Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate

Robert Chesney*

Leon Panetta appeared on *PBS Newshour* not long after the raid that killed Osama bin Laden.[1] He was the Director of the Central Intelligence Agency at that time, and during the course of the interview he took up the question of the CIA's role in the attack. It had been "a 'title 50' operation," he explained, invoking the section of the U.S. Code that authorizes the activities of the CIA.[2] As a result, Panetta added, he had exercised overall "command."[3]

This surely confused at least some observers. The mission had been executed by U.S. Navy SEALs from Joint Special Operations Command (JSOC) after all, and both operational and tactical command seemed to have resided at all times with JSOC personnel.[4] But for those who had been following the evolution of the CIA and JSOC during the post-9/11 period, Panetta's account would not have been surprising. The bin Laden raid was, from this perspective, merely the latest example of an ongoing process of convergence among military and intelligence activities, institutions, and authorities.

* Charles I. Francis Professor in Law, University of Texas School of Law. Special thanks to Suzanne Spaulding, and thanks as well to participants at workshops at Vanderbilt and New York University including Norman Abrams, Philip Alston, Diane Marie Amann, David Golove, Monica Hakimi, Peter Margulies, Michael Newton, Deborah Pearlstein, Richard Pildes, Harvey Rishikof, Christopher Slobogin, Stephen Vladeck, Matthew Waxman, Benjamin Wittes, and Ingrid Wuerth. I am also grateful to William Banks, David Barron, David Donatti, Chris Donesa, Louis Fisher, Jonathan Fredman, Martin Lederman, and A. John Radsan for their comments.

1. *CIA Chief Panetta: Obama Made 'Gutsy' Decision on Bin Laden Raid*, NEWSHOUR, May 3, 2011, *available at* http://www.pbs.org/newshour/bb/terrorism/jan-june11/panetta_05-03.html.

2. *Id*. Title 50 is a section of the U.S. Code addressing a range of security topics, including the standing authorities of the CIA. Title 10, in contrast, is a section of the Code devoted exclusively to the armed forces. Reflecting this distinction, the argot of national security lawyers uses "Title 50 authority" and "Title 10 authority" as shorthands for the notion that there are distinct spheres of intelligence and military operations and that each is subject to a distinct set of standing statutory authorizations and constraints.

3. *Id*.

4. Nicholas Schmidle, *Getting Bin Laden: What Happened That Night in Abbottabad*, THE NEW YORKER, Aug. 8, 2011, http://www.newyorker.com/reporting/2011/08/08/110808fa_fact_schmidle. Panetta was quick to add during his *NewsHour* interview that Admiral William H. McRaven, Commander of JSOC, had maintained actual command during the raid. *See supra* note 1.

The convergence trend is not a post-9/11 novelty. It has much deeper roots than that. The trend has accelerated considerably over the past decade, however, thanks to an array of policy, budgetary, institutional, and technological developments. And as the trend accelerates, it is becoming increasingly clear that it has profoundly important implications for the domestic law architecture governing military and intelligence activities.

That architecture is a complex affair, including what might be described as "framework" statutes and executive branch directives generated in fits and starts over the past forty years. Ideally, it serves to mediate the tension between the desire for flexibility, speed, and secrecy in pursuit of national defense and foreign policy aims, on one hand, and the desire to preserve a meaningful degree of democratic accountability and adherence to the rule of law, on the other. Of course, the legal architecture has never been perfect on this score, or even particularly close to perfection. But the convergence trend has made the current architecture considerably *less* suited towards these ends.

First, it reduces the capacity of the existing rules to promote accountability. The existing rules attempt to promote accountability in two ways. They promote it *within* the executive branch by requiring explicit presidential authorization for certain activities, and they promote accountability *between* the executive branch and Congress by requiring notification to the legislature in a broader set of circumstances. Convergence undermines these rules by exposing (and exacerbating) the incoherence of key categorical distinctions upon which the rules depend, including the notion that there are crisp delineations separating intelligence collection, covert action, and military activity. As a result, it is possible, if not probable, that a growing set of exceptionally sensitive operations – up to and including the use of lethal force on an unacknowledged basis on the territory of an unwitting and non-consenting state – may be beyond the reach of these rules.

