterreo," also meant "to frighten." OXFORD LATIN DICTIONARY 530 (P.G.W. Glare ed., 1982).

tecture that implements and oversees contemporary counterterrorism. The first set of barriers is doctrinal. Contemporary doctrine—in areas ranging from "Special Needs" to "State Secrets" to standing—has not successfully metabolized new deterrence.

The second set of barriers is institutional. Owing to flawed organizational dynamics, the national security state has not proved adept at operationalizing a deterrence-based approach to counterterrorism in a systematic way. Similarly, institutions nominally poised to oversee counterterrorism policy and practice have proved inadequate to the task of addressing the issues generated by a new-deterrence–based strategy.

I
THE EMERGENCE OF NEW DETERRENCE

Invoking new deterrence implicitly raises questions about traditional deterrence and the differences between the two. Traditional deterrence thinking,[21] more than any other theory or strategy, has supplied the foundation for America's national security and the country's aspiration to global stability since the advent of the Cold War.[22] New deterrence does not represent a break with this traditional thinking, which may still serve counterterrorism purposes under certain bounded conditions,[23] so much as a series of refinements to it.

---

[21] *See generally* THOMAS C. SCHELLING, THE STRATEGY OF CONFLICT (1980 ed. 1981) (applying game theory to the international politics of deterrence); GLENN H. SNYDER, DETERRENCE AND DEFENSE: TOWARD A THEORY OF NATIONAL SECURITY (1961) (elaborating the foundations of strategic deterrence).

[22] To be certain, deterrence is not the only strategy. *See* Adam Garfinkle, *Does Nuclear Deterrence Apply in the Age of Terrorism?*, FOREIGN POL'Y RES. INST. (May 2009), http://www.fpri.org/footnotes/1410.200905.garfinkle.nucleardeterrenceterrorism.html (explaining that deterrence operates alongside "compellence" and "reassurance"). Garfinkle goes on to recognize that "there are basically two ways to achieve [deterrence]: through the threat of punishment and through the efficacy of defense. Either way, you can tell when deterrence fails, but not necessarily when it succeeds . . . ." *Id*.

[23] Classical deterrence can be effective when terrorist groups are state-sponsored and their patrons can be threatened or under conditions where other vehicles for "delegated deterrence" may be available. Daryl J. Levinson, *Collective Sanctions*, 56 STAN. L. REV. 345, 349 (2003) (defining "delegated deterrence" as a strategy that "aim[s] sanctions not at the individual wrongdoer but at some target group that is well-positioned to monitor and control him"). Certain governments have imposed normatively extreme group sanctions—like destroying the houses of suicide bombers. *See* Efraim Benmelech et al., *Counter-Suicide-Terrorism: Evidence from House Demolitions* 3 (Nat'l Bureau of Econ. Research, Working Paper No. 16493, 2010), *available at* http://www.nber.org/papers/w16493.pdf (describing the Israeli Defense Forces' demolition of Palestinian homes). Similarly, the material support statute effectively imposes group sanctions by punishing donations to proscribed terrorist groups. 18 U.S.C. § 2339B(b)–(c) (2012) (authorizing civil penalties and injunctions); *see also* Holder v. Humanitarian Law Project, 130 S. Ct. 2705, 2731 (2010) (holding that the material support statute did not violate plaintiffs' First Amendment

These refinements translate theoretical insights generated in the context of a bipolar nuclear showdown to a world of asymmetric threats and nonstate actors. I focus on three features of new deterrence: tailoring, layering, and denying.

A. Tailoring

Emerging scholarly literature emphasizes how deterrence can work in a tailored fashion, accounting for nonstate adversaries.[24] As one commentator recently explained, "tailored deterrence rejects [traditional deterrence theory's] unitary rational actor assumptions, requiring instead that each adversary be viewed as a complex system of unique decisionmakers."[25] This insight carries important implications. Al Qaeda, a classic nonstate actor, has a very different ideological, strategic, and operational outlook than Hezbollah, which enjoys the patronage of a powerful regional state actor.[26] And both these groups will respond differently than domestic terrorists to

---

rights, even where applied to the support of noncriminal activities of designated foreign terrorist organizations).

[24] *See* Jeffrey S. Lantis, *Strategic Culture and Tailored Deterrence: Bridging the Gap Between Theory and Practice*, 30 CONTEMP. SECURITY POL'Y 467, 470 (2009) (describing tailored deterrence as an approach which accounts for the identity and objectives of the adversary in crafting policies that seek to alter the behavior of those actors); M. Elaine Bunn, *Can Deterrence Be Tailored?*, STRATEGIC F., Jan. 2007, at 1–2, *available at* http://cyberanalysis.pbworks.com/f/SF225.pdf ("The evolution of American thinking about deterrence can be characterized, in broad terms, as moving from deterring one actor during the Cold War to multiple actors now . . . .").

[25] Sean P. Larkin, *The Limits of Tailored Deterrence*, 63 JOINT FORCE Q. 47, 52 (2011). Larkin's point might be viewed as a variation on the familiar distinction between general and specific deterrence in criminal law. *See, e.g.*, Mark C. Stafford & Mark Warr, *A Reconceptualization of General and Specific Deterrence*, *in* READINGS IN CONTEMPORARY CRIMINOLOGICAL THEORY 26, 27–28 (Peter Cordella & Larry Siegel eds., 1996) (distinguishing between the two depending on the "nature of prior direct experience of legal punishment" (emphasis omitted)).

[26] *See* Bernard Haykel, Op-Ed, *The Enemy of My Enemy Is Still My Enemy*, N.Y. TIMES, July 26, 2006, at A17 (describing a bitter ideological rivalry between Hezbollah and Al Qaeda); Alexander Marquardt, *Hezbollah and al Qaeda Fighters Edging Closer to Full Scale Confrontation*, ABC NEWS, May 10, 2013, http://abcnews.go.com/International/hezbollah-al-qaeda-fighters-edging-closer-confrontation/story?id=19144119 (discussing escalating conflicts between Hezbollah and Sunni rebel groups in the Syrian civil war). *Compare Counterterrorism 2014 Calendar*, *Al-Qa'ida*, Nat'l Counterterrorism Ctr., http://www.nctc.gov/site/groups/al_qaida.html (last visited Jan. 29, 2014) (describing Al-Qaeda's so-called global strategy), *with Counterterrorism 2014 Calendar*, *Al-Qa'ida in the Arabian Peninsula (AQAP)*, NAT'L COUNTERTERRORISM CTR., http://www.nctc.gov/site/groups/aqap.html (last visited Jan. 29, 2014) (describing AQAP's more regionally-oriented organizations), *and Counterterrorism 2014 Calendar*, *Hizballah*, NAT'L COUNTERTERRORISM CTR., http://www.nctc.gov/site/groups/hizballah.html (last visited Jan. 29, 2014) (describing Hezbollah's more regionally-oriented organizations).

deterrence strategies,[27] with "[s]ome groups [being] more readily deterrable than others."[28] Moreover, tailored deterrence teaches that effective policy needs to adapt to differences *within* a given group or network[29]: Terrorist foot soldiers behave differently than operational commanders, financiers, and propagandists.[30]

---

[27] Some, like Marc Sageman, have taken the view that radicalized individuals and small groups now pose a greater threat than organized groups. *See generally* MARC SAGEMAN, LEADERLESS JIHAD: TERROR NETWORKS IN THE TWENTY-FIRST CENTURY (2008) (outlining the process of radicalization for individual and small groups of terrorists and proposing policy recommendations to counter the particular dangers of these less organized groups). Others disagree and maintain that (at least as of 2008) Al Qaeda core remains important. *See* Bruce Hoffman, *The Myth of Grass-Roots Terrorism: Why Osama Bin Laden Still Matters*, 87 FOREIGN AFF. 133, 134–35 (2008) (citing multiple analyses concluding that Al Qaeda remains a viable threat).

[28] ANDREW R. MORRAL & BRIAN A. JACKSON, RAND CORP., UNDERSTANDING THE ROLE OF DETERRENCE IN COUNTERTERRORISM SECURITY 19 (2009), *available at* http://www.rand.org/pubs/occasional_papers/2009/RAND_OP281.pdf; *see also* Garfinkle, *supra* note 22 ("Here there is no substitute for understanding the groups you want to deter. . . . [In contrast to Hamas and Hezbollah,] Al Qaeda . . . has no social context; it has no social program of any kind, so it is much harder to hold anything at risk its leaders care about."); *cf.* LONG, *supra* note 3, at 80–83 (discussing the proposition that nonstate terrorist actors are immune to fear and therefore undeterrable). The fundamental differences between terror groups also raise questions about interpreting the Authorization for the Use of Military Force (AUMF), Pub. L. No. 107-40, 115 Stat. 224 (2001), to encompass an ever wider and more disparate group of covered terror organizations. For instance, the Obama Administration is said to consider only some members of the Somalia-based terrorist group, al Shabab, to be covered by the AUMF. Charlie Savage, *U.S. Tests New Approach to Terrorism Cases on Somali Suspect*, N.Y. TIMES, July 7, 2011, at A10 ("[T]he administration does not consider the United States to be at war with every member of the Shabab . . . . [Only those who] were integrated with Al Qaeda or its Yemen branch and were said to be looking beyond the internal Somali conflict.").

[29] Davis and Jenkins urged this very point early in the post-9/11 era:

> It is a mistake to think of influencing al Qaeda as though it were a single entity; rather, the targets of U.S. influence are the many elements of the al Qaeda *system*, which comprises leaders, lieutenants, financiers, logisticians and other facilitators, foot soldiers, recruiters, supporting population segments, and religious or otherwise ideological figures. A particular leader may not be easily deterrable, but other elements of the system (e.g., state supporters or wealthy financiers living the good life while supporting al Qaeda in the shadows) may be. What is needed is a multifaceted strategy that tailors influences to targets within the system. Terrorists are not a uniform group with an on-off switch.

PAUL K. DAVIS & BRIAN MICHAEL JENKINS, RAND CORP., DETERRENCE & INFLUENCE IN COUNTERTERRORISM, at xi–xii (2002), *available at* http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1619.pdf.

[30] *See* Elbridge A. Colby, *Expanded Deterrence: Broadening the Threat of Retaliation*, 149 POL'Y REV. 43, 52 (2008) ("[T]he vast majority of terrorists, even those contemplating catastrophic attacks against us, have some kind of rationale in mind, a strategy, a rational calculus that we can affect. . . . Broadening our deterrent threat will let us seize more levers on these groups' behavior." (footnotes omitted)).

In addition, tailoring requires a deep understanding of whether, by whom, and how messages will be received,[31] including whether potential aggressors will translate messages into updated beliefs about an attack's costs and benefits. Regardless of whether "terrorist groups closely monitor the American press and change practices in response to leaks,"[32] Al Qaeda leadership attends to at least some signals sent by Washington.[33] Evidence obtained at the Abottabad compound,[34] for example, or contained in the Al Qaeda in the Arabian Peninsula–linked *Inspire* magazine,[35] attest to terrorist groups' familiarity with American counterterrorism practices and pathologies.

---

[31] *See* Shmuel Bar, *Deterring Terrorists: What Israel Has Learned*, 149 POL'Y REV. 29, 31 (2008) ("[D]eterrence is the result of mutual perceptions—self-image and the image of the enemy. These perceptions are laden with cultural and psychological overtones and passed through overlapping prisms of history, culture, language, and ideology.").

[32] Note, *Media Incentives and National Security Secrets*, 122 HARV. L. REV. 2228, 2232 (2009). Staunch proponents of national security secrecy frequently summon this argument to support their claims. *See, e.g.*, Memorandum from Cent. Intelligence Agency in Response to a Request for Unclassified Information Regarding the Impact of Leaks on the War Against Terrorism 1 (June 14, 2002), *available at* http://www.fas.org/sgp/bush/dod071202.pdf ("[A]l-Qa'ida operatives are extremely security conscious and have altered their practices in response to what they have learned from the press about our capabilities.").

[33] *See* JOSHUA ALEXANDER GELTZER, US COUNTER-TERRORISM STRATEGY AND AL-QAEDA: SIGNALLING AND THE TERRORIST WORLD-VIEW 1 (2010) ("[O]ne audience set for American counter-terrorist actions and rhetoric consists of the terrorist and would-be terrorist, who are known to be out there watching and listening carefully . . . ."). This receptivity sets terrorists apart from common criminals, concerning whom the state's potential to communicate effectively has long been a subject of scholarly doubt. *See* DAVID M. KENNEDY, DETERRENCE AND CRIME PREVENTION: RECONSIDERING THE PROSPECT OF SANCTION 41 (2009) (referring to "tantalizing instances suggesting that clear, credible messages can have considerable impact" but noting that "[t]here is no reason to believe that the 'messages' authorities seek to send get through, or that what does get through is interpreted as intended"). To the degree traditional deterrence has purchase in a portion of the criminal-justice world, it would seem to be in the realm of white-collar crime. *See* J. Scott Dutcher, Comment, *From the Boardroom to the Cellblock: The Justifications for Harsher Punishment of White-Collar and Corporate Crime*, 37 Ariz. ST. L.J. 1295, 1308 (2005) (arguing that deterrence is more effective against white-collar and corporate crime than against other types of crime, in part because white-collar and corporate criminals, generally, are more aware of deterrence signals).

[34] *See* Peter Bergen, *Bin Laden: Seized Documents Show Delusional Leader and Micromanager*, CNN (May 3, 2012, 7:33 AM), http://www.cnn.com/2012/04/30/opinion/bergen-bin-laden-document-trove (describing Bin Laden's awareness of American counterterrorism capabilities, including a description of America's "great accumulated expertise of photography . . . [that] can even distinguish between houses that are frequented by male visitors at a higher rate than is normal").

[35] *See* Yahya Ibrahim, *$4,200*, INSPIRE, Nov. 2010, at 15, *available at* http://www.investigativeproject.org/documents/testimony/375.pdf ("That is what we call leverage. A $4,200 operation will cost our enemy billions of dollars.").

Nevertheless, messages directed at deterring terrorist actors may fall on deaf ears or even embolden the adversary.[36]

B. Layering

Strategic studies literature emphasizes the importance of a layered approach to deterrence. Unlike Cold War deterrence, which was centrally predicated on the ultimate instrument of power (the nuclear weapon) deployed by a single institution (the military), counterterrorism deterrence depends on a complex set of interactions between many instruments and policies distributed over a wide range of institutions.[37]

New deterrence entails two types of layering. First, there is the possibility of synchronic layering, in which various instruments of power operating in concert may "exceed an adversary's threshold for deterrence."[38] Synchronic layering argues for measuring deterrence's effectiveness in the context of a complex system.[39] Second, diachronic layering (sometimes referred to as "cumulative deterrence") argues that the overall benefit conferred by a sustained deterrence posture may exceed the sum of interventions taken over time.[40] Importantly, diachronic layering is compatible with periodic outbreaks of violence (on both sides),[41] a phenomenon that is familiar to the context of

---

[36] *See, e.g.*, Bruno S. Frey, *How to Deal with Terrorism*, ECONOMISTS' VOICE, Aug. 2006, at 1, 1 ("History and recent experience suggest, however, that deterrence is *ineffective* and may even be *counterproductive* in dealing with terrorism."). The idea that official efforts may be not merely unproductive but even counterproductive is explored in Tom R. Tyler et al., *Legitimacy and Deterrence Effects in Counterterrorism Policing: A Study of Muslim Americans*, 44 L. & SOC'Y REV. 365, 385–86 (2010).

[37] Of course there is analysis of the strategic implications if a group like Al Qaeda were to use weapons of mass destruction. *See, e.g.*, Kenneth C. Brill & Kenneth N. Luongo, *On Nuclear Terrorism*, INT'L HERALD TRIB., Mar. 16, 2012, at 6 (arguing that the threat of nuclear terrorism requires a global security response).

[38] BRIAN A. JACKSON ET AL., RAND CORP., EFFICIENT AVIATION SECURITY: STRENGTHENING THE ANALYTIC FOUNDATION FOR MAKING AIR TRANSPORTATION SECURITY DECISIONS 75 (2012), *available at* http://www.rand.org/pubs/monographs/MG1220.html.

[39] *See* MORRAL & JACKSON, *supra* note 28, at 19 ("[T]he value of [a particular deterrence] measure [should be] weighed in the context of the overall homeland and national security system of which it is a part.").

[40] *See* Doron Almog, *Cumulative Deterrence and the War on Terrorism*, 34 PARAMETERS 4, 6 (2004) (discussing how decades of military and counterterrorism victories by Israeli security forces induced a reduction of threats and successful attacks by neighboring countries and Palestinian terrorist groups).

[41] *See, e.g.*, DANIEL BYMAN, A HIGH PRICE: THE TRIUMPHS AND FAILURES OF ISRAELI COUNTERTERRORISM 3–4 (2011) ("Israel has put several skilled terrorist groups out of business, deterred others and their sponsors, and managed to survive and prosper in the face of ceaseless violence . . . .").

crime and of private law[42] but represents a significant conceptual break with the tradition of nuclear deterrence. The Cold War featured two adversaries capable of mutual annihilation, so the failure of deterrence was imagined to mean all-out war.[43] But the current strategic landscape is more diverse. Where the adversary is fractured and breaches of security—even large terror attacks—are likely to be less damaging than a nuclear attack, officials can reestablish a deterrent effect even after an attack.[44]

C. Denying

Third, and perhaps most distinctive, strategic studies literature has rehabilitated a long-neglected concept of deterrence, "deterrence by denial" (DbD),[45] which Glenn Snyder, a founder of strategic deterrence theory, pioneered.[46] DbD is distinct from the more familiar concept of deterrence by punishment, which both the United States and Soviet Union employed during the Cold War and roughly tracks the sense of deterrence employed by scholars of criminal and tort law.[47] The intuition behind DbD is that deterrence can be

---

[42] *See* Thomas Rid, *Deterrence Beyond the State: The Israeli Experience*, 33 CONTEMP. SECURITY POL'Y 124, 124–26 (2012) (arguing that the Israeli national security and defense apparatus employs a deterrence strategy informed by the criminological sense of deterrence by punishment); David Ignatius, *Drone Deterrence*, WASH. POST, Oct. 5, 2011, at A19 (discussing continued, but more restrained, use of drone strikes to deter terrorist groups).

[43] *See* LEON WIESELTIER, NUCLEAR WAR, NUCLEAR PEACE 75 (1983) ("Deterrence must be the only public arrangement that is a total failure if it is successful only 99.9 percent of the time."); *cf.* U.S. JOINT CHIEFS OF STAFF, JOINT DOCTRINE: CAPSTONE AND KEYSTONE PRIMER 1 (1997), *available at* http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/938.pdf ("Deterrence is our first line of our national security. If deterrence fails, our objective is winning the nation's wars.").