Second, the convergence trend undermines the existing legal architecture along the rule-of-law dimension by exposing latent confusion and disagreement regarding which substantive constraints apply to military and intelligence operations. Is international law equally applicable to all such operations? Is an agency operating under color of "Title 50" at liberty to act in locations or circumstances in which the armed forces ordinarily cannot? These questions are not in fact new, but thanks to convergence they are increasingly pressing.

Government lawyers are well aware of these issues, and in fact have been grappling with them for much of the past decade, if not longer.[5] For

5. *See* John Rizzo, National Security Law Issues – A CIA Perspective, Address delivered at a conference of the American Bar Association Standing Committee on Law and National Security (May 5, 2010), *available at* http://www.abanet.org/natsecurity/multimedia/WS_30274.mp3 (noting that "this discussion has been going on inside the

many years, however, public reference to them was quite limited. The most important early post-9/11 example came in 2003, when *The Washington Times* reported that the Senate Select Committee on Intelligence was quietly attempting to expand its oversight authority in order to encompass certain clandestine military operations in response to concern about the expanding role of special operations units in the war on terrorism.[6] That effort failed in the face of fierce pushback from the Pentagon and the Senate and House Armed Services Committees,[7] but not before drawing at least some attention to the disruptive impact convergence even then was having on the accountability system.[8]

In more recent years, the media has begun to pay more sustained attention, frequently noting that the complications associated with convergence impact question of substantive authority as well as accountability. In 2010, for example, *The Washington Post* reported that a fierce interagency debate was underway in connection with "which agency should be responsible for carrying out attacks" online, with the CIA categorizing certain attacks as covert actions which are "traditionally its turf" and the military taking the position that such operations are "part of its mission to counter terrorism, especially when, as one official put it, 'al-Qaeda is everywhere.'"[9] And the same *Washington Post* story indicated that the Justice Department's Office of Legal Counsel had produced a draft opinion in spring 2010 "that avoided a conclusive determination on whether computer network attacks outside battle zones were covert or not," but that nonetheless concluded that "[o]perations outside a war zone would require the permission of countries whose servers or networks might be implicated."[10] Subsequent stories about the use of lethal force in Yemen have also raised the issue of host-state permission, suggesting that JSOC but not the CIA would be obliged to act only with such permission, and that as a result JSOC units might at times prefer to operate under color of the CIA's authority[11] (as happened in Pakistan with Osama bin Laden, and again in Yemen with Anwar al-Awlaki).[12]

executive branch for many years . . . this is not a post-9/11 phenomenon"). *See also* Matthew Dahl, *Event Summary: The bin Laden Operation – The Legal Framework* (May 25, 2011), *available at* http://www.americanbar.org/content/dam/aba/administrative/law_national_security/covert_action_event.authcheckdam.pdf).

6. Bill Gertz, *Congress To Restrict Use of Special Ops.: Presidential Finding Would Be Required*, WASH. TIMES, Aug. 13, 2003, at A1.

7. *See* Jennifer Kibbe, *The Rise of the Shadow Warriors,* FOREIGN AFFAIRS 102, 107 (Mar./Apr. 2004).

8. *See id*. Kibbe deserves substantial credit for her early identification of the convergence issue and its disruptive impact on the accountability system.

9. *See, e.g.,* Ellen Nakashima, *Pentagon Is Debating Cyber-Attacks*, WASH. POST, Nov. 6, 2010, at A1.

10. *Id*.

11. *See, e.g.,* Julian Barnes & Adam Entous, *Yemen Covert Role Pushed: Foiled Bomb*

These accounts give a sense of the range of legal questions that convergence generates, as well as the debates that surround them within the government. And that in turn is enough to frame the investigation that follows.

I proceed in two parts, beginning in Part I with a descriptive account of the convergence trend itself. Part I opens with a focus on events in the 1980s and 1990s that presaged the accelerated convergence of the post-9/11 period. Attempts by the military to develop within the special forces community capacities quite similar to those of the CIA are described in Part I.A, and CIA flirtations with the use of deadly force against terrorists are described in Part I.B. Against that backdrop, Part I.C. then explores how convergence has manifested over the past decade, with an emphasis on the CIA's kinetic turn, JSOC's parallel expansion, the development of hybrid CIA-JSOC operations, and the emergence of cyberspace as an operational domain.

Readers already familiar with the convergence phenomenon may wish to skip ahead to Part II, which examines the impact of convergence on the domestic legal architecture relevant to such activities.[13] Part II.A. clarifies what I have in mind when I refer to a domestic legal architecture, as it traces the emergence and growth of standing rules relating to (i) the internal executive branch decisionmaking process, (ii) information-sharing between the executive branch and Congress, and (iii) substantive authorizations and prohibitions relating to certain types of activity. The remainder of Part II analyzes the impact of convergence on each of these rules, demonstrating the manner in which convergence creates new problems for (and exacerbates existing problems in) the existing legal architecture. The key issues include: the increasingly large and significant set of military operations that are not subject to either presidential authorization or legislative notification; lingering suspicion with respect to what law if any

Plot Heightens Talk of Putting Elite U.S. Squads in CIA Hands, WALL ST. J., Nov. 1, 2010, at A1; Greg Miller, *CIA will Direct Yemen Drones*, WASH. POST, June 14, 2011, at A1; Siobhan Gorman & Adam Entous, *CIA Plans Yemen Drone Strikes: Covert Program Would Be a Major Expansion of U.S. Efforts To Kill Members of al Qaeda Branch*, WALL ST. J., June 14, 2011, at A8; Greg Miller & Julie Tate, *CIA Shifts Focus to Killing Targets*, WASH. POST, Sept. 1, 2011.

12. Jennifer Griffin & Justin Fishel, *Two U.S.-Born Terrorists Killed in CIA-Led Drone Strike*, FOXNEWS.COM (Sept. 30, 2011), http://www.foxnews.com/politics/2011/09/30/us-born-terror-boss-anwar-al-awlaki-killed/.

13. Many of the operations at issue in the convergence context, such as the use of drones to kill, raise a host of international law issues. *See, e.g.,* Philip Alston, *The CIA and Targeted Killings Beyond Borders* (New York University Public Law and Legal Theory, Working Paper No. 303, 2011); Robert Chesney, *Who May Be Killed? Anwar al-Awlaki as a Case Study in the International Legal Regulation of Lethal Force*, 13 Y.B. OF INT'L HUMANITARIAN LAW 3 (2010). Those questions are beyond the scope of this paper. This paper *does*, however, address whether there is variation in *domestic* law with respect to whether and when U.S. government entities must comply with certain bodies of international law (though without regard to what those bodies of international law happen to require).

restrains the CIA's use of lethal force; confusion with respect to whether and why the CIA might be at greater liberty than JSOC to conduct operations without host-state consent; and the difficulty of mapping the existing architecture onto operations conducted in cyberspace. I embed my recommendations for reform within the analysis at each step along the way. To summarize, I offer four recommendations.

Enhance Accountability within the Executive Branch. The current legal architecture requires presidential approval for "covert action" programs, but the situation is complicated with respect to unacknowledged military operations. An unacknowledged military operation must be authorized by the President or at least the Secretary of Defense if it is collateral to an *anticipated* overt military operation that is not yet imminent but for which operational planning has been authorized – a sweeping set of circumstances. But no such approval is required if the operation is collateral to ongoing hostilities. This makes sense if the unacknowledged operation occurs in the combat zone. If it occurs on the territory of another state outside the "hot" battlefield, however, the risks are sufficient to warrant extension of the requirement of presidential or at least secretarial authorization. Notably, press accounts indicate that former Secretary of Defense Robert M. Gates had insisted upon such an approach for *lethal* operations outside the hot battlefield, as a matter of policy. At a minimum, that policy should be codified. Better still to extend it to all unacknowledged military operations outside the combat zone. The degree of accountability involved should be commensurate with the risks, and in light of convergence there is little reason to calibrate that judgment differently for the military than for the CIA, at least not outside combat zones.