[44] *Cf.* Martha Crenshaw, *Will Threats Deter Nuclear Terrorism?*, *in* DETERRING TERRORISM: THEORY AND PRACTICE 136, 143 (Andreas Wenger & Alex Wilner eds., 2012) (arguing that, in deterrence, "[t]he defender does not say 'we will keep hitting you over the head with this hammer so you don't even think of attacking us' but rather 'we are not hitting you now but will hit you really hard later if you cross this line' ").

[45] *See* DEP'T OF DEFENSE, DETERRENCE OPERATIONS: JOINT OPERATING CONCEPT 24 (Version 2.0, 2006), *available at* http://www.dtic.mil/futurejointwarfare/concepts/do_joc_v20.doc (stressing the need for military strategists to consider means by which to deny adversaries the benefits of hostile actions toward the United States, rather than simply focusing on retaliatory costs which could be imposed).

[46] *See* SNYDER, *supra* note 21, at 14–16 (discussing the theory behind deterrence by denial).

[47] Thomas Rid convincingly argues that strategists have not paid sufficient heed to the criminological literature on deterrence by punishment. Rid, *supra* note 42, at 126. In particular, he observes that Israel's deterrence strategy resembles criminological deterrence by punishment because Israeli strategy views deterrence as being fundamentally compatible with outbreaks of violence. *See id.* at 125 (discussing Israeli leaders' assumption that political violence could be curtailed but not eliminated). Like strategic deterrence, traditional criminal-law deterrence has emphasized deterrence-by-

achieved by denying benefits to an adversary for pursuing a particular course of behavior. DbD entails chipping away at the odds that an adversary will pull off an attack or that it will reap large benefits if it does, thereby causing group leaders to reconsider their initial decision. In this respect, DbD measures are conceptually distinct from defensive measures in that the latter are "designed primarily to fend off an opponent in the event of an attack" while the former are "intended to convince an adversary not to attack in the first place."[48]

DbD can operate in different registers. It may function at a highly strategic level by denying a terrorist group the desired political payoff of a successful attack by promoting a spirit of resilience in society or resistance by political elites to acceding to terrorist demands.[49] Or it may function operationally by making "terrorists believe that an attack is likely to fail, [so] they will be less motivated to waste time and resources by attempting to carry it out."[50] Indeed, there is some evidence, though at this point it remains more suggestive than definitive, that sufficient operational risk has deterred terrorists.[51]

---

punishment. *See* Paternoster, *supra* note 4, at 766 ("The concept of deterrence is quite simple—it is the omission of a criminal act because of the fear of sanctions or punishment."); *see also* Paul H. Robinson & John M. Darley, *Does Criminal Law Deter? A Behavioural Science Investigation*, 24 OXFORD J. LEGAL STUD. 173, 175 (2004) (explaining the key variables as (1) the potential offender's knowledge of the law; (2) the potential offender's ability to make a rational choice; and (3) the net cost of the crime, as determined by the probability of punishment, severity of punishment, delay, and benefit).

[48] Kroenig & Pavel, *supra* note 10, at 23; *see also* Robert F. Trager & Dessislava P. Zagorcheva, *Deterring Terrorism: It Can Be Done*, 30 INT'L SECURITY 87, 90–91 (2005), *available at* http://www.jstor.org/stable/4137488 ("[W]here punishment seeks to coerce the enemy through fear, denial depends on causing hopelessness." (quoting DAVID E. JOHNSON ET AL., CONVENTIONAL COERCION ACROSS THE SPECTRUM OF OPERATIONS 17 (2012))).

[49] *See, e.g.*, Max Abrahms, *The Political Effectiveness of Terrorism Revisited*, 45 COMP. POL. STUD. 366, 367 (2012) ("My principal finding is that terrorist campaigns are an inherently unprofitable coercive tactic because governments resist complying when their civilians are the focus of substate attack.").

[50] Kroenig & Pavel, *supra* note 10, at 28; *cf.* ROBERT W. ANTHONY, INST. FOR DEF. ANALYSIS, DETERRENCE AND THE 9-11 TERRORISTS 6 (2003), *available at* www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA430351 ("According to intelligence reports, an interviewed terrorist said an attack was aborted because they believed that the chance of failure was a value in [an unacceptable] range.").

[51] *See* DAVIS & JENKINS, *supra* note 29, at xii ("[T]he empirical record shows that even hardened terrorists dislike operational risks and may be deterred by uncertainty and risk."); Kroenig & Pavel, *supra* note 10, at 29 (referencing "many cases in which terrorists were deterred from carrying out an attack by the fear of failure"). In one well-known case, a naturalized American in contact with Al Qaeda leadership in Pakistan called off a plan to attack the Brooklyn Bridge because "the weather [wa]s too hot," referring to overt police presence. Eric Lichtblau, *U.S. Cites Al Qaeda in Plot to Destroy Brooklyn Bridge*, N.Y. TIMES, June 20, 2003, at A1, *available at* http://www.nytimes.com/2003/06/20/us/threats-responses-terror-us-cites-al-qaeda-plot-destroy-brooklyn-bridge.html?pagewanted=all&src=pm.

DbD bears a conceptual affinity to situational crime prevention (SCP).[52] SCP emphasizes the importance of designing and managing the setting of crime in order to "increas[e] the associated risks and difficulties and reduc[e] the rewards."[53] SPC measures include "target hardening"[54] and property marking, intruder alarms, electronic merchandise tags,[55] surveillance of specific

[52] *See* Ronald V. Clarke, *Situational Crime Prevention*, *in* 19 BUILDING A SAFER SOCIETY: STRATEGIC APPROACHES TO CRIME PREVENTION 91 (Michael Tonry & David P. Farrington eds., 1995) (setting out the theory). For a discussion on the connection between SCP and deterrence strategies, see Anthony A. Braga & David M. Kennedy, *Linking Situational Crime Prevention and Focused Deterrence Strategies*, *in* THE REASONING CRIMINOLOGIST: ESSAYS IN HONOUR OF RONALD V. CLARKE 65 (Nick Tilley & Graham Farrell eds., 2012). More generally, there is evidence that national security norms have come to shape the criminal law landscape. *See* Dru Stevenson, *Effect of the National Security Paradigm on Criminal Law*, 22 STAN. L. & POL'Y REV. 129, 137–38 (2011) ("When we do incorporate elements of deterrence, the new paradigm shifts the focus towards lowering the rewards of illegal activity (by foiling terrorist plots or conspiracies before they succeed) or raising the investment costs for criminals . . . rather than traditional deterrence, which focused on the threat of punishment.").

[53] Clarke, *supra* note 52, at 91; *see also* Maurice Cusson, *Situational Deterrence: Fear During the Criminal Event*, *in* 1 CRIME PREVENTION STUDIES 55, 56 (Ronald V. Clarke ed., 1993), *available at* http://www.popcenter.org/library/crimeprevention/volume_01/03cusson.pdf (noting that "[a] potential offender can also be deterred by . . . self-defense measures," including fear "of being bitten by a watch dog or of setting off an alarm; because the area seems to be too closely watched; or because he feels that his potential victim looks dangerous").

[54] The SCP literature illuminates a perennial issue surrounding new deterrence, namely its alleged tendency to displace risk by shifting it away from certain more hardened targets to softer ones. *See* Thomas A. Repetto, *Crime Prevention and the Displacement Phenomenon*, 22 CRIME & DELINQUENCY 166, 168–69 (1976) (discussing the five potential forms of displacement). Some empirical studies suggest displacement is limited in scope. *See* René B.P. Hesseling, *Displacement: A Review of the Empirical Literature*, *in* 3 CRIME PREVENTION STUD. 197, 217–19 (Ronald V. Clarke ed., 1994) (noting from empirical studies that, while limited target and place displacement may occur, not all crime prevention measures lead to displacement, and it may be avoided by design). Indeed, some research shows that SCP measures may diffuse benefits to the surrounding area. Ronald V. Clarke & David Weisburd, *Diffusion of Crime Control Benefits: Observation on the Reverse of Displacement*, *in* 2 CRIME PREVENTION STUD. 165, 167–69 (1994); *see also* Rob T. Guerette & Kate J. Bowers, *Assessing the Extent of Crime Displacement and Diffusion of Benefits: A Review of Situational Crime Prevention Evaluations*, 47 CRIMINOLOGY 1331, 1345–46 (2009) (concluding from a systematic review of 102 evaluations based on 574 observations of SCP techniques that the likelihood of diffusion was 27% and the likelihood of displacement was 26%).

[55] Electronic article surveillance (EAS) tags trigger an alarm as the shopper exits unless store employees remove the tags at checkout. Tampering causes ink tags to stain and ruin the stolen merchandise, denying the thief the crime's benefit. *See* John E. Eck, *Preventing Crime at Places*, *in* EVIDENCE-BASED CRIME PREVENTION 241, 258–59 (Lawrence W. Sherman et al. eds., 2002) (discussing the effect of ink tags on shoplifting). A number of studies show a correlation between tag usage and theft reduction. *See, e.g.*, Read Hayes & Robert Blackwood, *Evaluating the Effects of EAS on Product Sales and Loss: Results of a Large-Scale Field Experiment*, 19 SECURITY J. 262, 265 (2006) (surveying various EAS studies that found loss reduction). Unsurprisingly, a study of hidden EAS tags showed no

locations, personal identification numbers, and automated traffic enforcement.[56]

* * *

None of these innovations in deterrence theory—tailoring, layering, or denying—supply a comprehensive theoretical foundation for counterterrorism or other emerging national security challenges.[57] But taken together, they can explain a great deal about contemporary strategy and practice.

II
Insights and Illustrations

The emergence of new deterrence carries significant implications for the practice of contemporary counterterrorism. I emphasize three insights and illustrate each with a concrete example. The first is counterterrorism at scale—that is, how counterterrorism operates through widespread programs, rather than merely through individual interventions. I illustrate by reference to airport screening.

The second insight regards the role of secrecy. The received wisdom is that national security is the site of a Manichean struggle between secrecy and transparency,[58] with officials consistently looking

---

resulting reduction in theft. *See id.* at 271–72 ("EAS, like any deterrent, must be readily apparent and reinforced to those it is deployed to deter . . . .").

[56] A study of Automated Traffic Enforcement Systems (ATES) using cameras at dangerous Philadelphia intersections showed a ninety-six percent reduction in red light violations after the installation and advertisement of the ATES system. Benton H. Page, Automatic Traffic Systems: The Efficacy of Such Systems and Their Effect on Traffic Law 13–14 (Mar. 2009) (unpublished manuscript), *available at* http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=benton_page. But reductions in violations need not translate into greater safety, for example, if the presence of cameras produces accidents when drivers slam on their brakes. *See* Barbara Langland-Orban et al., *An Update on Red Light Camera Research: The Need for Federal Standards in the Interest of Public Safety*, 8 Fla. Pub. Health Rev. 1, 5 (2011) ("Unfortunately, [Red Light Cameras] encourage abrupt stops, which are not always anticipated by trailing drivers.").

[57] Several commentators have discussed the application of deterrence theory in the context of cyber security. *See, e.g.*, William J. Lynn III, *Defending a New Domain*, 89 Foreign Aff. 97, 99–100 (2010) ("[D]eterrence will necessarily be based more on denying any benefit to attackers than on imposing costs through retaliation. The challenge is to make the defenses effective enough to deny an adversary the benefit of an attack despite the strength of offensive tools in cyberspace."); *see also* Stephen J. Lukasik, *A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains*, *in* Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy 120 (2010) ("Deterrence, on the Cold War retaliation model, is unlikely to be effective in dealing with cyber force. . . . [I]t must be based on broader concepts than retaliation and punishment.").

[58] *See generally* Daniel Patrick Moynihan, Secrecy: The American Experience (1998) (discussing and questioning the role of secrecy throughout American history); Stephen Schulhofer, *Oversight of National Security Secrecy in the United States*, *in* Secrecy, National Security and the Vindication of Constitutional Law 22

to maximize the former in order to promote security. But new deterrence teaches that the situation is more complex, with the government engaging in a nuanced calibration of concealment and revelation to advance its strategic objectives. Here my example is the use of sting operations in counterterrorism.

The third insight regards the role of psychology in counterterrorism. Like terrorism itself, which ultimately seeks widespread dissemination of fear and distrust, counterterrorism operates in a psychological register.[59] In particular, new deterrence draws attention to how the government deploys fear and distrust as part of its counterterrorism repertoire. I adduce drone policy as an example.

A. Scale and Stops

One of the signal contributions of adopting the new-deterrence lens is the way it clarifies the scale of counterterrorism. Legal practitioners and scholars tend to employ a tactical focus and emphasize the role of the individual in terrorism and counterterrorism. Recent scholarship and reporting on executive branch lawyering emphasizes the "individuation" of responsibility in asymmetric warfare. Professor Blum observes that the individuation of warfare requires new norms for deciding which individuals and groups may be lawfully targeted, which may influence how and when nations go to war.[60] And Professors Issacharoff and Pildes argue that, while pursuing counterterrorism policies of detention and targeting, the military should make decisions through adjudicative processes.[61] In this emerging literature, traditional assumptions about the collective nature of war have given way to new norms of individuality in asymmetric warfare.

The trend toward individuation is evident beyond the ascription of legal and moral responsibility to individual warriors. It is also tied to the manner in which individual cases drive official counterterrorism

(David Cole et al. eds., 2013) (describing oversight of the executive's decision to classify information).

[59] *See, e.g.*, Aziz Z. Huq, *The Political Psychology of Counterterrorism*, 9 ANN. REV. LAW & SOC. SCI. 71 (2013) (reviewing social science literature on the psychology of counterterrorism).

[60] Blum, *supra* note 19, at 48–50, 76–79. Blum further identifies certain upsides of the turn to individualization, including heightened recognition of the need to protect all citizens, but also certain potential downsides, including the dampening of a liberal democracy's willingness to wage even a just war and the extension of a war mentality to domestic policing. *Id.*

[61] Issacharoff & Pildes, *supra* note 19, at 1596–97 (arguing that the increased individuation of warfare has led the military to undertake a quasi-adjudicative role in determining its enemy and advocating for the elaboration of more robust legal, moral, and policy frameworks).

decisions both from the perspective of policy and of law.[62] It goes without saying that planning the raid that killed Osama Bin Laden[63] or deciding the proper forum in which to try Khalid Sheikh Mohammed[64] consumed enormous amounts of time among senior administration officials, including (at least concerning the former) the President. But the President and his staff have also actively participated in relatively less-weighty decisions.[65] As Daniel Klaidman has written, deciding how and where to detain a low-level Somali terrorist named Ahmed Warsame required no fewer than a dozen meetings of cabinet and sub-cabinet level officials.[66] Meanwhile, top administration lawyers produced an extensive Office of Legal Counsel memo on the legality of targeting Anwar al-Aulaqi.[67]

What the legal world has tended to miss in its focus on individual cases—and what new deterrence clarifies—is the degree to which counterterrorism operates at scale.[68] This insight refers to more than

---

[62] *See generally* Rebecca Ingber, *Interpretation Catalysts and Executive Branch Legal Decisionmaking*, 38 YALE J. INT'L L. 359, 372–77 (2013) (providing background information on the multifarious processes by which executive branch legal decisionmaking occurs).

[63] *See* Nicholas Schmidle, *Getting Bin Laden*, NEW YORKER (Aug. 8, 2011), http://www.newyorker.com/reporting/2011/08/08/110808fa_fact_schmidle (describing the evolution of the plan to kill Bin Laden).

[64] *See* Anne E. Kornblut & Carrie Johnson, *Obama to Help Pick Location of Terror Trial; Responding to Backlash Alleged 9/11 Mastermind Was to Be Tried in New York*, WASH. POST, Feb. 12, 2010, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/11/AR2010021105011.html (naming seven senior White House staff members, in addition to President Obama and Attorney General Holder, who have been involved with selecting the trial location).

[65] A former Secretary of Defense in the Obama administration recently suggested that a pattern of White House micro-management characterized decisionmaking across a range of national security issues. ROBERT M. GATES, DUTY: MEMOIRS OF A SECRETARY AT WAR 566–67, 586–87 (2014).

[66] DANIEL KLAIDMAN, KILL OR CAPTURE: THE WAR ON TERROR AND THE SOUL OF THE OBAMA PRESIDENCY 249 (2012).

[67] Scholars debate the appropriate role of the OLC in supplying legal foundations for security decisions. *Compare* Trevor W. Morrison, *Constitutional Alarmism*, 124 HARV. L. REV. 1688, 1713–23 (2011) (book review) (defending the OLC against the charge that it serves as a rubber stamp for the executive branch), *with* Bruce Ackerman, *Lost Inside the Beltway: A Reply to Professor Morrison*, 124 HARV. L. REV. F. 13, 16–17, 19–22 (2011), *available at* http://www.harvardlawreview.org/media/pdf/vol124forum_ackerman.pdf (arguing that the Office's leadership by political appointees and close contact with the White House erodes its ability to offer unbiased and apolitical legal opinions).

[68] The new-deterrence lens also reveals how counterterrorism scales inter-temporally: Like risk regulation, counterterrorism is an ongoing effort to manage a constellation of threats that never meaningfully disappears. *See* Samuel J. Rascoff, *Domesticating Intelligence*, 83 S. CAL. L. REV. 575, 582–85, 604–06 (2010) (explaining how domestic intelligence should be characterized as risk assessment); Jessica Stern & Jonathan B. Wiener, *Precaution Against Terrorism*, 9 J. RISK RES. 393, 441 (2006) (describing how counterterrorism can "draw valuable insights from risk analysis"). This insight is familiar to criminologists but may be more surprising to traditional national security scholars, who

the number of terrorists on the government's radar; the point is that counterterrorism practices have a programmatic reach. Scale is about terrorism without proper names attached. It is not that focusing on certain high-value individuals is not a key element of counterterrorism; it is simply that emphasizing the headline-grabbing raids, detentions, or trials obfuscates the broader picture that new deterrence helps to reveal.

To illustrate counterterrorism at scale, it is useful to consider a program that does not command the same attention as drone strikes or military commissions, but nevertheless has become a signature feature of modern American counterterrorism: airport security. The conventional official line states that the purpose of the Transportation Security Administration (TSA) screening is to detect passengers with weapons.[69] Passengers sacrifice a little bit of time and sanity to allow for the detection and interdiction (followed, no doubt, by arrest/incapacitation) of would-be terrorists wielding bombs or box cutters. Meanwhile, on an equally conventional critique, TSA protocol represents "security theater"—"[t]here are huge costs, like an annual $4 billion payroll for TSA workers alone plus all the gizmos, construction, and maintenance expenses . . . to deal with the remote chance of finding a culprit."[70] If the real reason behind TSA screenings is to detect and interdict, then the program has to be judged a colossal failure.[71]

But new deterrence suggests that the standard arguments miss an important feature of airport screening: The purpose is not (or at any

---

expect war to have an endpoint. *Cf*. BOBBITT, *supra* note 16, at 236 ("Whereas wars in previous eras aimed for the capture of particular leaders or territory by means of battle, in the coming period conventional battles will be rare, violence will be directed almost entirely at civilians, and victory for states . . . will lie in precluding such attacks in the first place."); Gabriella Blum, *The Fog of Victory*, 24 EUR. J. INT'L L. 391, 393–96 (2013) ("[T]he formulation of victory now requires more long-term, abstract, and complex, less tangible and immediate terms. War, in other words, can no longer be reduced into a military campaign."); Robert M. Chesney, *Postwar*, 5 HARV. NAT'L SECURITY J. 305 (2014) (arguing that a transition from an "armed-conflict" to "postwar" definition of the U.S. conflict with Al Qaeda would not have a significant impact on its level of violence).