Enhance Information-Sharing with Congress. Operations constituting "covert action" must be reported to the House and Senate Intelligence Committees; by contrast, the unacknowledged military operations discussed above are not subject to this requirement. A separate law requires notification to Congress when the armed forces are deployed in circumstances involving a likelihood of hostilities, but given the strict interpretation of "hostilities" adopted in relation to the conflict in Libya it seems clear that a considerable amount of unacknowledged military activity might escape notification to Congress under that regime as well. An effort was made in 2003 to close this gap by requiring unacknowledged military activity to be reported to the Intelligence Committees when activity occurs outside the geographic confines of a state where the United States has an overt combat presence. The effort failed in the face of resistance from the Pentagon and the House and Senate Armed Services Committees. It should be revived, but with notification being made to the Armed Services Committees, subject to an option for close-hold notifications, based on the Gang of Eight model. All such notification scenarios should be modified, however, to include participation by the chief majority and minority

counsels of the relevant committees (creating, in effect, a "Gang of Twelve" system).

Clarify Substantive Constraints on Title 50 Operations. It should be made clear that all U.S. government agencies comply with the law of war in any operation to which the law of war applies, regardless of whether the operation is categorized as a Title 10 or a Title 50 activity and regardless of which particular agency carries it out. This is not necessarily a change from current policy, but it would help to address concerns that critics have raised with respect to whether the CIA conforms its drone operations to law of war standards. On the other hand, it would not be appropriate to adopt a similar express commitment vis-a-vis international law's treatment of state sovereignty, given lingering uncertainty with respect to whether and when international law prohibits one state from conducting espionage, covert action, or other operations within another state's territory in the first place.

Clarify Authorization and Accountability for Cyberoperations. Operations in cyberspace tend to defy categorization by type (collection, covert action, or military activity) or geographic location. This causes problems on all the dimensions mentioned above, while also raising difficult questions regarding when an agency has the affirmative authority to conduct such operations in the first place. Legislation can resolve much of this uncertainty by (i) clarifying that the military has standing authority to conduct computer network attacks (unacknowledged or otherwise) when acting in a defensive capacity or under color of a statutory authorization for the use of military force, and (ii) providing timely notification to the House and Senate Armed Services Committees of such operations when they have or are likely to have significant consequences outside a theater of combat operations.

I. THE CONVERGENCE TREND

The notion of "convergence" between military and intelligence activities would likely have seemed strange prior to the second half of the twentieth century. The U.S. military was no stranger to the business of intelligence after all. On the contrary, it had engaged in the collection and analysis of intelligence throughout American history, at least during times of armed conflict, and during World War II had developed the Office of Strategic Services (OSS) as the very embodiment of a "military" organization devoted to the full spectrum of "intelligence" activities.

But the center of gravity shifted in the late 1940s when the Truman administration and Congress began reorganizing the national security establishment to suit the imperatives of the Cold War and America's newfound status as the predominant Western global power. To be sure, executive branch departments had often exercised intelligence functions in the past, but prior to 1946 there had never been a free-standing agency, let alone a *civilian* one, intended to be distinct from the military establishment

and capable of relatively disinterested analysis, reporting directly to the President, devoted to collection, analysis, and covert action. Thus it was a significant novelty when President Harry S. Truman ordered the creation of the Central Intelligence Group in 1946 as a civilian successor to the OSS and when Congress the next year transformed that body into the CIA.[14]

Over the following decades, the CIA became the predominant institution associated with human intelligence, or HUMINT, collection, outside the context of open armed conflict.[15] It also became the repository of America's covert action capacity as that realm of activity became increasingly significant during the Cold War. As a result of both developments, the notion of a distinction between military and intelligence activities came to seem more meaningful than it had been in the past. Various legal developments described below in Part II.A., reinforced and embodied that notion as well. The distinction was always tenuous, however, and by the early 1980s the early signs of convergence already were apparent.

A. Convergence and the Military in the 1980s

Though it is true that the late 1970s and early 1980s saw a significant revival in Cold War tensions, there were some during that same period who were turning their attention at least in part to unconventional threats involving noncommunist, non-state adversaries. One such strategic thinker was General Edward Meyer, the Army's Chief of Staff from 1979 to 1983. According to one of his subordinates, Meyer believed that America's "adversaries were affecting us below the threshold of war," and America needed to build its capacity to respond in kind.[16]

From Meyer's perspective, the situation did not call for a greater CIA role so much as for the military to expand its own capacity to fight in the shadows – above all through Special Operations Forces (SOF). Of course, the military already had some such capacity, as illustrated by the Army's 1st Special Operations Detachment-Delta (Delta Force) and the Navy's SEAL Team Six. These units were capable of executing small-scale kinetic operations such as hostage rescue, including in denied areas. Or at least they could do so when supplied with the necessary tactical intelligence to support such operations. And thus a question had arisen: Should SOF units rely on the CIA and the rest of the Intelligence Community (including the

14. *See generally* AMY ZEGART, FLAWED BY DESIGN: THE EVOLUTION OF THE CIA, JCS, AND NSC (1999).

15. Signals intelligence, or SIGINT, by contrast, has been the bailiwick of the DoD's National Security Agency (NSA), even as to non-military surveillance.

16. Seymour Hersh, *Who's in Charge Here?*, N.Y. TIMES, Nov. 22, 1987 (quoting Lt. Col. Michael Foster, who served in the Army's Special Operations Division during Meyer's tenure in the early 1980s).

Defense Intelligence Agency and the Service intelligence agencies) to provide them with intelligence and non-kinetic forms of covert support, or should the SOF community develop parallel, in-house capacities?

The issue came to a head twice during the Tehran hostage crisis in 1979-1980. Famously, the Carter administration authorized a Delta Force rescue operation (Operation Eagle Claw).[17] But obtaining the tactical intelligence and covert logistical support necessary for that mission proved to be exceedingly difficult. The CIA failed to provide it, possibly reflecting contemporaneous personnel and morale problems CIA was experiencing in the late 1970s and early 1980s[18] and certainly reflecting the problems caused by the capture of CIA personnel and files during the embassy takeover.[19] In any event, the SOF community ultimately came to the conclusion that "there existed nowhere in the national capability an organization to provide this vital support,"[20] including within the military itself.[21]

Operation Eagle Claw ultimately was aborted because of a deadly accident at a staging area within Iran. Planning for another rescue operation (Operation Snowbird) began soon after, however, and this time the military took steps to create the intelligence and logistical support services it needed.[22] Toward that end, the Joint Chiefs of Staff authorized creation of

17. *See* MARK BOWDEN, GUESTS OF THE AYATOLLAH: THE FIRST BATTLE IN AMERICA'S WAR WITH MILITANT ISLAM (2006).

18. Caryle Murphy & Charles R. Babcock, *Army's Covert Role Scrutinized: Financial Probe Raises Fear that Special Units "Got Carried Away,*" WASH. POST, Nov. 29, 1985, at A1, A8-A9; *see also* James Bamford, *Where Secret Armies Clash by Night*, WASH. POST, July 3, 1988, at X11 (reviewing STEVEN EMERSON, SECRET WARRIORS: INSIDE THE COVERT MILITARY OPERATIONS OF THE REAGAN ERA (1988)); Hersh, *supra* note 16 (noting "widespread belief" that CIA "had been weakened" in this respect, and contending that this perception incentivized the Army to develop its SOF-based capacity for clandestine operations).