[69] The agency recently expanded its efforts to providing security at "sporting events, music festivals, rodeos, highway weigh stations and train terminals." Ron Nixon, *T.S.A. Expands Duties Beyond Airport Security*, N.Y. TIMES, Aug. 6, 2013, at A11, *available at* http://www.nytimes.com/2013/08/06/us/tsa-expands-duties-beyond-airport-security.html.

[70] Harvey Molotch, *Ten Ways We Get It Wrong at Security—and Some Fixes to Make Things Better*, HUFFINGTON POST (Oct. 8, 2012, 6:38 PM), http://www.huffingtonpost.com/harvey-molotch/how-to-improve-airport-security_b_1949714.html.

[71] *See* Juliet Lapidos, *Does the TSA Ever Catch Terrorists? If They Do, for Some Reason They Won't Admit It.,* SLATE (Nov. 18, 2010, 6:12 PM), http://www.slate.com/articles/news_and_politics/explainer/2010/11/does_the_tsa_ever_catch_terrorists.html (questioning whether TSA has prevented a terrorist attack in the past or caught individuals aside from "random nut jobs").

rate, not exclusively) to prevent any individual attack, but to deter a larger pool of would-be terrorists from even trying.[72] Deterrence is central to the design of airport security.[73] Thus, the Department of Homeland Security's National Strategy for Aviation Security embraces the idea that "layered security deters attacks, which otherwise might be executed in a multiple, simultaneous, catastrophic manner, by continually disrupting an adversary's deliberate planning process."[74] Similarly, the threat of Air Marshals leads to a "perception of security [that] may change the attackers' choices, creating additional security for flights with no marshal present through deterrence."[75]

To interpret airport security in a larger framework of new deterrence is certainly not to ascribe Panglossian excellence to current policy.[76] But noting the role that deterrence plays here points the way for a more informed conversation about how counterterrorism operates at scale, which in turn, makes possible a more sophisticated debate about the relative strengths and weaknesses of contemporary practices.[77]

---

[72] *See id.* ("TSA airport screeners [may] prevent terrorist attacks through their very existence—deterring plots by hanging around."). Perhaps because the tactical arguments for the success of airport security and other mass transportation hubs are hard to sustain (as opposed to, say, drone strikes or prosecutions where visible successes abound), security officials have been relatively more explicit about how they aim to achieve success.

[73] Bruce Schneier disagrees. He contends that:

> The argument that the TSA, by its very existence, deters terrorist plots is . . . spurious. There are two categories of terrorists. The first, and most common, is the amateurs, like the guy who crashed his plane into the Internal Revenue Service building in Austin. They are likely to be sloppy and stupid, and even pre-9/11 airplane security is going to catch them. The second is the well-briefed, well-financed and much rarer plotters. Do you really expect TSA screeners, who are busy confiscating water bottles and making people remove their belts and shoes, to stop the latter sort?

Bruce Schneier, *Economist Debates: Airport Security*, ECONOMIST (Mar. 20, 2012), http://www.economist.com/debate/days/view/820. It is telling that, whereas Schneier begins by making a point about the limits of deterrence, his criticism is ultimately directed at the TSA's inability to detect and interdict.

[74] U.S. DEP'T OF HOMELAND SEC., NATIONAL STRATEGY FOR AVIATION SECURITY 18 (2007), *available at* http://www.hsdl.org/?collection/stratpol&id=4.

[75] JACKSON ET AL., *supra* note 38, at 82.

[76] *See, e.g.*, Thomas Frank, *Most Fake Bombs Missed by Screeners; 75% Not Detected at LAX; 60% at O'Hare*, USA TODAY, Oct. 18, 2007, at A1, *available at* http://usatoday30.usatoday.com/travel/news/2007-10-17-airport-security_N.htm ("Security screeners at two of the nation's busiest airports failed to find fake bombs hidden on undercover agents posing as passengers in more than 60% of tests last year . . . ."). Even if domestic security checkpoints provided absolute protection, terrorist groups can and have identified new vulnerabilities by threatening, for example, international cargo flights into the United States.

[77] For such a discussion, see *infra* Subpart III.B.

B. Secrecy and Stings

For the last decade, analysis of national security law has largely assumed that officials try to maximize the secrecy of their work. Whether by (over)classifying work product,[78] evading congressional overseers,[79] prosecuting leakers,[80] invoking the State Secrets privilege in civil litigation,[81] or maintaining the secrecy of executive-[82] or judicial-branch[83] lawmaking, national security officials consistently have resisted calls for greater transparency[84]—or so the conventional story goes.

New deterrence confounds that story. Effective counterterrorism strategy also requires transparency. But new-deterrence transparency is about more than robust decisionmaking processes and effective

---

[78] *See, e.g.*, ELIZABETH GOITEIN & DAVID M. SHAPIRO, BRENNAN CTR. FOR JUSTICE, REDUCING OVERCLASSIFICATION THROUGH ACCOUNTABILITY 7–11 (2011), *available at* http://www.brennancenter.org/publication/reducing-overclassification-through-accountability (explaining how frequent "overclassification" prevents federal agencies from sharing information and precludes the public debate necessary for democratic government).

[79] When testifying before the Senate Select Committee on Intelligence in March 2013, the Director of National Intelligence, James R. Clapper, made it clear that he was no fan of greater transparency or oversight, stating, "An open hearing on intelligence matters is something of a contradiction in terms." Mark Mazzetti & David E. Sanger, *Security Chief Says Cyberattacks Will Meet with Retaliation*, N.Y. TIMES, Mar. 13, 2013, at A4.

[80] *See, e.g.*, David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512, 513–18 (2013) (discussing how the lack of prosecutions of those who leak secret governmental information can be seen as a tool used by the executive branch).

[81] *See, e.g.*, Fazaga v. FBI, 884 F. Supp. 2d 1022, 1028–29 (C.D. Cal. 2012) (finding for the government on state secrets grounds in a lawsuit challenging FBI surveillance of Muslim communities in southern California).

[82] *See* Charlie Savage & Scott Shane, *Memo Cites Legal Basis for Killing U.S. Citizens in Al Qaeda*, N.Y. TIMES, Feb. 5, 2013, at A6, *available at* http://www.nytimes.com/2013/02/05/us/politics/us-memo-details-views-on-killing-citizens-in-al-qaeda.html (describing the nonrelease of the Office of Legal Counsel's memo justifying the killing of Anwar al-Aulaqi). *But see* Mark Mazzetti & Scott Shane, *Memos Spell Out Brutal C.I.A. Mode of Interrogation*, N.Y. TIMES, Apr. 17, 2009, at A1, *available at* http://www.nytimes.com/2009/04/17/us/politics/17detain.html (describing President Obama's decision to release torture memos from the Office of Legal Counsel penned during the Bush Administration).

[83] *See, e.g.*, Letter from Dianne Feinstein, U.S. Senator, et al., to John D. Bates, Presiding Judge, Foreign Intelligence Surveillance Court (Feb. 13, 2013), *available at* http://graphics8.nytimes.com/packages/pdf/opinion/batesletter.pdf (requesting that sections of the opinions of the Foreign Intelligence Surveillance Court containing legal analysis be declassified under established procedure in order to inform public debate over FISA).

[84] *See generally* Laura K. Donohue, *The Shadow of State Secrets*, 159 U. PA. L. REV. 77 (2010) (analyzing how state secrets doctrine is invoked both by the government and private actors); Stephen J. Schulhofer, *Secrecy and Democracy: Who Controls Information in the National Security State?* (N.Y.U. Pub. L. & Legal Theory, Working Paper No. 217, 2010) (discussing the history of secrecy within the executive branch, the legislative branch's constrained ability to check improper secrecy, and strategies for change going forward).

oversight;[85] it is ultimately about communication with the adversary,[86] which cannot occur exclusively in secret.[87] As two proponents of DbD have written,

> The United States can . . . publicize the extensiveness and depth of its homeland security measures. Perhaps, more importantly, the United States should put aside excessive concerns with secrecy and become more willing to publicize foiled attacks. Broadcasting examples of the terrorists who fail could encourage potential terrorists to reassess the likelihood that their own plot will succeed.[88]

This observation generalizes across the broad landscape of deterrence-based counterterrorism, where success depends on a mixture of secrecy and transparency.[89] To be sure, certain government officials prize secrecy well past the point of necessity, and motivating much of the concealment are bureaucratic, political, and personal logics, rather than strategic rationales.[90] But many contemporary counterterrorism practices are hiding in plain sight.[91]

To take the most banal example, measures like subway searches or airport screenings are hardly invisible. Even a nominally covert program like drone warfare is so prominent in parts of Pakistan as to

---

[85] *Cf*. Seth F. Kreimer, *Rays of Sunlight in a Shadow "War": FOIA, the Abuses of Anti-Terrorism, and the Strategy of Transparency*, 11 LEWIS & CLARK L. REV. 1141, 1218–19 (2007) ("Given the volatility of information, it takes only one success to achieve disclosure, while efforts at concealment must be renewed with each threatened revelation.").

[86] *See* FRANKLIN E. ZIMRING & GORDON J. HAWKINS, DETERRENCE: THE LEGAL THREAT IN CRIME CONTROL 142 (1973) ("[T]he deterrence threat may perhaps best be viewed as a form of advertising.").

[87] *See* KENNEDY, *supra* note 33, at 41 ("What is not known cannot deter.").

[88] Kroenig & Pavel, *supra* note 10, at 30. Just how many foiled plots of this sort exist is open to question.

[89] For a game theoretic analysis of whether maintaining secrecy about defensive resource allocation is preferable, see Jun Zhuang & Vicki M. Bier, *Secrecy and Deception at Equilibrium, with Applications to Anti-Terrorism Resource Allocation*, 22 DEF. & PEACE ECON. 43 (2011).

[90] *See* Jameel Jaffer, Op-Ed., *Selective Secrecy; U.S. Officials Hurt Our Democracy by Withholding Information from the Courts but Then Disclosing It to the Public Whenever It Suits Their Needs*, L.A. TIMES, Apr. 6, 2011, at A17, *available at* http://articles.latimes.com/2011/apr/06/opinion/la-oe-jaffer-nationalsecurity-20110406 (positing that officials conceal information and then later disclose the very same information due to personal or political motivations).

[91] It is itself interesting that, in the face of this complicated reality, many observers of national security focus on what remains hidden. *See* Michael Sheehan, Statement at the Center on Law and Security: Secrecy Then and Now (Apr. 12, 2007), *in* SECRECY AND GOVERNMENT: AMERICA FACES THE FUTURE 22, 22–23 (2009), *available at* http://www.lawandsecurity.org/Portals/0/Documents/SecrecyPrivacy.pdf ("There are no secrets in Washington. . . . [B]ut there are temporarily held pieces of information that eventually get out that are very important.").

be a central fact of life for many who live there.[92] Whereas certain strategists criticize the drone fleet for being insufficiently stealthy,[93] new-deterrence thinking might dictate the opposite conclusion, namely that the perceptible presence of drones deters terrorist organizations by clearly communicating the existence and extent of the program. Regarding the administration's surveillance of financial transactions through the SWIFT clearinghouse,[94] Treasury officials "injected [broad discussions of financial surveillance] into any testimony" as "part of an explicit communications strategy to explain what [they] were doing without revealing the details of the methods [they] were using."[95]

Finally, it bears mentioning that the complicated relationship between secrecy and revelation demanded by new deterrence plays out in the legal arena as well.[96] On one level, public laws are exercises in revelation. For example, while reports of the details of the NSA Prism program created a sensation, the FISA Amendments Act of 2008 (hardly a secret document) seems to have authorized the collection in question.[97] On the other hand, legal interpretations that are

---

[92] *See* INT'L HUMAN RIGHTS & CONFLICT RESOLUTION CLINIC AT STAN. LAW SCH. AND GLOBAL JUSTICE CLINIC AT N.Y. UNIV. SCH. OF LAW, LIVING UNDER DRONES: DEATH, INJURY, AND TRAUMA TO CIVILIANS FROM US DRONE PRACTICES IN PAKISTAN 55, 80–99 (2012) [hereinafter LIVING UNDER DRONES], *available at* http://www.livingunderdrones.org/download-report/ (describing the impact of drone strikes on daily life, including the deleterious effects on mental health, access to education, and performing cultural traditions like proper burials).

[93] *See* James D. Perry, *Can Unmanned Aerial Systems Contribute to Deterrence?*, *in* DETERRENCE: RISING POWERS, ROGUE REGIMES, AND TERRORISM IN THE TWENTY-FIRST CENTURY 215, 230–31 (Adam B. Lowther ed., 2012) (explaining the reasons why the United States should increase its stealthy drone fleet after noting that "[a] major capability shortfall of the proposed hunter-killer fleet is that neither the Predator nor the Reaper is stealthy").

[94] The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a member-owned cooperative headquartered in Belgium. It provides a network enabling over 10,000 financial institutions and corporations to send and receive information regarding financial transactions.

[95] JUAN C. ZARATE, TREASURY'S WAR: THE UNLEASHING OF A NEW ERA OF FINANCIAL WARFARE 59 (2013). Although the White House sought to maintain the secrecy of the particulars of the program, it simultaneously anticipated and prepared for their revelation through a leak. *See* Juan C. Zarate, *New York Times and Terrorism: When Lapdogs Roar*, SALON (Sept. 7, 2013, 11:00 AM), http://www.salon.com/2013/09/07/new_york_times_and_terrorism_when_lapdogs_roar.

[96] *See* Elizabeth S. Anderson & Richard H. Pildes, *Expressive Theories of Law: A General Restatement*, 148 U. PA. L. REV. 1503, 1531–64 (2000) (arguing that "expressive considerations" provide the best explanation for constitutional law in the contexts of the Equal Protection Clause, the Establishment Clause, the Dormant Commerce Clause, and federalism).

[97] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISA Amendments Act of 2008), Pub. L. No. 110-261, § 702, 112 Stat. 2436, 2438 (codified at 50 U.S.C. § 1881a (2006 & Supp. I 2008)); *cf.* Rascoff, *supra* note 68, at 639–43 (explaining

crucial to the oversight of national security programs—such as opinions of the Foreign Intelligence Surveillance Court (FISC)[98] or the Justice Department's memorandum authorizing a lethal strike against American citizen Anwar al-Aulaqi[99]—have been withheld. Part of the reasoning is that these legal analyses themselves contain secrets or that in a world in which government is expected to operate at the outer limits of legal authority,[100] to disclose those limits publicly is, in effect, to reveal national security secrets. On this view, to maintain strategic ambiguity, it is necessary to be vague about legal interpretation.[101] In sum, new deterrence subtly refocuses the debate

---

that the FISA Amendments Act of 2008 allowed for programmatic surveillance of certain telephone calls and emails for foreign intelligence purposes).

98 *See* RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 207 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf ("[I]n order to further the rule of law, FISC opinions or, when appropriate, redacted versions of FISC opinions, should be made public in a timely manner, unless secrecy of the opinion is essential to the effectiveness of a properly classified program.").

99 The Department of Justice eventually released publicly a white paper, previously distributed to Congress, that sets out its core legal theory. DEP'T OF JUSTICE, LAWFULNESS OF A LETHAL OPERATION DIRECTED AGAINST A U.S. CITIZEN WHO IS A SENIOR OPERATIONAL LEADER OF AL-QA'IDA OR AN ASSOCIATED FORCE, *available at* http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf. On April 2, 2014, a unanimous panel of the United States Court of Appeals for the Second Circuit ordered the release of a redacted version of the memorandum. New York Times Co. v. U.S. Dep't of Justice, No. 13-422 L, 2014 WL 1569514, at *1 (2d Cir. Apr. 21, 2014).

100 In a 2007 speech, then-CIA Director Michael Hayden expressed this tendency:

> At a confirmation hearing a couple of years ago, one of the senators asked if I would respect American civil liberties in carrying out my intelligence tasks. I, of course, said that I would. I also told him that I had a duty to play aggressively—right up to the line. Playing back from the line protected me but didn't protect America. I made it clear I would always play in fair territory, but that there would be chalk dust on my cleats.

Michael V. Hayden, Former Dir., CIA, Commencement Address at Duquesne University (May 4, 2007), *available at* https://www.cia.gov/news-information/speeches-testimony/2007/cia-directors-address-at-duquesne-university-commencement.html (internal quotation marks omitted) (last updated June 20, 2008, 8:49 AM).

101 *See generally* Jack Goldsmith, *The Irrelevance of Prerogative Power, and the Evils of Secret Legal Interpretation*, *in* EXTRA-LEGAL POWER AND LEGITIMACY PERSPECTIVES ON PREROGATIVE (Clement Fatovic & Benjamin A. Kleinerman eds., 2013) (discussing disincentives for the executive branch to disclose legal interpretations of national security matters in the context of promoting a transparent regime for executive branch officials). Proponents of secret law can carry their arguments too far. A recent example is the Pentagon's claim that categorizing particular terror groups as covered by the 2001 Authorization for the Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001), would be strategically disadvantageous because group members would be emboldened by that status. *See* Cora Currier, *Who Are We at War With? That's Classified*, PROPUBLICA (July 26, 2013), http://www.propublica.org/article/who-are-we-at-war-with-thats-classified (reporting that Pentagon officials have stated that releasing such a list would allow terrorist forces to build credibility); *see also* Jack Goldsmith, *DOD's Weak Rationale for Keeping*

away from a zero-sum contest between secrecy and transparency and toward a more nuanced account.