19. Richelson notes that some CIA officers had been taken hostage, and that some Iranian CIA assets were either missing or dead as a result of the revolution. *See* Jeffrey T. Richelson, *"Truth Conquers All Chains": The U.S. Army Intelligence Support Activity, 1981-1989*, 12 INT'L J. INTEL. & COUNTERINTEL. 168, 169 (1999). Richelson also quotes an anonymous government official asserting that "the agency [CIA] people were preoccupied with keeping their cover and could not provide equipment or information for the [rescue] operation." *Id*.

20. BRIEF HISTORY OF UNIT, *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB46/document11.pdf (partially-redacted government document describing the origins of the Intelligence Support Activity unit) [hereinafter BRIEF HISTORY].

21. *See* Memorandum from Lt. Gen. Philip Gast, Director of Operations for the Joint Chiefs of Staff, to Director of the Defense Intelligence Agency (Dec. 10, 1980), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB46/document6.pdf. General Gast, notably, had served in Iran as chief of a military advisory contingent between 1977 and October 1979. *See* U.S. AIR FORCE, BIOGRAPHY OF LIEUTENANT GENERAL PHILIP C. GAST, http://www.af.mil/information/bios/bio.asp?bioID=5502.

22. Richelson suggests that the military also took the initiative prior to the aborted Eagle Claw mission, dispatching "at least two teams of individuals" who entered Iran on false passports and "attempted to collect the required on-the-ground intelligence." Richelson,

the Foreign Operations Group (FOG), which "was an adhoc [*sic*] organization" tasked with providing "a combination of intelligence collection and operational support to a striking force."[23] FOG's work never came to fruition, as the Iranians released the hostages upon the inauguration of President Ronald Reagan in January 1981. But in the meantime the Joint Chiefs of Staff's Director of Operations already had recommended institutionalizing FOG because the "current DOD/Service HUMINT structure is not organized to satisfy" the "need of military planners to have accurate and timely situation oriented operational and environmental data."[24] Within two weeks of Reagan's inauguration, Army Chief of Staff Meyer responded by "authoriz[ing] creation of the US Army Intelligence Support Activity, or ISA, to "institutionaliz[e] in a DoD special unit . . . a worldwide, immediately responsive capability similar to that developed over a one year period in the Tehran crisis."[25]

ISA encountered rough waters almost immediately.[26] It reportedly became involved in a private effort to rescue POWs allegedly still held in Laos,[27] and this and other allegations spurred the DoD Inspector General to conduct an investigation culminating in the conclusion that ISA "lacked proper oversight mechanisms for its missions and its expenditures."[28] Secretary of Defense Caspar W. Weinberger was alarmed, as was Deputy Secretary of Defense Frank C. Carlucci, who had been the second highest ranking official at CIA previously. Carlucci wrote in May 1982 that he found the Inspector General's report "disturbing in the extreme," adding that "[w]e seem to have created our own CIA, but like Topsy,

supra note 19, at 169.

23. BRIEF HISTORY, *supra* note 20.

24. Richelson, *supra* note 19, at 170 (quoting Memorandum from Lt. Gen. Philip C. Gast, Director of Operations, to Lt. Gen. Eugene Tigh, Director, Defense Intelligence Agency (Dec. 10, 1980)).

25. BRIEF HISTORY, *supra* note 20.

26. So too did the contemporaneous Yellow Fruit initiative, which may or may not have been related to ISA. Yellow Fruit operated under cover of a business based in Northern Virginia, apparently with the aim of ensuring operational security on the part of other special operations units (as well as possible involvement in securing logistical support for other military or CIA operations, such as the provision of transportation or communications equipment). *See* Murphy & Babcock, *supra* note 18. Whatever its origins, allegations of gross financial improprieties brought Yellow Fruit to an end in 1983. For an overview of Yellow Fruit and its demise, see Hersh, *supra* note 16. For more detail, including allegations that a Swiss bank account created for Yellow Fruit later was used to support arms shipments to the Contras, see Dan Morgan, *Secret Army Account Linked to Contra Aid: North, Secord Possibly Involved, Official Says,* WASH. POST, Apr. 22, 1987, at A1; Jeff Gerth, *Pentagon Linking Secret Army Unit to Contra Money*, N.Y. TIMES, Apr. 22, 1987, at A1.