One of the most contentious counterterrorism practices has been arresting terrorism suspects as part of sting operations.[102] Unsurprisingly, officials champion the practice, lauding the benefits of thwarted plots.[103] Critics, meanwhile, argue that sting operations do not detect serious would-be terrorists so much as manufacture unconvincing ones;[104] accordingly, they often call for a reinvigoration of the entrapment defense.[105]

Although these two (admittedly stylized) accounts reach very different conclusions, they share a key assumption: Both treat incapacitation as the measure of a sting operation's value. New deterrence instructs that this premise misses the mark. The value of sting operations (and the prosecutions based on them) may inhere beyond preventing discrete attacks in the messages they send to would-be terrorists. The sting operation might be understood as the visible part of an otherwise largely hidden surveillance regime.[106]

Enemy Identities Secret, LAWFARE (July 26, 2013, 11:07 AM), http://www.lawfareblog.com/2013/07/dods-weak-rationale-for-keeping-enemy-identities-secret/ (criticizing the notion that the identities of United States enemies should be kept secret). But opponents often paper over the strategic benefits of secret law. For example, one commentator argues that, "in order for drones to have a deterrent effect, the United States's adversaries need to know that it can and will impose a cost if they take a particular course of action," which is impossible if those adversaries "don't understand U.S. policy or don't even know whether they are being targeted." Job C. Henning, *Embracing the Drone*, INT'L HERALD TRIB., Feb. 21, 2012, at 6. And Professor Kitrosser argues that "[o]n a practical level, it is difficult to imagine why knowledge of the precise legal framework for conducting covert surveillance would advantage terrorists who already know that they can be spied on covertly." Heidi Kitrosser, *"Macro-Transparency" as Structural Directive: A Look at the NSA Surveillance Controversy*, 91 MINN. L. REV. 1163, 1200–01 (2007). For the reasons stated above, these strategic conclusions are open to question.

102 *See generally* Jacqueline E. Ross, *The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany*, 55 AM. J. COMP. L. 493, 496–97, 503–07, 511–13 (2007) (analyzing and critiquing aspects of undercover policing).

103 *See, e.g.*, Press Release, Dep't of Justice, Oregon Resident Convicted in Plot to Bomb Christmas Tree Lighting Ceremony in Portland (Jan. 31, 2013), *available at* http://www.justice.gov/opa/pr/2013/January/13-nsd-141.html ("I applaud all those who worked so diligently to thwart this plot and ensure no one was harmed." (quoting Lisa Monaco, Assistant Attorney Gen. for Nat'l Sec.)).

104 *See, e.g.*, CTR. FOR HUMAN RIGHTS & GLOBAL JUSTICE, N.Y. UNIV. SCH. OF LAW, TARGETED AND ENTRAPPED: MANUFACTURING THE "HOMEGROWN THREAT" IN THE UNITED STATES 2–3 (2011), *available at* http://chrgj.org/wp-content/uploads/2012/07/targetedandentrapped.pdf (arguing that government agents incited or pressured defendants to participate in terrorist plots devised by the government).

105 *See id.* at 15–18, 39–40 (discussing an objective standard for determining entrapment, rather than the subjective standard currently used by the U.S. legal system).

106 *See* ANDREW SONG, TECHNOLOGY, TERRORISM, AND THE FISHBOWL EFFECT: AN ECONOMIC ANALYSIS OF SURVEILLANCE AND SEARCHES 18 (2003), *available at* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2003-04.pdf (listing several

Taken together, these overt and covert phenomena allow the government to maintain deterrence through a combination of straightforward messaging and bluffing.[107]

As Cato Institute Research Fellow Julian Sanchez observed:

> One possible motive for these elaborate and highly publicized stings is that, whether or not the particular people they indict would have moved from rage to action without prompting, the steady stream of news reports will eventually force any candidate for jihad to assume that an "Al Qaeda recruiter" who approaches them is *much* more likely to be an FBI informant or undercover agent than a genuine operative. That's likely to make it much harder for any real recruiters who've gone undetected to rope in anyone savvy enough to be truly dangerous.[108]

An open question—an answer to which requires more empirical data—is whether the government's prosecution of relatively amateur would-be terrorists based on stings is likely to be effective in deterring better-trained terrorists.[109] But it bears remembering that the viability

---

limitations to the government's ability to use secret surveillance to prevent harm through official interventions). Song overstates the case in claiming that "[t]he consequence is a loss in social welfare due to privacy disutility and avoidance . . . [with] no corresponding benefit from an increase in public safety because there is no actual surveillance." *Id.* The FBI has historically aimed to employ fear of even nonexistent surveillance as an instrument of power. *See* Mark Mazzetti, *Burglars Who Took On F.B.I. Abandon Shadows*, N.Y. TIMES, Jan. 7, 2014, at A1 (stolen FBI documents spoke of the need to "enhance the paranoia" and foster the impression that there's an "F.B.I. agent behind every mailbox"). That said, Song is correct that this approach raises important normative issues because "[i]ndividuals may begin to (rationally) suspect that there is some possibility of surveillance even when in fact there is none." SONG, *supra*, at 18.

107 *See, e.g.*, THOMAS C. SCHELLING, ARMS AND INFLUENCE 35 (1966) (discussing how nations both make sincere threats and bluff in their quest for deterrence). Early in his career, Schelling favored ambiguous pronouncements as part of successful deterrence. *See* LONG, *supra* note 3, at 9 (explaining that Schelling thought deterrence is "often enhanced by not being entirely clear in declaratory threats"). One example of such a deterrence policy was Saddam Hussein's attempt at "deterrence by doubt." *Id.* at 73. Caught between threats from the United States (pushing for compliance with nuclear inspections) and regional threats from Iran and fellow Iraqis, Saddam tried to maintain an ambiguous policy on WMDs, but he ultimately failed. *Id*.

108 Julian Sanchez, *Why Sting?*, JULIANSANCHEZ (Sept. 30, 2011), http://www.juliansanchez.com/2011/09/30/why-sting/. Relatedly, the FBI's involvement in defanging the Ku Klux Klan included the perception that government agents had penetrated the organization. The Klan's awareness of deep penetration by undercover agents and informants guaranteed high levels of internal paranoia and difficult organizational mobilization. *See* DAVID CHALMERS, BACKFIRE: HOW THE KU KLUX KLAN HELPED THE CIVIL RIGHTS MOVEMENT 97–98, 151 (2003) (noting the government's attempt to project that "one out of every six Klansmen worked for the FBI").

109 This is really a specific application of a familiar puzzle in the literature on stings. *See, e.g.*, Robert H. Langworthy, *Do Stings Control Crime? An Evaluation of a Police Fencing Operation*, 6 JUST. Q. 27, 27 (1989) (finding generally that the stings evaluated had a "negative environmental impact" and served "reflexive . . . police organizational goals").

of the deterrence-based account of stings does not depend on who is prosecuted. The mere fact of prosecution can alter terrorists' perceptions of future success by implying a pervasive surveillance network[110] facilitated by technology.[111] As Alex Wilner observed of Canadian counterterrorism, the fact that the country's "intelligence community clearly has the means and the tools to uncover plots expeditiously" creates an "overwhelming perception . . . that terrorists are unlikely to evade Canada's watchful eye."[112] In sum, the meaning of a sting operation and subsequent trial must include the strategic benefits of revealing the fact of undercover surveillance as well as the normative costs implied by widespread surveillance.[113] This in turn illustrates the

[110] *See* MORRAL & JACKSON, *supra* note 28, at 23–24 ("[T]he possible existence of [counterterrorism] programs may cast a heavy cloud of uncertainty over the success probability [of terrorist activities], with discouraging results for operational planners."). Of course, signaling can go wrong for the government, especially when it cedes its monopoly on the message. *See, e.g.*, Jon D. Michaels, *Deputizing Homeland Security*, 88 TEX. L. REV. 1435, 1459–60 & n.122 (2010) (raising concerns about the manner in which private contractors are made part of counterterrorism operations and noting how their involvement may end up disserving some of the government's national security interests).

[111] *See* Cara Buckley, *Police Plan Web of Surveillance for Downtown*, N.Y. TIMES, July 9, 2007, at A1 (noting the advent of "an extensive web of cameras and roadblocks designed to detect, track and deter terrorists" in New York City). While the "Ring of Steel" did not prevent the London attacks of July 7, 2005, the surveillance system remains a significant element of Britain's counterterrorism strategy. *See Anti-Terror Crackdown in the City*, COURIER (Feb. 11, 2014, 9:58 AM), http://www.thecourier.co.uk/business/news/anti-terror-crackdown-in-the-city-1.213970 (describing the City of London Police's continued use of the Ring of Steel and plans to improve its deterrent effect). For a prescient analysis of the privacy issues pervasive surveillance implicates, see Jennifer Mulhern Granholm, *Video Surveillance on Public Streets: The Constitutionality of Invisible Citizen Searches*, 64 U. DET. L. REV. 687 (1987).

[112] Alex Wilner, *Canada's Counter-Terrorism Strategy: Deterrence Through Disclosure*, EMBASSY, Feb. 10, 2012, http://www.embassymag.ca/dailyupdate/view/canadas_counterterrorism_strategy_deterrence_through_disclosure_02-10-2012. More generally, as a British official has explained, "deterrence can be achieved by overt activity intended to counter the terrorist at the reconnaissance, preparation, attack, and escape phases." MORRAL & JACKSON, *supra* note 28, at 18 (quoting David Veness, *Low Intensity and High Impact Conflict*, TERRORISM & POL. VIOLENCE, Winter 1999, at 14).

[113] Some scholarship in criminal law considers undercover policing and prosecutions in the context of counterterrorism. *See* Bruce Hay, *Sting Operations, Undercover Agents, and Entrapment*, 70 MO. L. REV. 387, 395–96, 417–19 (2005) (discussing how criminal sting operations sometimes include possible terrorist suspects as part of a larger analysis of the costs and benefits of sting operations); Stevenson, *supra* note 52, at 161–62 (explaining how sting operations are one way in which national security logic has affected criminal law). Hay, for example, states that

> When deterrence is the objective, the government creates something akin to the well-known market for lemons. The government introduces lemons—phony criminal opportunities—that resemble the genuine article. To the would-be offender, the risk of being caught in a trap makes it costlier to seize apparent opportunities for crime. . . . Governments can take steps to encourage this fear, sometimes even spreading false or exaggerated rumors of the existence of sting operations.

complicated relationship between transparency and secrecy entailed by new deterrence.

C. Psychology and Strikes

New deterrence also enriches understanding of the role of fear and emotion in counterterrorism. Terrorism aims at communicating vulnerability and sowing distrust; violent attacks are, in a sense, means to bring about these more intangible objectives.[114] (Thus, building sufficient social resiliency to withstand terrorist attacks, as new deterrence counsels, deprives terrorists of an important goal, even when an attack succeeds.[115]) But fear[116] and distrust are also part of the counterterrorism repertoire.[117] Inevitably this fact raises serious

---

Hay, *supra*, at 412–13; *see also* Shirin Sinnar, *Questioning Law Enforcement: The First Amendment and Counterterrorism Interviews*, 77 BROOK. L. REV. 41, 67–68 (2011) ("The Department of Justice explained its post-9/11 interviews of several thousand Arab immigrants as an attempt to . . . ensure[ ] that potential terrorists sheltering themselves within our communities were aware that law enforcement was on the job in their neighborhoods." (internal quotation marks omitted)). Stevenson discusses stings as mechanisms for deterring terrorist activity, noting that rather than pursuing deterrence by punishment, "newer methods boost the up-front transaction costs of committing crimes." Stevenson, *supra* note 52, at 140–41.

114 Those intangible purposes, in turn, are likely subordinate to more long-term political or social objectives. *See* Jeremy Waldron, *Terrorism and the Uses of Terror*, 8 J. ETHICS 5, 8–9, 16–17 (2004) (characterizing terrorism as a mode of coercion in which the actor imposes some of the threatened costs before making political or social demands).

115 Thus Adam Garfinkle's useful admonition:

> We need to stop taking overboard steps that show we're afraid, which tell every potential terrorist, whether domestic or foreign, that it's easy to scare Americans—that all you have to do is frighten the Americans once, and they'll do extremely expensive and counterproductive things, essentially bureaucratizing and thus perpetuating their own paranoia.

Garfinkle, *supra* note 22. In Israel, one study found that a decrease in media "disaster marathon[ing]" during the Second Intifada as compared with the First resulted in greater societal resiliency. Tamar Liebes & Zohar Kampf, *Routinizing Terror: Media Coverage and Public Practices in Israel, 2000–2005*, 12 HARV. INT'L J. PRESS & POL. 108, 109–11, 114 (2007).

116 Jon Elster has described two kinds of fear—one that is essentially an input for a cost-benefit analysis and another that is experienced more viscerally. JON ELSTER, ALCHEMIES OF THE MIND: RATIONALITY AND THE EMOTIONS 233 (1999).

117 *Cf.* Cusson, *supra* note 53, at 56 ("Deterrence is the inhibiting influence that fear exercises over the potential [criminal] offender."). More generally, the use of psychological techniques is a key element of warfare. *See* Joshua E. Kastenberg, *Tactical Level PSYOP and MILDEC Information Operations: How to Smartly and Lawfully Prime the Battlefield*, 2007 ARMY LAW. 61, 61 & n.6, 63 (2007) (explaining some of the psychological operations conducted by the federal government); Peter J. Smyczek, *Regulating the Battlefield of the Future: The Legal Limitations on the Conduct of Psychological Operations (PSYOP) Under Public International Law*, 57 A.F. L. REV. 210, 219–20 (2005) (describing the history behind PSYOP and explaining that "deception[ ] and intimidation go hand in hand with armed combat and have been used throughout the ages by some of history's most successful armies").

normative issues. First is the foundational question of what it means for the state to manage terrorist risk through the potentially widespread, deliberate employment of fear.[118] Rich sociological and historical literature attest to the emotional costs of aggressive national security tactics.[119] Second is a concern about the distribution of fear and whether the government considers race and religion when employing it.[120] My central point here, however, is not normative so much as conceptual: Whereas policymakers, lawyers, and the general public often define counterterrorism as the sum of so many violent interventions, new deterrence reminds us that counterterrorism also operates in a psychological register.

Unlike traditional deterrence, which conveys its message through fear of being caught and punished, new deterrence relies on a wider and subtler range of official modalities that go to the likelihood of terrorist success. For example, the government may aim to demoralize an adversary by telegraphing the state's overwhelming might. The state might do so by "spreading false or exaggerated rumors of the

---

[118] *See* Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 121–22 (2008) (arguing that the Fourth Amendment centrally enshrines not a guarantee of privacy but a right of security); *see also* Stuart Macdonald, *Why We Should Abandon the Balance Metaphor: A New Approach to Counterterrorism Policy*, 15 ILSA J. INT'L & COMP. L. 95, 98, 107–13 (2008) (distinguishing between the objective and subjective senses of security in the context of counterterrorism policy and drawing on psychology and sociology to argue that "the aim of counterterrorism legislation should be to increase objective security").

[119] *See, e.g.*, David Cunningham & John Noakes, *"What If She's from the FBI?" The Effects of Covert Forms of Social Control on Social Movements*, *in* SURVEILLANCE AND GOVERNANCE: CRIME CONTROL AND BEYOND 175, 186–91 (Mathieu Deflem ed., 2008) (examining the "relationship between emotion and covert forms of social control" and arguing that "the targets of surveillance, infiltration, and counterintelligence activities often suffer a significant emotional toll that shapes social movement dynamics").

[120] *See* Complaint at 1, Raza v. City of New York, No. 13-cv-03448 (E.D.N.Y. June 18, 2013), *available at* http://www.aclu.org/files/assets/nypd_surveillance_complaint_final.pdf (alleging that the NYPD used religious profiling in its surveillance of New Yorkers who were Muslim); *see also* Hina Shamsi & Patrick C. Toomey, *ACLU Sues NYPD over Unconstitutional Muslim Surveillance Program*, ACLU BLOG RTS. (June 18, 2013, 10:14 AM), http://www.aclu.org/blog/national-security-religion-belief-technology-and-liberty-criminal-law-reform/aclu-sues-nypd (reporting on *Raza*). The complaint alleges that NYPD surveillance targeting the entire Muslim community (provocatively termed the "Muslim Surveillance Program" in the complaint) is based on the "false and unconstitutional premise[ ] that Muslim religious beliefs and practices are a basis for law enforcement scrutiny" in the absence of individualized suspicion of criminal activity. Complaint, *supra*, at 1–2. The complaint alleges that the activities in question have failed to generate a single lead while imposing stigma and suspicion on hundreds of thousands of Muslim New Yorkers. *See id*. at 2 (noting that the program has put an "unwarranted badge of suspicion and stigma" on Muslims); *cf.* Michael S. Schmidt, *Report Says T.S.A. Screening Is Not Objective*, N.Y. TIMES, June 5, 2013, at A17 (discussing a Department of Homeland Security Inspector General report claiming that putatively behavioral methods for screening at airports may, in fact, rely on profiling).

existence of sting operations,"[121] sowing a sense of distrust within a cell by implying that one among them is on an official payroll, or even conveying an image of officials as irrational and prone to unmeasured violence.[122]

These tendencies are illustrated by drone warfare, which has emerged as one of the most contentious features of American counterterrorism over the last five years,[123] generating debate about the morality of killing remotely,[124] the legality of the practice under international and domestic law,[125] the allocation of power within government to execute and oversee drone strikes,[126] and the net utility of the practice.[127]

---

121 Hay, *supra* note 113, at 413.

122 *Cf.* SCHELLING, *supra* note 107, at 37 ("[I]t does not always help to be, or to be believed to be, fully rational, cool-headed, and in control of oneself or one's country."). Schelling cites Khrushchev's famous outburst at the General Assembly as an example of a deliberately created irrational persona, intended to increase uncertainty as to his potential behavior toward the United States. *Id.* at 39.

123 *See, e.g.*, PATRICK B. JOHNSTON & ANOOP K. SARBAHI, THE IMPACT OF US DRONE STRIKES ON TERRORISM IN PAKISTAN AND AFGHANISTAN 2–3 (2013), *available at* http://patrickjohnston.info/materials/drones.pdf (noting that drone strikes are a key policy concern); Kenneth Anderson, *The Case for Drones*, COMMENT. MAG., June 2013, at 14–15 (reporting that drone warfare has come under increasing attack from both liberals and conservatives).

124 *See, e.g.*, Scott Shane, *The Moral Case for Drones*, N.Y. TIMES, July 15, 2012, at SR4 (noting that the morality of drone warfare has sparked spirited debate).

125 *See* Philip Alston, *The CIA and Targeted Killings Beyond Borders*, 2 HARV. NAT'L SECURITY J. 283, 286–87 (2011) (arguing that the CIA drone program operates in violation of international law); *see also* LIVING UNDER DRONES, *supra* note 92, at 103–18 (discussing aspects of international law pertinent to the use of drones); Charlie Savage, *At White House, Weighing Limits of Terror Fight*, N.Y. TIMES, Sept. 16, 2011, at A1, *available at* http://www.nytimes.com/2011/09/16/us/white-house-weighs-limits-of-terror-fight.html (discussing a disagreement between Jeh Jonson, then General Counsel at the Department of Defense, and Harold Koh, then Legal Adviser at the State Department, as to the legal scope of the conflict with Al Qaeda and who could be targeted for killing and where).

126 *See, e.g.*, Jens David Ohlin, *The Duty to Capture*, 97 MINN. L. REV. 1268, 1326–29 (2013) (discussing a potential role for neutral arbiters in the legitimacy of targeted killing).

127 *See* Audrey Kurth Cronin, *Why Drones Fail: When Tactics Drive Strategy*, FOREIGN AFF. July–Aug. 2013, at 44, *available at* http://www.foreignaffairs.com/articles/139454/audrey-kurth-cronin/why-drones-fail (contending that devoting resources to the drone program entails significant opportunity costs and undermines the goal of defeating al-Qaeda). President Obama recently discussed the strategic, ethical, and legal implications of drone strikes:

> [I]t is a hard fact that U.S. strikes have resulted in civilian casualties, a risk that exists in every war. And for the families of those civilians, no words or legal construct can justify their loss. For me, and those in my chain of command, those deaths will haunt us as long as we live, just as we are haunted by the civilian casualties that have occurred throughout conventional fighting in Afghanistan and Iraq. But as Commander-in-Chief, I must weigh these heartbreaking tragedies against the alternatives.

One of the defining features of debates surrounding drone strikes is an asymmetry in their structure. Proponents of the practice typically define success as killing specific known terrorists while critics argue that "[Al] Qaeda officials who are killed by drones will be replaced. The group's structure will survive and it will still be able to inspire, finance and train individuals and teams to kill Americans."[128] Critics also point to potential strategic downsides (putting aside the more obvious legal and ethical issues),[129] including radicalizing local populations against the United States.[130]

Missing from these debates is an awareness of how drone warfare participates in new deterrence,[131] with strategic success defined not merely by reference to incapacitating individual terrorists but also by deterring terrorists from joining the fight in the first place.[132]

Barack Obama, U.S. President, Remarks by the President at the National Defense University (May 23, 2012, 2:01 PM), *available at* http://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university.

128 Dennis C. Blair, *Drones Alone Are Not the Answer*, N.Y. TIMES, Aug. 15, 2011, at A21, *available at* http://www.nytimes.com/2011/08/15/opinion/drones-alone-are-not-the-answer.html. Regional experts, such as Yemen scholar Greg Johnsen, have expressed similar views. *See* Gregory D. Johnsen, *The Wrong Man for the C.I.A.*, N.Y. TIMES, Nov. 20, 2012, at A27, *available at* http://www.nytimes.com/2012/11/20/opinion/john-brennan-is-the-wrong-man-for-the-cia.html (arguing that John Brennan's nomination as CIA Director was a mistake because of his heavy involvement in the drone program, which has assisted Al Qaeda's recruiting efforts in Yemen).

129 American officials tout the accuracy of drones, sometimes advancing claims about their virtual infallibility. John Brennan, while serving as the President's senior advisor on counterterrorism, expressed the view that drone strikes had led to no civilian casualties. Scott Shane, *C.I.A. Is Disputed on Civilian Toll in Drone Strikes*, N.Y. TIMES, Aug. 12, 2011, at A1, *available at* http://www.nytimes.com/2011/08/12/world/asia/12drones.html?pagewanted=all&_r=0.

130 *See* Cronin, *supra* note 127, at 44 ("Although they can protect the American people from attacks in the short term, they are not helping to defeat al Qaeda, and . . . may be creating sworn enemies out of a sea of local insurgents. It would be a mistake to embrace killer drones as the centerpiece of U.S. counterterrorism."). David Carter recently argued that terrorists pursue "a strategy of provocation" by "carry[ing] out attacks that elicit a forceful response which harm civilians more than group members, helping groups gain support and power." David B. Carter, Provocation and the Strategy of Terrorist and Guerilla Attacks 3 (Aug. 24, 2013) (unpublished manuscript), *available at* http://www.iilj.org/courses/documents/Carter_strategicterror.pdf.

131 As former CIA Director Michael Hayden explained, "[b]y making a safe haven feel less safe, we keep al Qaeda guessing. We make them doubt their allies, question their methods, their plans, even their priorities." Perry, *supra* note 93, at 229.

132 As Shanker and Schmitt have written, while "[t]he immediate, tactical goal [i]s to bring about the death of Al Qaeda leaders," the drone campaign has "proved to be a deterrent in itself, pushing Al Qaeda senior leaders deeper into hiding, preventing their gathering together, and keeping them constantly on alert, in motion, and off balance." SCHMITT & SHANKER, *supra* note 7, at 241. Indeed, a recent RAND study found "evidence that drone strikes might have a deterrent effect that lasts between two and five weeks." JOHNSTON & SARBAHI, *supra* note 123, at 24.

Indeed, there is evidence that the drone program has caused changes in behavior on the ground. According to Foust, "drone strikes have resulted in three broad changes to terrorist group behaviors: rejecting technology, going into hiding, and violently attacking those suspected of participating in the targeting process."[133] The relentless presence of drones above certain areas may drain terrorist organizations of their resolve and convince them of the United States's steadfast intent to disrupt their activities.[134] The journalist Pir Zubair Shah tells a particularly evocative story of his time spent among militants in Pakistan:

> On the other side of the Tochi River, in the village of Khatai, lived a famous Taliban commander whom the Pakistani military had once tried to kill. The operation had been a debacle; the military lost at least two senior officers, and hundreds of soldiers found themselves besieged not only by Taliban fighters but by the local villagers. But the small, lethal machine flying far overhead had accomplished what the Pakistani soldiers could not. "Nowadays he doesn't live here all the time," my host that night said as he pointed toward the commander's nearby compound. "There are drones in the air now."[135]

This is hardly to suggest that the presence of certain strategic benefits outweighs strategic downsides, even setting aside entirely urgent questions of law and morality. But it is intended to recognize that debates about drone warfare have largely ignored a crucial component of the practice that is clarified by new deterrence.

III
Doctrinal and Institutional Barriers

The current legal architecture of national security supplies an inadequate foundation and means of oversight for new-

---

133 Joshua Foust, Am. Sec. Project, Understanding the Strategic and Tactical Considerations of Drone Strikes 10 (2013), *available at* http://www.scribd.com/doc/121483783/Understanding-the-Strategic-and-Tactical-Considerations-of-Drone-Strikes.

134 *See* Gabriella Blum & Philip Heymann, *Law and Policy of Targeted Killing*, 1 Harv. Nat'l Security J. 145, 167 (2010) ("[T]he demonstration of superiority in force and resolve may . . . dishearten the supporters of terrorism."). Blum and Heymann argue that drones can deter "[d]espite the adverse effects such operations may have on the attitudes of the local population toward the country employing targeted killings," *id.*, thus incorporating deterrence into the cost-benefit analysis of an earlier-noted argument, *see supra* note 130 and accompanying text (referencing the argument of some commentators that drone attacks harm the United States by radicalizing local populations).

135 Pir Zubair Shah, *My Drone War*, Foreign Pol'y (Feb. 27, 2012), http://www.foreignpolicy.com/articles/2012/02/27/my_drone_war.

deterrence–based counterterrorism.[136] This is true both at the level of judge-made doctrine[137] and institutional dynamics. I take up each in turn, highlighting conceptual and operational mismatches with emerging strategic realities.

A. Doctrine

Legal doctrine is insufficiently attuned to the strategic realities highlighted by new deterrence. I illustrate by reference to contemporary judicial opinions on Special Needs,[138] State Secrets,[139] and

---

[136] These goals need not—and indeed, should not—be viewed as mutually contradictory. *Cf.* Jack Goldsmith, *Reflections on NSA Oversight, and a Prediction that NSA Authorities (and Oversight, and Transparency) Will Expand*, LAWFARE (Aug. 9, 2013, 7:52 AM), http://www.lawfareblog.com/2013/08/reflections-on-nsa-oversight-and-a-prediction-that-nsa-authorities-and-oversight-and-transparency-will-expand/ ("[S]crupulous oversight and regulation of NSA *empowers and enhances its mission*."). In previous work, I have described these goals as converging under the banner of "governance." Rascoff, *supra* note 68, at 575–76. For critical takes on the familiar image of tradeoffs between security and liberty, see JEREMY WALDRON, TORTURE, TERROR, AND TRADE-OFFS: PHILOSOPHY FOR THE WHITE HOUSE 22–23 (2010) (arguing that there is a lack of precision used when balancing security and liberty).

[137] Perennial questions surround the proper roles of specialized courts in this area. *Compare* Jack L. Goldsmith & Neal Katyal, Op-Ed., *The Terrorists' Court*, N.Y. TIMES, July 11, 2007, at A19 ("A sensible first step is for Congress to establish a comprehensive system of preventive detention that is overseen by a national security court composed of federal judges with life tenure."), *with* Sophia Brill, Comment, *The National Security Court We Already Have*, 28 YALE L. & POL'Y REV. 525, 526 (2010) (arguing that the D.C. Circuit in effect performs this function). Of late, there has been considerable attention devoted in the press to the FISA court, including the manner in which judges are selected to serve on the tribunal. *See* Editorial, *More Independence for the FISA Court*, N.Y. TIMES, July 29, 2013, at A16, *available at* http://www.nytimes.com/2013/07/29/opinion/more-independence-for-the-fisa-court.html ("There are so many deeply troubling things about the Foreign Intelligence Surveillance Court that it is difficult to know where to begin, but a good place might be the method by which the court's judges are chosen."); *see also* Neal K. Katyal, Op-Ed., *Who Will Mind the Drones?*, N.Y. TIMES, Feb. 21, 2013, at A27, *available at* http://www.nytimes.com/2013/02/21/opinion/an-executive-branch-drone-court.html (arguing for a national security court located within the executive, rather than a "drone court" staffed by generalist federal judges in the judiciary).

[138] The doctrine stems from a concurrence by Justice Blackmun in which he argued that "[o]nly in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable, is a court entitled to substitute its balancing of interests for that of the Framers." New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring in the judgment).

[139] First articulated in *United States v. Reynolds*, the State Secrets privilege allows the government to prevent the disclosure of secret information related to national security in civil litigation. 345 U.S. 1, 7–8 (1953). The privilege is formally invoked by the head of the government department which controls the secret information. Judges "must determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege is designed to protect." *Id.* (footnote omitted).

standing[140] in the counterterrorism setting.

1. Special Needs

Special Needs doctrine invites courts to test the Fourth Amendment constitutionality of counterterrorism programs at scale, which would seem to offer a limited opportunity for courts to consider the new-deterrence foundations of counterterrorism programs. And indeed, although not inherently about national security,[141] the doctrine has figured prominently in the counterterrorism setting. Examples include court consideration of airport screening with magnetometers[142] or the FISA court's jurisprudence on bulk surveillance.[143] And yet, conceptual and practical problems in the application of Special Needs doctrine have limited its utility in overseeing contemporary counterterrorism.

Special Needs doctrine involves a two-part test. First, as a threshold matter, the immediate purpose of the challenged search must be distinct from the ordinary evidence-gathering associated with criminal investigation.[144] Second, once the government satisfies this

---

[140] *Lujan v. Defenders of Wildlife* provides the classic rendition of the elements of standing: (1) "an injury in fact," (2) that the injury "be fairly . . . trace[able] to the challenged action of the defendant," and (3) it must be "likely . . . that the injury will be redressed by a favorable decision." 504 U.S. 555, 560–61 (1992) (internal quotation marks omitted). *See generally* Heather Elliott, *The Functions of Standing*, 61 STAN. L. REV. 459 (2008) (discussing the function of each element of the standing doctrine).

[141] Special Needs has been applied in a wide range of settings, including sobriety checkpoints, Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 449–50 (1990), checkpoints designed to obtain information about hit-and-runs, Illinois v. Lidster, 540 U.S. 419, 427 (2004), and, recently, DNA testing of arrestees, Maryland v. King, 133 S. Ct. 1958, 1963, 1969, 1978, 1981–82 (2013).

[142] *See* United States v. Marquez, 410 F.3d 612, 617 (9th Cir. 2005) (reasoning that the screening was designed "first, to prevent passengers from carrying weapons or explosives onto the aircraft; and second, to deter passengers from even attempting to do so").

[143] *See In re* Directives Pursuant to Section 105B, 551 F.3d 1004, 1010–11 (FISA Ct. Rev. 2008) (holding that the special needs exception applies in the context of foreign surveillance); *see also* Jennifer Granick & Christopher Sprigman, *The Secret FISA Court Must Go*, DAILY BEAST (July 24, 2013), http://www.thedailybeast.com/articles/2013/07/24/the-secret-fisa-court-must-go.html (criticizing the FISA court's invocation of Special Needs in *In re Directives*). On the FISA court's Special Needs cases generally, see Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES, July 7, 2013, at A1, *available at* http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html.

[144] New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring in the judgment) ("Only in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable, is a court entitled to substitute its balancing of interests for that of the Framers."); *see also id.* at 357 (Brennan, J., concurring in part and dissenting in part) ("Only where the governmental interests at stake exceed those implicated in any ordinary law enforcement context . . . is it legitimate to engage in a balancing test to determine whether a warrant is indeed necessary.").

threshold requirement, the court must determine whether the search is reasonable by balancing several competing considerations.[145] As to the first prong, the question of what triggers analysis under Special Needs is increasingly conceptually confused in national security cases. As to the latter, the doctrine has proved relatively toothless in the face of executive branch claims of national security necessity. Thus, new-deterrence security claims raising issues of scale tend to confound the courts.

The Second Circuit's opinion in *MacWade v. Kelly*—perhaps the most fully reasoned (publicly available) national security Special Needs case—is illustrative.[146] The case grew out of a challenge to the NYPD's subway search program, which was designed "chiefly to deter terrorists from carrying concealed explosives onto the subway system and, to a lesser extent, to uncover any such attempt."[147] NYPD selects checkpoint locations and varies their location, number, staffing, and scheduling. The individual officers select travelers based on a predetermined selection rate, "search only those containers large enough to carry an explosive device," and search only to the extent needed to ensure there is no explosive device in the container.[148] Furthermore, the search program is part of a larger, deterrence-based approach to counterterrorism,[149] which includes "critical response vehicle surges" based on "intelligence and . . . analysis about which targets the terrorists may have under surveillance,"[150] combined with "Hercules"

---

145 "These balancing factors include (1) the weight and immediacy of the government interest; (2) the nature of the privacy interest allegedly compromised by the search; (3) the character of the intrusion imposed by the search; and (4) the efficacy of the search in advancing the government interest." MacWade v. Kelly, 460 F.3d 260, 269 (2d Cir. 2006) (citations omitted) (internal quotation marks omitted).

146 *See id.* at 267–69 (discussing prior case law upholding warrantless searches at airports because the purpose of these searches was not to prevent terrorists from hijacking planes and because the danger posed by terrorists plots was great).

147 *Id.* at 264.

148 *Id.* at 264–65. There is robust academic literature on "randomization" and the Fourth Amendment. *E.g.*, Bernard E. Harcourt & Tracey L. Meares, *Randomization and the Fourth Amendment*, 78 U. CHI. L. REV. 809 (2011).

149 *See* Raymond W. Kelly, *Safeguarding Citizens and Civil Liberties*, 59 RUTGERS L. REV. 555, 563 (2007) ("Other measures build on Richard Clarke's point that, when the terrorists can't know for certain what level of security will be in place at a given target, the chances of an attack diminish."); *see also* Katherine Lee Martin, *"Sacrificing the End to the Means": The Constitutionality of Suspicionless Subway Searches*, 15 WM. & MARY BILL RTS. J. 1285, 1292–93 (2007) ("The witnesses [in *MacWade*] maintained that terrorists prefer predictability and that random searches add unpredictability to the planning and implementation of an attack, which increases the risk of failure and ultimately encourages terrorists 'to choose . . . an easier target.'" (second alteration in original) (quoting *MacWade*, 460 F.3d at 266–67)).

150 Kelly, *supra* note 149, at 563; *see also* Francine Prose, *The Unthinkable, Right Around the Corner*, N.Y. TIMES, Jan. 27, 2008, at CY3 ("Every day, as many as 76 cars,

teams deployed to "pay sudden, unannounced visits to sensitive locations throughout the city."[151]

In passing on the constitutionality of the program, the Second Circuit first noted that the program "aims to prevent a terrorist attack on the subway" and therefore concluded that it met the threshold requirement.[152] The court then considered the balancing factors and found that the searches are reasonable. First, the court characterized the threat to public transportation systems as "sufficiently immediate" in light of attacks in other countries and domestic attempts.[153] Second, the court found that "a subway rider who keeps his bags on his person possesses an undiminished expectation of privacy therein."[154] Third, the court found the search to be minimally invasive.[155] Fourth, and most significant for present purposes, the court accepted trial evidence that the program is "a reasonably effective means of addressing the government interest in deterring and detecting a terrorist attack on the subway system."[156]

---

each from a different precinct in the five boroughs, converge in one place, 'combat-park' with their backs to the sidewalk, receive a terrorism briefing and get assignments to speed off to multiple locations.").

151 Kelly, *supra* note 149, at 563; *see also* Craig Horowitz, *The NYPD's War on Terror*, N.Y. MAG. (Feb. 2, 2003), http://nymag.com/nymetro/news/features/n_8286/ ("These small teams arrive in black Suburbans, sheathed in armor-plated vests and carrying 9-mm. submachine guns—sometimes with air or sea support. Their purpose is to intimidate and to very publicly mount a show of force. . . . [T]he Hercules Teams were designed to disrupt [terrorists'] planning.").

152 *MacWade*, 460 F.3d at 270–71.

153 *Id.* at 272.

154 *Id.* at 273.

155 *See id.* (giving five reasons why the search was narrowly tailored, including that passengers receive notice and may decline; that the police only search containers that could contain explosives; that the searches are only seconds long; that they are conducted in the open by uniformed personnel; and finally, that police are not exercising discretion when selecting whom to search).

156 *Id.* (internal quotation marks omitted). Similarly, the Fifth Circuit upheld a roadblock/checkpoint at a military base, reasoning that "[s]topping vehicles at regular intervals . . . reasonably advances the purposes of the checkpoint because it deters individuals from driving while unlicensed and or transporting weapons and thereby endangering base personnel. It provides a gauntlet, random as it is, that persons bent on mischief must traverse." United States v. Green, 293 F.3d 855, 862 (5th Cir. 2002). The Fifth Circuit went on to say of the (then) newly emerging post-9/11 security landscape, "[t]he same deterrence theory surely drives the recent adoption of random luggage searches at the nation's airports." *Id.* at 862 n.40. In *Cassidy v. Chertoff*, the Second Circuit (per then-Judge Sotomayor) relied on the Fifth Circuit precedent to conclude that random security screening of passengers on New York City ferries "appears to be reasonably calculated to serve its goal of deterring potential terrorists." 471 F.3d 67, 86 (2d Cir. 2006) (citing *Green*, 293 F.3d at 862).

The decision reveals both conceptual limitations identified above.[157] First, concerning the court's claim that the prevention of a terror attack on the subway counted as a special need, the doctrine is inattentive to an emerging trend, namely the absorption of ordinary criminal law modalities into national security law. On a range of issues from electronic surveillance law,[158] to detention policy,[159] to institutional design,[160] the government has attempted to collapse the boundary between prosecutions and national security by reconceptualizing the former as specific applications of the latter. As David Kris has explained, "[national security] prosecution is not an end in itself. . . . Law enforcement personnel . . . must see themselves as part of a larger effort . . . to protect national security."[161] But if ordinary law enforcement methods are increasingly regarded as elements of counterterrorism operating at scale, then it is not clear how

---

157 *See* L. Rush Atkinson, *The Bilateral Fourth Amendment and the Duties of Law-Abiding Persons*, 99 GEO. L.J. 1517, 1565 & n.235 (2011) (discussing *MacWade* as an example of law-abiding individuals incurring costs in order to avoid a search, and suggesting that a future court might, unlike the *MacWade* court, consider the potential social costs of innocents' avoidance of checkpoints in weighing whether a search is reasonable); *cf.* Cynthia Lee, *Package Bombs, Footlockers, and Laptops: What the Disappearing Container Doctrine Can Tell Us About the Fourth Amendment*, 100 J. CRIM. L. & CRIMINOLOGY 1403, 1427, 1458–60 (2010) (discussing *MacWade* in the context of the "erosion" of the container doctrine).

158 As the FISA Court of Review noted in its *In re Sealed Case* opinion (the first it ever issued), "prosecutions can be, and usually are, interrelated with other techniques used to frustrate a foreign power's efforts." 310 F.3d 717, 743 (FISA Ct. Rev. 2002). *See generally* David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487 (2006) (describing the rise and fall of a barrier between the Department of Justice's intelligence and law enforcement arms).

159 *See id.* at 527–28 (arguing that, with the fall of the FISA wall, detention via "civilian prosecution will tend to be available as one of several options" for national security policymakers).

160 In response to concerns about a lack of coordination among the Department of Justice's national security components, the 2006 Patriot Act reauthorization created the National Security Division (NSD), which combines all national security functions (including representation before the FISA court and counterterrorism and counterespionage prosecutions) under an Assistant Attorney General for National Security. USA PATRIOT Improvement and Reauthorization Act of 2005, § 506, 28 U.S.C. §§ 507A, 509A (2012); *National Security Division*, U.S. DEPARTMENT JUST. (May 16, 2013), http://www.justice.gov/jmd/mps/manual/nsd.htm (describing the various functions of the National Security Division).

161 David S. Kris, *Law Enforcement as a Counterterrorism Tool*, 5 J. NAT'L SECURITY L. & POL'Y 1, 30 (2011); *cf.* Cusson, *supra* note 53, at 62 ("The complementary nature of situational prevention and legal punishment goes both ways. A sentencing policy intended to punish shoplifting more systematically and more severely would not make much of an impact if stores were to have poor surveillance.").

the "specialness" of national security programs can be consistently maintained.[162]

Second, although the Second Circuit did engage in judicial review of a counterterrorism program at scale, going so far as to acknowledge its roots in new deterrence,[163] *MacWade* attests to the inherent tensions that arise when courts are confronted with government claims of national security necessity.[164] For example, the court noted that it was not conducting a "searching examination of effectiveness" because the political branches are more competent to make such a determination.[165]

Furthermore, the court rejected the plaintiffs' contention that assessment of constitutionality necessitates a measurement of the program's deterrent effect.[166] Thus, reviewing courts essentially cede the task of assessing efficacy to the very officials who design and operate the challenged programs.[167] In sum, while Special Needs doctrine has

---

[162] *Cf.* Ric Simmons, *Searching for Terrorists: Why Public Safety Is Not a Special Need*, 59 DUKE L.J. 843, 893 (2010) ("A terrorist attempting to carry a bomb onto a subway . . . is not a latent or hidden hazard. He is an individual attempting to commit an extremely serious crime. Any attempt to deter or detect his actions is purely a law enforcement function, and should be treated as such." (internal quotation marks omitted) (citing Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 668 (1989))). Simmons attempts to assimilate all terrorism to crime. The more powerful critique, I contend, is that all criminal prosecutions in this area are increasingly assimilated to national security. It is telling that the New York City Police Department, by way of fortifying its argument that the subway searches in question are constitutional, represented to the Second Circuit that it had never commenced a prosecution based on contraband discovered in a subway search prompted by counterterrorism concerns. *MacWade*, 460 F.3d at 265 n.1.

[163] *See supra* note 156 and accompanying text (discussing Second Circuit and Fifth Circuit cases that exemplify new deterrence).

[164] *See* Robert M. Chesney, *National Security Fact Deference*, 95 VA. L. REV. 1361 (2009) (evaluating several arguments for deferring to the executive branch in national security matters and concluding that such deference might be sensible in certain contexts); *cf.* Ricardo J. Bascuas, *Fourth Amendment Lessons from the Highway and the Subway: A Principled Approach to Suspicionless Searches*, 38 RUTGERS L.J. 719, 719, 784–85 (2007) (arguing that the "balancing test" employed by courts in the evaluation of suspicionless searches tends to yield unprincipled results, and that instead of a balancing approach, courts should undertake a threshold inquiry of whether the government is able to demonstrate "a threat of imminent physical harm"). It is interesting—if beyond the scope of this Article—to compare the posture of courts in national security cases, in which deference to executive claims of efficacy are at their apogee, to ordinary crime settings, in which courts sometimes express the view that the effectiveness of certain strategies is irrelevant to the constitutional analysis. *See, e.g.*, Floyd v. City of New York, No. 08 Civ. 1034 (SAS), 2013 WL 4046209, at *1 (S.D.N.Y. Aug. 12, 2013) ("[T]his case is not about the effectiveness of stop and frisk in deterring or combating crime.").

[165] MacWade v. Kelly, 460 F.3d 260, 273 (2d Cir. 2006).

[166] *Id.* at 274 ("The concept of deterrence need not be reduced to a quotient before a court may recognize a search program as effective."); *id.* at 275 ("[T]he absence of a formal study of the Program's deterrent effect does not concern us.").

[167] *See* STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 106 (2012) ("Absent an extraordinary, life-

proven uniquely amenable to judicial consideration of counter-terrorism programs at scale in concept, in practice it has not yet been fully adequate for the task.

2. *State Secrets*

The State Secrets Privilege[168] is one of several legal technologies[169] that courts use to shield government secrets from public disclosure. The Privilege derives from courts' assumption that national security inevitably depends upon maximizing government secrecy. But new deterrence reveals a more complex relationship between secrecy and transparency, and that is where the doctrinal underpinnings of the privilege are in tension with strategic reality.

State Secrets doctrine does include a judicial check on the other branches' invocation of secrecy.[170] The judiciary "must make an independent determination whether the information is privileged,"[171] and remove the evidence in question (even if it means terminating the lawsuit)[172] when "from all the circumstances of the case . . . there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged."[173] But operationalizing the doctrine against the backdrop of new deterrence reveals two challenges, each nicely illustrated by reference to a recent case involving secrecy in stings and surveillance.

The first challenge is framing and contextualizing the secret at issue.[174] In *Fazaga v. FBI*, plaintiffs in Southern California alleged

---

threatening emergency (a report of a terrorist truck bomb about to detonate, for example) the core values of the Fourth Amendment require objective, individualized justification when law enforcement officers conduct stops and searches that carry a significant prospect of criminal prosecution.").

168 *See* United States v. Reynolds, 345 U.S. 1, 7–8 (1953) (debuting the modern doctrine); *see also* Donohue, *supra* note 84, at 77 (examining state secrets cases from the years 2001 to 2009).

169 Such technologies include invocation of the Classified Information Procedures Act, 18 U.S.C. app. §§ 1–16 (2006), the so-called Glomar defense to a FOIA request, *see* Phillippi v. CIA, 546 F.2d 1009, 1013–14 (D.C. Cir. 1976) (describing the defense's origins), and leak prosecutions, *see* Pozen, *supra* note 80.

170 For a thoughtful consideration of the role of courts in managing secrecy regimes generated by the political branches, see Adam M. Samaha, *Government Secrets, Constitutional Law, and Platforms for Judicial Intervention*, 53 UCLA L. REV. 909 (2006).

171 Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190, 1202 (9th Cir. 2007).

172 *See* Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1079 (9th Cir. 2010) (stating that dismissal may sometimes be required).

173 United States v. Reynolds, 345 U.S. 1, 10 (1953).

174 Deterrence interests are on display in recent court submissions by senior intelligence officers. Responding to Edward Snowden's public disclosure of certain surveillance operations, intelligence officials have decided to narrow some of their privilege claims under the State Secrets doctrine and the statutory provisions of the National Security Act. *See* 50 U.S.C.A. § 3024(i)(1) (West 2013) ("The Director of National Intelligence shall

that dragnet spying by the FBI in houses of worship, among other places, violated religious liberty and various other constitutional and statutory protections.[175] They claimed that a government informant, as part of a surveillance scheme dubbed "Operation Flex," attempted to recruit numerous community members during visits to six major Southern California mosques.[176] The plaintiffs sought to uncover and enjoin the program,[177] but the district court ultimately agreed with the government that State Secrets barred litigation of the case lest information damaging to national security emerge in the course of the litigation.

The court mainly focused on the secret nature of the surveillance and the likelihood that individuals might destroy evidence or flee after learning they were under a government microscope.[178] But it also observed that "[d]isclosure of those *not* under investigation by the FBI is . . . dangerous because individuals who desire to commit terrorist acts may then be motivated to do so upon discovering that

---

protect intelligence sources and methods from unauthorized disclosure."). Intelligence officials have abandoned their privilege claims with respect to the mere existence of specific surveillance programs, but they continue to assert privilege with respect to the nature and scope of the surveillance programs disclosed by Snowden. In making the case for why they cannot confirm or deny whether the plaintiffs in *Jewel v. NSA*, No. 08-cv-04373-JSW (N.D. Cal. filed Sept. 18, 2008), and *Shubert v. Obama*, No. 07-cv-693-JSW (N.D. Cal. filed May 11, 2007), were subjected to certain surveillance modalities, Director Clapper and Acting Deputy Director Fleisch argue that to confirm who has been (or could be) subject to surveillance might cause the target to alter his behavior or take extra precautions to avoid surveillance. Public Declaration of James R. Clapper, Dir. of Nat'l Intelligence, at ¶ 34, Jewel v. NSA, No. 08-cv-04373-JSW (N.D. Cal. filed Sept. 18, 2008) [hereinafter Clapper Declaration], *available at* http://www.dni.gov/files/documents/1220/DNI%20Clapper%202013%20Jewel%20Shubert%20SSP%20Unclassified%20Signed%20Declaration.pdf; Unclassified Declaration of Frances J. Fleisch, Nat'l Sec. Agency, at ¶ 37, Jewel v. NSA, No. 08-cv-04373-JSW (N.D. Cal. filed Sept. 18, 2008) [hereinafter Fleisch Declaration], *available at* http://www.dni.gov/files/documents/1220/NSA%20Fleisch%202013%20Jewel%20Shubert%20Declaration%20Unclassified.pdf.

To reveal that someone has not been the subject of surveillance would lead to "adversaries [knowing] that a particular individual has avoided scrutiny and is a secure source for communicating." Clapper Declaration, *supra*, at ¶ 34. In light of such revelations, individuals not under surveillance might be emboldened to help terrorist organizations or "alternatively, such a person may be unwittingly utilized or even forced to convey information through a secure channel to a foreign adversary." Fleisch Declaration, *supra*, at ¶ 37.

175 Fazaga v. FBI, 884 F. Supp. 2d 1022, 1028–29 (C.D. Cal. 2012).

176 *Id.* at 1031. Plaintiffs learned of the informant's identity in a separate criminal proceeding where the prosecution introduced recordings of the defendant. *Id.* at 1032–33.

177 *See* First Amended Complaint Class Action at 68–69, Fazaga v. FBI, No. SACV11-00301JST(VBKx) (C.D. Cal. 2011), *available at* http://www.aclusocal.org/cases/fazaga/first-amended-complaint/ (requesting an order that the defendants destroy or return all information obtained through the program).

178 *Fazaga*, 884 F. Supp. 2d at 1044.

they are not being monitored."[179] In other words, the government's "secret" included not only what it was doing, but also what it wasn't doing.[180] This acknowledges the complexity of the secrecy-transparency relationship in new deterrence, particularly the government's desire to obscure specifics about certain counterterrorism programs.[181] But at the same time, the court failed to account for any limits on the Privilege: Where do state secrets begin and end?

After framing and contextualizing the secret at issue, the second challenge is striking the appropriate balance between secrecy and transparency. Although this has always been difficult,[182] the task is considerably more complicated against the backdrop of new deterrence. The exchange rate between units of transparency and units of damage to national security is no longer (if it ever was) one-to-one. Thus, when the *Fazaga* court reasoned that "[d]isclosure of subjects under investigation would undoubtedly jeopardize national security . . . because persons under investigation would be alerted to the FBI's interest in them and cause them to flee, destroy evidence, or alter their conduct so as to avoid detection,"[183] it failed to consider that disclosure might also promote national security via its deterrent message.[184]

3. Standing

The emphasis that new deterrence places on the psychological dimensions of counterterrorism—including the employment of fear as an instrument of official power—has not been incorporated into, indeed has been rejected by, prevailing legal doctrine. This past term, the Supreme Court reaffirmed its unwillingness to accord standing to plaintiffs alleging an injury rooted, at least in part, in fear.[185] In so

---

179 *Id.*

180 *See, e.g.*, Dianne Feinstein, *Mend but Don't End the NSA Data Programs*, WASH. POST, July 31, 2013, at A15 ("Only 22 highly vetted NSA analysts can approve a query of this database—and only when they have a reasonable, articulable suspicion that the number is connected to terrorism.").

181 *See, e.g.*, *supra* note 106 and accompanying text (introducing the concept in the context of sting operations).

182 *See* United States v. Reynolds, 345 U.S. 1, 8 (1953) (noting that this balancing often "presents real difficulty").

183 *Fazaga*, 884 F. Supp. 2d at 1044.

184 *See id.* at 1029 ("The Attorney General's privilege claim in this action requires the Court to wrestle with the difficult balance that the state secrets doctrine strikes between the fundamental principles of liberty, including judicial transparency, and national security.").

185 *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1141 (2013) (noting that the alleged harms by the plaintiffs "are simply the product of their fear of surveillance, which is insufficient to create standing" (citations omitted)).

doing, a sharply divided Court reaffirmed its forty-year-old precedent, also produced by a sharply divided court, in *Laird v. Tatum*.[186]

In *Laird*, the Court refused to find standing based on mere "knowledge that a governmental agency was engaged in certain activities or from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some *other* and additional action detrimental to that individual."[187] Instead, it was necessary for standing purposes that "the complainant was either presently or prospectively subject to the regulations, proscriptions, or compulsions that he was challenging."[188] The Court held that "[a]llegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm . . . ."[189] *Laird*'s distinction between "subjective" and "objective" chills has predictably caused confusion in the courts[190] and an insightful body of academic criticism.[191]

This past term in *Clapper v. Amnesty International USA*, Justice Alito, writing for the Court's conservative majority, reasoned that the plaintiffs' efforts (including expenditures) to avoid the possibility of

---

[186] 408 U.S. 1 (1972). One of the more striking features of the case was then-Justice Rehnquist's decision not to recuse himself despite previously opining on the lawsuit as Assistant Attorney General for the Office of Legal Counsel. *See* Ross E. Davies, *The Reluctant Recusants: Two Parables of Supreme Judicial Disqualification*, 10 GREEN BAG 2D 79, 82–84 (2006), *available at* http://www.greenbag.org/v10n1/v10n1_from_the_bag_davies.pdf (explaining the controversy surrounding Justice Rehnquist's decision). As the Court's opinion garnered only a bare majority, *Laird*, 408 U.S. at 1, Justice Rehnquist supplied the deciding vote.

[187] *Laird*, 408 U.S. at 11.

[188] *Id.*

[189] *Id.* at 13–14. The Court seemed to reason that the plaintiffs were trying, through a claimed chilling effect, to ground entitlement to standing on the very fact of surveillance. *See id.* at 13 & n.7 ("[R]espondents [have] left somewhat unclear the precise connection between the mere existence of the challenged system and their own alleged chill . . . .").

[190] *See* Scott Michelman, *Who Can Sue Over Government Surveillance?*, 57 UCLA L. REV. 71, 89–99 (2009) (discussing the legal disarray regarding standing since *Laird v. Tatum*). Daniel Solove argues that

> Lower courts have interpreted *Laird* to mean that the mere presence of the police or recording of information at public meetings do not constitute cognizable First Amendment injuries. However, when plaintiffs have produced evidence of deterrence (as opposed to mere allegations of discomfort or dislike), courts have found cognizable First Amendment injuries.

Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 144 (2007) (footnote omitted); *see also* Eric Lardiere, Comment, *The Justiciability and Constitutionality of Political Intelligence Gathering*, 30 UCLA L. REV. 976, 1006–07 (1983) (surveying post-*Laird* case law).

[191] *E.g.*, Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685 (1978); Michael N. Dolich, Note, *Alleging a First Amendment "Chilling Effect" to Create a Plaintiff's Standing: A Practical Approach*, 43 DRAKE L. REV. 175 (1994); Note, *The Chilling Effect in Constitutional Law*, 69 COLUM. L. REV. 808 (1969).

surveillance amounted to self-inflicted injuries not traceable to the passage of the FISA Amendments Act of 2008.[192] Meanwhile, Justice Breyer, writing in dissent, found that the plaintiffs had met their burden to show constitutionally relevant injury based on his understanding that the programs were sufficiently broad in scope, and that the government was sufficiently motivated and capable of collecting intelligence.[193]

What *Laird* said, and *Clapper* effectively reaffirms, is that courts are hesitant to review government deployment of fear in national-security programs. That is because the Court continues to assume that the mere fact of government surveillance is a nonevent.[194] New deterrence instructs otherwise: Using surveillance and other official modalities to instill fear may serve a core strategic purpose.[195]

---

[192] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1152 (2013). In another criticized part of the opinion, the Court relied on a government commitment that criminal defendants exposed to punishment because of evidence derived from surveillance authorized by the FISA Amendments Act of 2008 would receive notice, and therefore be able to establish standing to challenge the law. *Id*. at 1154 n.8; *see also* Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N.Y. TIMES, July 16, 2013, at A11, *available at* http://www.nytimes.com/2013/07/16/us/double-secret-surveillance.html (questioning the Solicitor General's representation during oral argument that targets would be informed of surveillance if prosecuted, and thus have standing to challenge the law). The government's position apparently implicates an internal Department of Justice rivalry that has (for the moment) been won by advocates of disclosure. *See* Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES, Oct. 17, 2013, at A3, *available at* http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html (discussing the disagreement between lawyers in the Solicitor General's office, who believed that information gathered from FISA surveillance would be disclosed to criminal defendants, and lawyers in the National Security Division, who rejected the existence of any such obligation).

[193] *See Clapper*, 133 S. Ct. at 1160 (Breyer, J., dissenting) ("[F]ederal courts frequently entertain actions for injunctions and for declaratory relief aimed at preventing future activities that are reasonably likely or highly likely, but not absolutely certain, to take place. And that degree of certainty is all that is needed to support standing here.").

[194] As the ACLU's Jameel Jaffer recently observed, "dragnet surveillance will be poisonous to the freedoms of inquiry and association" because it will cause citizens to "hesitate before visiting controversial Web sites, discussing controversial topics or investigating politically sensitive questions." Charlie Savage, *Broader Sifting of Message Data by N.S.A. Is Seen*, N.Y. TIMES, Aug. 8, 2013, at A1, *available at* http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html.

[195] *See* Brian Calabrese, Note, *Fear-Based Standing: Cognizing an Injury-in-Fact*, 68 WASH. & LEE L. REV. 1445, 1447, 1456–76 (2011) (explaining the doctrine of fear-based standing as it currently exists in three distinct strains—alleged chilling effect injury, pre-enforcement fear, and anticipatory harm injury—and advocating an analytical framework for courts to adopt when deciding fear-based standing arguments); *cf.* Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 269 (2013) (noting the troubling nature of technologies that facilitate "broad, indiscriminate, and continuous" surveillance).

For example, a recent lawsuit alleged an impermissible infringement of religious exercise due to pervasive surveillance in mosques.[196] As the complaint sets out, and as common sense and some precedent dictate,[197] the potential presence of government informants in houses of worship can profoundly alter the dynamics of a religious community, chilling everything from popular attendance to ventilation by religious leaders of hot-button issues. To be certain, the adjudication of such allegations entails careful consideration of the nature and extent of government interference.[198] But—and this is the nub—such consideration ought to take place on the merits.[199]

There is a limited exception to the *Laird* rule when plaintiffs' fears are based on prospective criminal liability.[200] But stingy application of the exception only proves the rule. In *Hedges v. Obama*,[201] a post-*Clapper* decision, the Second Circuit denied standing to two different sets of plaintiffs in a challenge to the detention provisions of

---

196 *See* First Amended Complaint at 2, Fazaga v. FBI, No. SACV11-00301JST(VBKx) (C.D. Cal. 2011), *available at* http://www.aclusocal.org/cases/fazaga/first-amended-complaint/.

197 In the 1989 case of *Presbyterian Church (U.S.A.) v. United States*, the Ninth Circuit held that the plaintiff churches had standing to challenge the conduct of INS agents who wore "body bugs" and surreptitiously recorded church services:

> If . . . the churches can in fact prove their allegations of a decrease in congregants' participation in worship services and other religious activities, of the cancellation of a Bible study class, of the diversion of clergy energy from pastoral duties, and of congregants' reluctance to seek pastoral counseling, they would establish that the surveillance of religious activity has directly interfered with the churches' ability to carry out their religious mission. Churches, as organizations, suffer a cognizable injury when assertedly illegal government conduct deters their adherents from freely participating in religious activities protected by the First Amendment.

870 F.2d 518, 520, 523 (9th Cir. 1989).

198 *See* Younger v. Harris, 401 U.S. 37, 51 (1971) (noting that the presence of "chilling effect[s]" does not necessarily render a statute unconstitutional, for "it is well settled that the statute can be upheld if the effect on speech is minor in relation to the need for control of the conduct and the lack of alternative means for doing so"). The balance is inevitably very delicate. To take a recent example, Boston Marathon bomber Tamerlan Tsarnaev was an outspoken critic of the moderate tone of his local mosque in Cambridge, Massachusetts, at one point shouting down the Imam for daring to compare Dr. Martin Luther King, Jr. to the prophet Muhammad. Judith Miller, *How to Stop Terrorists Before They Kill*, WALL ST. J., Apr. 25, 2013, at A15, *available at* http://online.wsj.com/news/articles/SB10001424127887324874204578440992247444754. Some writers suggest that more aggressive surveillance might have prevented the Tsarnaevs' attack. *See id.* (citing terrorism experts who stated that the attacks would have been prevented by New York City's aggressive monitoring system).

199 *See* Laird v. Tatum, 408 U.S. 1, 3 (1972) (dismissing for lack of standing); ACLU v. NSA, 493 F.3d 644, 648 (6th Cir. 2007) (same).

200 *See* Babbitt v. Farm Workers, 442 U.S. 289, 302 (1979).

201 724 F.3d 170 (2d Cir. 2013).

the National Defense Authorization Act of 2012.[202] The court found plaintiffs' fear of detention to be noncognizable because the statute is not criminal in nature.[203] Thus, the Second Circuit effectively closed the door to claims rooted in new (rather than traditional) deterrence. Standing doctrine in national security cases reveals and reinforces a gap between legal doctrine and strategic reality shaped by new deterrence.

* * *

In sum, across a broad range of judicial doctrines in national security jurisprudence, courts have not proved ready for the task of governing counterterrorism policies grounded in new deterrence. These doctrinal barriers are, in turn, compounded by a series of institutional barriers.

B. Institutions

Due to the nature of judge-made law and the circumstances of its production, especially in national security cases,[204] it is understandable why doctrine has not kept pace with the emerging reality of new deterrence. But at first blush it is harder to see why national security organizations have not leveraged new-deterrence thinking more successfully in operationalizing and overseeing counterterrorism policies. To put a fine point on it, many of these institutions were designed

---

202 Pub. L. No. 112-81, 125 Stat. 1298.

203 *See Hedges*, 724 F.3d at 200 (distinguishing military detention statute from a "typical statute imposing criminal or civil penalties"). In so doing, and despite the court's insistence otherwise, it appeared to veer in the direction of deferring to the national security executive. *See id.* at 204 (noting that, while courts have an important role to play in assessing military detention, the fact that the Constitution allocates to the President broad discretion in military affairs means that plaintiffs have a higher burden in showing standing); *see also* Al-Aulaqi v. Obama, 727 F. Supp. 2d 1, 52 (D.D.C. 2010) ("[D]ecision-making in the realm of military and foreign affairs is textually committed to the political branches . . . ."). But a court no more trenches on the executive's national security competency when it pronounces on the constitutionality of surveillance law, for example, than when it rules on the material support statute.

204 Unlike counterpart institutions overseas, American courts have been notoriously reluctant to superintend counterterrorism policy. *See, e.g.*, Rick Pildes, *Does Judicial Review of National-Security Policies Constrain or Enable the Government?*, LAWFARE (Aug. 5, 2013, 1:48 PM), http://www.lawfareblog.com/2013/08/does-judicial-review-of-national-security-policies-constrain-or-enable-the-government/ (comparing American judicial restraint in national security with more activist approaches by, for example, Israeli judges); *see also* HCJ 769/02 Pub. Comm. Against Torture in Israel v. Israel (2) IsrLR 459 [2006] (Isr.) (adjudicating the legal framework for Israel's targeted killing program). I mean to stress the inadequacy of contemporary doctrine, not a congenital defect in courts as such, in grappling with the implications of new deterrence.

explicitly to implement deterrence strategy in the Cold War,[205] and yet, certain powerful institutional realities have interrupted the more thorough adoption of contemporary deterrence strategy, including by executive branch oversight bodies.

First, bureaucratically entrenched national security agencies have tended to pursue narrow, tactical agendas. But because new deterrence requires coordination and layering, this narrowing of focus has tended to promote and reinforce an incapacitationist outlook. Furthermore, relatively newer, weaker strategic agencies, which otherwise could promote new-deterrence strategizing and policymaking through more effective coordination, have been relatively ineffective. Second, certain potentially valuable executive-branch oversight bodies have not internalized the importance of new-deterrence thinking for their missions. I discuss each in turn.

1. Organization

Lack of strategic policymaking and coordination among agencies plays out in two ways. First, individual agencies that operate particular counterterrorism programs have come to wield extraordinary power.[206] Second, organizations designed to implement new deterrence by straddling traditional divides[207]—those between the intelligence community and the balance of the national security state,[208] between the practitioners of domestic and foreign counterterrorism, and between the more defensive architectural dimensions of

---

[205] It is conceivable that traditional deterrence pedigrees might actually make it more difficult for certain agencies to implement new-deterrence–based policies because of the subtly different outlooks they imply.

[206] *Cf.* Bruce Hoffman, *A Counterterrorism Strategy for the Obama Administration*, 21 TERRORISM & POL. VIOLENCE 359, 369 (2009) ("The predominantly tactical 'kill or capture' approach and metric that has largely guided our counterterrorist and counterinsurgent efforts to date is too narrow and does not sufficiently address the complexities of these unique operational environments.").

[207] Recent scholarly contributions have emphasized additional divides, including between local and national government agencies and between government officials and private contractors. *See* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 944–47 (2008) (discussing the cooperation between the government and private corporations in the production of counterterrorism intelligence and recommending a shift of compliance responsibility from the executive to private corporations in order better to protect individual rights, thus turning corporations into "bulwarks of accountable intelligence policy"); Matthew C. Waxman, *National Security Federalism in the Age of Terror*, 64 STAN. L. REV. 289 (2012) (emphasizing that a myopic focus on the horizontal organization of the national security apparatus is misplaced because it fails to recognize the importance of vertically shared antiterrorism functions).

[208] In traditional regulation, the same agency typically assesses and manages risk, but in national security matters, intelligence agencies assess, and the balance of the national security state manages.

counterterrorism and more classically offensive ones[209]—have been unable to realize their full potential.

Concerning the former, the most striking example is the Central Intelligence Agency. The CIA's Counterterrorism Center has assumed pride of place owing to the CIA's still officially secret drone fleet. When the 9/11 Commission recommended that the CIA terminate its paramilitary operations,[210] the Bush Administration balked, and the CIA has expanded its investment in tactical war-fighting ever since.[211] As Mark Mazzetti has written, "[t]argeted killings have made the CIA the indispensable agency for the Obama administration."[212] This shift in priorities, from classic espionage and global analysis toward locating and acquiring targets for drone warfare, tends to instantiate and reinforce a bias in favor of tactical decisionmaking. Indeed, in his confirmation hearing to become CIA Director, John Brennan (who had served as a Deputy National Security Advisor overseeing drone strikes at the White House) seemingly conceded that reprioritization was in order.[213] In their own ways, organizations as different from one another as the FBI, the Treasury Department,[214] and the Joint Special Operations Command[215] similarly manifest the prioritization of incapacitationist counterterrorism capabilities.

---

209 *See* BOBBITT, *supra* note 16, at 296–325 (discussing the breakdown of certain traditional antinomies in national security); *cf.* Jody Freeman & Jim Rossi, *Agency Coordination in Shared Regulatory Space*, 125 HARV. L. REV. 1131 (2012) (advocating greater interagency collaboration in policymaking).

210 NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., 9/11 COMMISSION REPORT 415 (2004), *available at* http://www.9-11commission.gov/report/911Report.pdf (recommending termination of paramilitary operations on the basis that the country "cannot afford to build two separate capabilities for carrying out secret military operations").

211 *See* MARK MAZZETTI, THE WAY OF THE KNIFE: THE CIA, A SECRET ARMY AND A WAR AT THE ENDS OF THE EARTH 228 (2013) (reporting that, concerning the CIA's drone program, a Vice Chairman of the Joint Chiefs of Staff inquired, "[W]hy we are building a second Air Force?").

212 *Id.* at 315.

213 *See Nomination of John O. Brennan to Be Director of the Central Intelligence Agency: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. 50 (2013) (statement of John O. Brennan) ("[T]he CIA should not be doing traditional military activities and operations.").

214 *See* Exec. Order No. 13,224, 3 C.F.R. 786 (2002) (empowering Treasury's Office of Foreign Asset Control to block all property and transactions with those deemed to be terrorists or terrorist supporters); *see also* Kindhearts for Charitable Humanitarian Dev., Inc. v. Geithner, 710 F. Supp. 2d 637, 642–43 (N.D. Ohio 2010) (casting doubt on the constitutionality of certain OFAC counterterrorism measures). *See generally* ZARATE, *supra* note 95 (discussing the Treasury's increasing involvement in counterterrorism).

215 JSOC's size has tripled since 9/11 and now includes over four thousand members. Marc Ambinder, *The Secret Team that Killed Osama bin Laden*, ATLANTIC (May 2, 2011, 10:20 AM), http://www.theatlantic.com/international/archive/2011/05/the-secret-team-that-killed-osama-bin-laden/238163/. For a more detailed breakdown of JSOC's structure, size,

In comparison, agencies designed to allocate resources and implement strategic thinking in a comprehensive way that maximizes the overall impact of American counterterrorism have remained relatively weak.[216] The case of the Directorate of Strategic and Operational Planning (DSOP) of the National Counterterrorism Center (NCTC) is instructive. The Intelligence Reform and Terrorism Prevention Act of 2004[217] designed DSOP to "conduct strategic operational planning for counterterrorism activities, integrating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities within and among agencies," as well as to "assign operational responsibilities to lead agencies for counterterrorism activities that are consistent with applicable law and that support strategic plans to counter terrorism."[218]

In addition to its statutory mission, DSOP possesses at least three institutional features that are conducive to participating in new-deterrence–based counterterrorism. First, it is located within the same agency that functions as the intelligence hub for all domestic and overseas counterterrorism intelligence. Because intelligence supplies the most meaningful data for implementing and calibrating new deterrence, DSOP is well situated to carry out this challenging task with the benefit of the most relevant information. Second, the NCTC reports directly to the President in its strategic planning capacity,

---

and history, see ANDREW FEICKERT, CONG. RESEARCH SERV., U.S. SPECIAL OPERATIONS FORCES (SOF): BACKGROUND AND ISSUES FOR CONGRESS 6–7 (2013), *available at* http://www.fas.org/sgp/crs/natsec/RS21048.pdf.

216 Commentators have also criticized more tactical-level coordinating bodies, such as Department of Homeland Security–sponsored Fusion Centers and FBI-led Joint Terrorism Task Forces. *E.g.*, *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 112th Cong. 53 (2011) (statement of Samuel J. Rascoff, Professor, NYU School of Law), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112shrg66620/pdf/CHRG-112shrg66620.pdf.

217 Pub. L. 108-458, 118 Stat. 3638.

218 Exec. Order No. 13,354, 3 C.F.R. 214 (2004), *amended by* Exec. Order No. 13,470, 3 C.F.R. 238 (2008); *cf.* 50 U.S.C.A. § 3056(d)(2)–(3) (West 2013) (codifying sections of the Intelligence Reform and Terrorism Prevention Act of 2004 and Executive Order 13,354). The legislation left the meaning and content of "strategic operational planning" relatively vague and undefined. *See* TODD M. MASSE, CONG. RESEARCH SERV., THE NATIONAL COUNTERTERRORISM CENTER: IMPLEMENTATION CHALLENGES AND ISSUES FOR CONGRESS 9 (2005) ("The act defines strategic operational planning as ' . . . the mission, objectives to be achieved, tasks to be performed, interagency coordination of activities, and the assignment of roles and responsibilities.'" (alteration in original) (quoting 50 U.S.C.A. § 3056(j)(2) (West 2013))); Sally Scudder, *Strategic Operational Planning and Congressional Oversight of Intelligence*, INSS DYNAMIC DIALOGUE (June 19, 2012, 1:19 PM), http://inssblog.wordpress.com/2012/06/19/strategic-operational-planning-and-congressional-oversight-of-intelligence/ ("Specifically, Congress didn't challenge or define the vague and contrary concept of 'strategic operational planning' . . . .").

which engenders some level of accountability. At the same time, it is sufficiently distinct from the West Wing to remain somewhat aloof from the day-to-day political pressures of the White House. Third, and perhaps most important, DSOP belongs to an agency that does not wield any particular counterterrorism tools and is consequently not susceptible to excessive focus on any single policy or program.

When the CIA actively engages in drone strikes, the FBI makes counterterrorism arrests, or the TSA oversees airport security, the NCTC's operational neutrality becomes a major asset. As such, the DSOP is particularly well positioned to take the broad view necessary for designing an overall counterterrorism strategy informed by new deterrence, including contemplating counterterrorism roles for government agencies far afield of the traditional national security state through the adoption of a "whole of government approach."[219]

---

[219] *See Nine Years After 9/11: Confronting the Terrorist Threat to the Homeland: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 111th Cong. 80 (2010) (statement of Michael Leiter, Director, National Counterterrorism Center), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-111shrg63832/pdf/CHRG-111shrg63832.pdf (listing a range of partner agencies from the FBI to the Department of Health and Human Services); *see also* Denis McDonough, Deputy Nat'l Sec. Advisor, Remarks on Partnering with Communities to Prevent Violent Extremism in America at the ADAMS Center (Mar. 6, 2011), *available at* http://www.cfr.org/terrorism/remarks-denis-mcdonough-deputy-national-security-advisor-partnering-communities-prevent-violent-extremism-america-march-2011/p24313 (recognizing the role of the Department of Education, for example, as part of a counter-radicalization strategy). The participation of the welfare state in national security functions is not unprecedented. For instance, the Department of Health and Human Services runs programs such as the National Health Security Strategy, *see* U.S. Dep't of Health & Human Servs., *National Health Security Strategy*, PUB. HEALTH EMERGENCY, http://www.phe.gov/preparedness/planning/authority/nhss/Pages/default.aspx (last modified Nov. 14, 2013), and the National Biodefense Science Board, *see* U.S. Dep't of Health & Human Servs., *National Biodefense Science Board (NBSB)*, PUB. HEALTH EMERGENCY, http://www.phe.gov/preparedness/legal/boards/nbsb/pages/default.aspx (last modified Jan. 27, 2014), and the Department of Agriculture hosts a food defense and security program, *see* U.S. Dep't of Agric., *Food Defense and Emergency Response*, FOOD SAFETY & INSPECTION SERV., http://www.fsis.usda.gov/food_defense_&_emergency_response/index.asp (last modified Dec. 6, 2013). More conceptually, the boundary between national security and the welfare state is itself historically contingent. *See* Mariano-Florentino Cuéllar, *"Securing" the Nation: Law, Politics, and Organization at the Federal Security Agency, 1939–1953*, 76 U. CHI. L. REV. 587 (2009) (analyzing and extracting theoretical insights from the Federal Security Agency which was created in 1939 and became the Department of Health, Education, and Welfare in 1953); *see also* United States v. Certain Parcels of Land in Peoria Cnty., Ill., 209 F. Supp. 483, 488 (S.D. Ill. 1962) ("The interstate system intended transcends state and local interest in the interest of a larger national purpose of providing a nationwide system of highways adequate to meet the needs of the national defense and interstate commerce."). More fundamentally, Charles Tilly's famous insight that "war makes states," Charles Tilly, *War Making and State Making as Organized Crime*, *in* BRINGING THE STATE BACK IN 169, 170 (Peter B. Evans et al. eds., 1985), might imply that cordoning off national security from the machinery of the state writ large is historically doomed. *Cf.* Jerry L. Mashaw, *Reluctant Nationalists: Federal Administration and Administrative Law in the Republican Era, 1801–1829*, 116 YALE L.J.

And yet DSOP still plays second fiddle in a tactically minded national security state. Some suggest that the White House itself—working through the National Security Council (NSC)—supplies the solution for insufficient strategic coordination.[220] But that is not necessarily true. The White House has retained a tactical focus on counterterrorism issues: The President is briefed personally as to individual drone strikes and discusses extensively whether and how to detain individual terror suspects.[221] Concerning the NSC, its core institutional strengths reside in two areas. First, it is well positioned to coordinate the work of agencies, whether for a civil war in Syria or the investigation of the Boston Marathon bombings. Second, the NSC is effective at defining American grand strategy.[222] But the NSC is weaker between these polar capacities, where counterterrorism strategy inevitably must take place. As former Deputy National Security Advisor for Counterterrorism Juan Zarate explained, "DSOP has served the function of a more granular policy planning staff for [counterterrorism] issues—one that can take policy and strategy [devised at the NSC level] and add a layer of specificity (e.g., action plans) that allows for more clarity of function and coordination."[223] He added that, in contrast to the NSC, DSOP "can also take a longer

1636, 1642 (2007) (arguing that the War of 1812 is connected tightly to the early emergence of the administrative state).

220 Although the Obama Administration formally collapsed the divide between the NSC and Homeland Security Council, these domains have remained separate in terms of staffing and operation. Josh Meyer, *Obama Joins His Security Councils; The Merging of Staffs Is Intended to End the 'Artificial Divide' Between Domestic and International Threats*, L.A. TIMES, May 27, 2009, at A15. Some commentators have criticized the merger. *See, e.g.*, Paul N. Stockton, *Reform, Don't Merge, the Homeland Security Council*, 32 WASH. Q. 107, 112 (2009) (arguing that the merger would burden the NSC with managing policy coordination problems among agencies, thus "leaving homeland security to get short shifted").

221 *See* Jo Becker & Scott Shane, *Secret 'Kill List' Proves a Test of Obama's Principles and Will*, N.Y. TIMES, May 29, 2012, at A1, *available at* http://www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html ("If John Brennan is the last guy in the room with the president, I'm comfortable, because Brennan is a person of genuine moral rectitude." (quoting Harold Koh)); *see also* GATES, *supra* note 65, at 566–67, 586–87 (criticizing the Obama White House's tendency to micromanage national security decisionmaking).

222 One clear example is leading the recalibration of foreign policy in the Middle East following the region's recent revolutionary movements. *See* David Ignatius, *Tom Donilon's Arab Spring Challenge*, WASH. POST (Apr. 26, 2011), http://articles.washingtonpost.com/2011-04-26/opinions/35262491_1_tom-donilon-yemen-white-house (discussing in particular the way in which Tom Donilon, former National Security Advisor for President Obama, saw an increased responsibility in "coordinating administration strategy for a revolution that will alter the foreign-policy map for decades").

223 E-mail from Juan C. Zarate, former Deputy Nat'l Sec. Advisor for Counterterrorism, to Samuel J. Rascoff, Assoc. Professor of Law, N.Y. Univ. Sch. of Law (Aug. 8, 2013, 15:23 EST) (on file with the New York University Law Review) (second alteration in original).

view if required to address issues that are likely to arise—with planning tied to future occurrences or scenarios."[224]

2. *Oversight*

The conceptually and institutionally complex issues raised by the oversight[225] of contemporary counterterrorism have generated a rich body of scholarship.[226] Nevertheless, scholars have largely ignored the implications of new deterrence and, more generally, have paid insufficient attention to how engagement with underlying strategy might empower oversight bodies to accomplish their missions. I focus on cost-benefit analysis and the capacity of generalist executive branch agencies[227] like the Office of Information and Regulatory Affairs (OIRA) as well as more specialized bodies such as the Privacy and Civil Liberties Oversight Board to become more effective overseers of counterterrorism policies rooted in new deterrence.[228]

First, OIRA within the Office of Management and Budget might seize on the issues highlighted by new deterrence to step up the role of cost-benefit analysis in this area.[229] While cost-benefit analysis has

---

[224] *Id.*

[225] It is worth noting that the literal meaning of "oversight" and "surveillance" are the same.

[226] *E.g.*, JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11 (2012); Anne Joseph O'Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World*, 94 CALIF. L. REV. 1655 (2006); Shirin Sinnar, *Protecting Rights from Within? Inspectors General and National Security Oversight*, 65 STAN. L. REV. 1027 (2013).

[227] Given the distinct oversight challenges with counterterrorism at scale, it makes sense for Congress and its specialized committees to play a role in this area. *See, e.g.*, Gary Schmitt, *Don't Save This Court*, WEEKLY STANDARD, Aug. 5, 2013, at 8, 9, *available at* http://www.weeklystandard.com/articles/don-t-save-court_741008.html (arguing that congressional committees, rather than the FISA court, should oversee bulk surveillance). But evidence from the recent past suggests that although the body may be well-positioned to interact with counterterrorism at the appropriate level of scale, numerous dynamics tend to undermine effective oversight by Congress. *See* Peter Wallsten, *Lawmakers Say Obstacles Limited Oversight of NSA's Telephone Surveillance Program*, WASH. POST (Aug. 11, 2013), http://www.washingtonpost.com/politics/lawmakers-say-obstacles-limited-oversight-of-nsas-telephone-surveillance-program/2013/08/10/bee87394-004d-11e3-9a3e-916de805f65d_story.html (observing that, in the view of some relevant oversight committee members, "the briefings in 2010 and 2011 on the telephone surveillance program were by definition one-sided affairs, with lawmakers hearing only from government officials steeped in the legal and national security arguments for aggressive spying").

[228] Tellingly, the report issued by the President's Review Group on Intelligence and Communications Technologies argues both for "the creation of a privacy and civil liberties policy official located both in the National Security Staff and the Office of Management and Budget," CLARKE ET AL., *supra* note 98, at 194, as well as for expanded powers for the Privacy and Civil Liberties Oversight Board or the creation of a new Civil Liberties and Privacy Protection Board, *id.* at 195–200.

[229] *See* Cass R. Sunstein, Commentary, *The Office of Information and Regulatory Affairs: Myths and Realities*, 126 HARV. L. REV. 1838, 1864–68 (2013) (providing a

come to dominate much of the administrative state,[230] it hardly has made a dent in the practice of national security. This may be a product of bureaucratic torpor[231] or a stubborn insistence on the uniqueness of the counterterrorism function.[232] As of 2008, "the executive branch ha[d] published no subsequent guidance on how the Department of Homeland Security (DHS) and other agencies implementing home-

practical perspective on the depth of OIRA's involvement in cost-benefit review). There have been occasional important calls for reform in this area. For example, Jessica Stern and Jonathan B. Wiener have proposed an oversight entity under presidential control that will be able to conduct "a full portfolio analysis of target risk reduction benefits, costs, ancillary benefits and countervailing risks." Stern & Wiener, *supra* note 68, at 439. And Robert J. Strayer has called for a "comparative analysis of the regulatory approaches to enhancing security," involving both qualitative inputs such as privacy concerns as well as quantified inputs of the costs and benefits of a given option. Robert L. Strayer, *Making the Development of Homeland Security Regulations More Democratic*, 33 OKLA. CITY U. L. REV. 331, 356 (2008). I have also argued for greater reliance on rationality review and public participation in national security. Rascoff, *supra* note 68, at 617–33.

230 A notable exception is criminal justice, which has largely eluded the potentially rationalizing influences of this methodology. *See* Brown, *supra* note 15 (describing how cost-benefit analysis could address structural dysfunction in the administration of criminal law).

231 As Mueller and Stewart have argued, for the Department of Homeland Security (DHS), "risk assessment seems to be simply a process of identifying a potential source of harm and then trying to do something about it without evaluating whether the new measures reduce risk sufficiently to justify their costs." John Mueller & Mark G. Stewart, *Balancing the Risks, Benefits, and Costs of Homeland Security*, 7 HOMELAND SECURITY AFF. 1, 3 (2011), *available at* http://www.hsaj.org/?fullarticle=7.1.16. Belcore and Ellig, employing a methodology established by Thomas McGarity, conclude that DHS is particularly adrift in formulating, and then addressing, a distinct regulatory problem. *See* Jamie Belcore & Jerry Ellig, *Homeland Security and Regulatory Analysis: Are We Safe Yet?*, 40 RUTGERS L.J. 1, 50–51 (2008) (referring to DHS's analyses as "seriously incomplete").

232 In *Electronic Privacy Information Center v. DHS*, the plaintiffs argued that the TSA should have subjected its new policy of screening all airline passengers with advanced imaging technology (instead of magnetometers) to notice-and-comment rulemaking. 653 F.3d 1, 3 (D.C. Cir. 2011). At oral argument, the government argued, "Congress has given the TSA responsibility to protect the traveling public from evolving threats using the latest technologies and 'should not have to stop every five minutes for comment and rulemaking.'" Nedra Pickler, *Group Says Body Scanners an 'Unreasonable Search*,' WASH. POST (Mar. 10, 2011, 6:17 PM), http://www.washingtonpost.com/wp-dyn/content/article/2011/03/10/AR2011031003628.html (quoting Deputy Assistant Attorney General Beth Brinkmann). The D.C. Circuit sided with the plaintiffs, rejecting TSA's argument. It found that "much public concern and media coverage have been focused upon issues of privacy, safety, and efficacy, each of which no doubt would have been the subject of many comments had the TSA seen fit to solicit comments upon a proposal to use [advanced imaging technology] for primary screening." *Elec. Privacy Info. Ctr.*, 653 F.3d at 6. As a result, TSA's policy was not merely a procedural rule, interpretive rule, or general statement of policy, but a substantive rule issued without notice-and-comment rulemaking. *See id.* at 5–8 (considering and rejecting each alternative). The court remanded without vacating the rule, *id.* at 11, and the notice-and-comment closed on June 24, 2013, Passenger Screening Using Advanced Imaging Technology, 78 Fed. Reg. 18,287, 18,287 (proposed Mar. 26, 2013).

land security regulations should make cost-benefit determinations."[233] There may be some change afoot, given that the recently issued report by the President's Review Group on Intelligence and Communications Technologies calls for employment of cost-benefit methodology in intelligence matters, reasoning that "surveillance decisions should depend (to the extent feasible) on a careful assessment of the anticipated consequences, including the full range of relevant risks."[234] But in practice, producing rational security is still very much a work in progress.

Cost-benefit analysis is potentially congenial to new deterrence.[235] First, the cost of a deterrence-based approach to security is likely to be lower than "a perfect defense [which] is overkill (and unachievable in any event)."[236] For example, "measures such as randomized screening and periodic surges in security levels at key sites . . . keep terrorists off guard, are less costly than a watertight defense, and if designed well, are sufficient for deterring terrorist attacks."[237] Furthermore, although measuring deterrence-based successes is notoriously challenging, analysts have successfully evaluated the effectiveness of, for example, drunk driving–based checkpoints,[238] which are analogous to some new-deterrence policies.

At the same time, cost-benefit analysis may be uniquely well designed to account for some of the social costs of new-deterrence

---

233 Strayer, *supra* note 229, at 345.

234 CLARKE ET AL., *supra* note 98, at 16.

235 *See* Brown, *supra* note 15, at 344 ("Deterrence is one example of how CBA can do a better job than traditional theories in predicting social costs and benefits.").

236 Kroenig & Pavel, *supra* note 10, at 30.

237 *Id*.

238 *See, e.g.*, James C. Fell et al., *Sobriety Checkpoints: Evidence of Effectiveness Is Strong, but Use Is Limited*, 5 TRAFFIC INJ. PREVENTION 220, 220 (2004) ("There is substantial and consistent evidence from research that highly publicized, highly visible, and frequent sobriety checkpoints in the United States reduce impaired driving fatal crashes by 18% to 24%."); *see also* Alena Erke et al., *The Effects of Drink-Driving* [sic] *Checkpoints on Crashes—A Meta-Analysis*, 41 ACCIDENT ANALYSIS & PREVENTION 914, 919–20 (2009) (finding in a global meta-analysis of sobriety checkpoint studies an approximate seventeen percent drop in alcohol-caused car crashes due to the checkpoints, although acknowledging variance between countries in the types of checkpoints employed); William N. Evans et al., *General Deterrence of Drunk Driving: Evaluation of Recent American Policies*, 11 RISK ANALYSIS 279, 279, 281 (1991) (finding that punitive laws are generally unhelpful in deterring drunken driving, but that roadside checkpoints—which the authors describe as being "designed to increase the probability of detection"—may "have a synergistic deterrent effect"); James C. Fell et al., *Why Are Sobriety Checkpoints Not Widely Adopted as an Enforcement Strategy in the United States?*, 35 ACCIDENT ANALYSIS & PREVENTION 897, 897, 901 (2003) (reporting numerous studies which have found that "frequent, highly publicized checkpoint programs substantially reduced alcohol-related crashes 10–15%," and that one difference between states with and without checkpoints is that "[s]tates with frequent checkpoint programs also have officials who understand the importance of deterring alcohol-impaired driving irrespective of the arrest rate").

policies. An example is the state's potentially overbroad employment of fear in counterterrorism.[239] Scholars of cost-benefit analysis argue that the methodology has the capacity to price abstract concepts like fear. For example, Professor Adler suggests that a properly designed oversight mechanism should not amount to "a simplistic balancing in which death- and injury-reduction are the sole regulatory benefits that are seen to counterbalance compliance costs," but should "focus (prima facie) on all constituents of welfare, including fear and anxiety."[240] If welfare measures are—at least in theory—capable of pricing fear instilled by terrorist attacks, then they should be equally up to the task of pricing fear generated by counterterrorism practices.

Sensitivity to underlying strategic pressures would also enhance the performance of specialized oversight bodies in tackling the strategic implications of, for example, secrecy. Consider the Privacy and Civil Liberties Oversight Board (PCLOB), born from a recommendation made by the 9/11 Commission.[241] The Board is empowered to:

> (1) analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and
>
> (2) ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.[242]

This is precisely the sort of organization that may make some headway because, unlike courts, the Board can navigate the boundaries between secrecy and transparency with a more comprehensive picture of the strategic landscape.[243]

---

[239] *Cf.* Eric A. Posner, *Fear and the Regulatory Model of Counterterrorism*, 25 HARV. J.L. & PUB. POL'Y 681, 684 (2002) ("[T]he regulatory response to terrorism must make fear the object of special concern.").

[240] Matthew D. Adler, *Fear Assessment: Cost-Benefit Analysis and the Pricing of Fear and Anxiety*, 79 CHI.-KENT L. REV. 977, 985 (2004).

[241] GARRETT HATCH, CONG. RESEARCH SERV., PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD: NEW INDEPENDENT AGENCY STATUS 1 (2012), *available at* http://www.fas.org/sgp/crs/misc/RL34385.pdf.

[242] 42 U.S.C. § 2000ee(c)(1)–(2) (Supp. V 2011).

[243] *See, e.g.*, PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 137–72 (2014), *available at* http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf (comparing the capabilities of the bulk metadata program with alternative information-gathering methods, gauging the efficacy of the metadata program, and weighing the value of the metadata program with its costs in terms of privacy and civil liberties).

The Board had a rocky start thanks to a controversy surrounding its independence from the White House.[244] In its latest, more independent, incarnation, it first achieved a quorum in August 2012 and a chairman was finally tapped in June 2013.[245] The most important limitation, though, is that the amount of power PCLOB ultimately wields is a matter of doubt and its budget has thus far been anemic. That said, it is suggestive that the President, in the weeks following the recent NSA revelations, chose to meet with the Board[246] and subsequently referenced it in a press conference focused on oversight of intelligence.[247]

CONCLUSION

Unlike the role that it played in the Cold War, deterrence hardly supplies a grand unified theory for all of contemporary counterterrorism. For example, counterterrorism necessarily entails tactical decisionmaking and discrete interventions prompted by incapacitationist logic. But deterrence plays a far greater role in counterterrorism than is generally assumed, especially by lawyers and legal academics. This insight carries broad implications for law, policy, and institutional design. In this Article I have drawn attention to the emergence of what I call new deterrence, which represents a cluster of refinements to classical deterrence theory designed to make the concept relevant to contemporary security challenges. I have highlighted implications of new deterrence for counterterrorism policy and law, and have drawn attention to certain barriers impeding the wider incorporation of new-deterrence–based logic in overseeing and organizing counterterrorism. But the project of deterring terror need not lead to a legal or institutional dead end. By more coherently aligning judicial doctrine with strategy, and by organizing the national security state and its overseers in a manner that incorporates the

---

244 *See* HATCH, *supra* note 241, at 4–5 (describing the White House controversy).

245 Steven Aftergood, *Senate Confirms Chair of Privacy & Civil Liberties Oversight Board*, SECRECY NEWS (May 8, 2013), http://blogs.fas.org/secrecy/2013/05/medine-pclob/.

246 Julie Pace, *Obama to Meet with Privacy, Civil Liberties Board*, TALKING POINTS MEMO (June 21, 2013, 10:14 AM), http://talkingpointsmemo.com/news/obama-to-meet-with-privacy-civil-liberties-board.php.

247 *Transcript: President Obama's August 9, 2013, News Conference at the White House*, WASH. POST, Aug. 9, 2013, http://www.washingtonpost.com/politics/transcript-president-obamas-august-9-2013-news-conference-at-the-white-house/2013/08/09/5a6c21e8-011c-11e3-9a3e-916de805f65d_story.html ("[A]s president, I've taken steps to make sure that [surveillance programs] have strong oversight by all three branches of government and clear safeguards to prevent abuse and protect the rights of the American people."). The President also mentioned the creation of a designated privacy and civil liberties officer within NSA. *Id.* This position will presumably complement posts such as exist in the ODNI, NCTC, and DHS.

teachings of new deterrence, progress can be made. The ambition of this Article is to stimulate new thinking along these lines. At the most basic level, national security law must rest upon a deep understanding of the practice of national security, including the strategies and institutions that define and shape it.[248] This Article serves as a call to greater scholarly and practical confrontation with the doctrinal and institutional corollaries to the rise of new deterrence.

---

[248] *See, e.g.*, Samuel J. Rascoff, *Establishing Official Islam? The Law and Strategy of Counter-Radicalization*, 64 STAN. L. REV. 125, 162–79 (2012) (arguing that law and strategy are necessarily intertwined in contemporary national security).