27. *See* Tim Weiner, *Covert Forces Multiply, Some Run Amok*, PHILL.COM (Feb. 10, 1987), http://articles.philly.com/1987-02-10/news/26179065_1_covert-action-covert-operations-black-budget.

28. Richelson, *supra* note 19, at 173.

uncoordinated and uncontrolled."[29] Invoking the "lesson of the 70s," Carlucci directed that all ISA operations be terminated in thirty days unless a more accountable structure could be devised, subject to approval from the DoD General Counsel as well as the Director of Central Intelligence.[30]

ISA survived, but emerged a far more constrained entity. From 1983 on, ISA would operate under a formal DoD "charter."[31] The charter imposed more intra-Army transparency and accountability, specifying that certain senior Army officials would have tasking and oversight authority over ISA's activities and requiring ISA to operate under the auspices of the Army's Assistant Chief of Staff for Intelligence rather than its Assistant Chief of Staff for Operations (as General Meyer originally had planned).[32] The charter did not restrict ISA's range of permitted activities in a substantive sense – on the contrary, the charter contemplated that ISA might engage in both collection and covert action – but it did make clear that the former could be conducted only with approval from both the CIA and Defense Intelligence Agency (DIA), and that the latter required compliance with Executive Order 12,333 governing intelligence activities[33] (discussed below in Part II.A.). Perhaps most significantly, the charter's concluding provision specified that the Army's General Counsel would be responsible for ensuring that "all congressional committees having pertinent legislative or appropriation oversight responsibilities are kept fully and currently informed of [ISA] activities in accordance with applicable statutes, Executive Orders, and DOD directives and regulations."[34]

It is unclear from the public record what became of ISA (and its successor organizations)[35] in the years that followed. The important point for now, however, is that more than thirty years ago, the military – and especially the SOF community within the military –was already reacting to a perceived trend in the direction of asymmetric threats by developing in-

29. Memorandum from Frank C. Carlucci, Deputy Secretary of Defense, on ISA Operations to Richard Stilwell, Deputy Under Secretary for Policy (May 26, 1982), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB46/document7.pdf. "Topsy" was a character in Harriet Beecher Stowe's 1852 novel *Uncle Tom's Cabin* who when asked how she had come into the world, could not explain how, saying only that she must have grown. This gave rise to the once-common saying "grew like Topsy," which originally conveyed a sense of unexplained origins but later came to suggest unconstrained proliferation as well.

30. *Id*.

31. *See* Richelson, *supra* note 19, at 175-176.

32. On Meyer's original approach, see Hersh, *supra* note 16.

33. *See* Richelson, *supra* note 19, at 175-76. *See also* UNIT CHARTER, CHARTER OF U.S. ARMY INTELLIGENCE SUPPORT ACTIVITY, *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB46/document8.pdf [hereinafter CHARTER].

34. CHARTER, *supra* note 33, ¶10(d)(3).

35. *See* Richelson, *supra* note 19, at 192 (suggesting that ISA lived on past its formal disestablishment in 1989, under various names, as a subordinate unit of Special Operations Command). *See also* MARK BOWDEN, KILLING PABLO: THE HUNT FOR THE WORLD'S GREATEST OUTLAW 72-73 (2001) (providing a list of alternative names).

house capacities that seemed to compete directly with functions associated with the CIA (including collection and covert action capacities). It was, in short, an early manifestation of convergence.

B. Convergence and the CIA from the 1980s until 9/11

Convergence also manifested within the CIA in the pre-9/11 era in mirror-image fashion. Just as the military experimented with CIA-like activities outside the context of the existing military components of the Intelligence Community, the CIA at around the same time was experimenting with military-like activities. Specifically, the CIA was flirting with the use of lethal force in circumstances in which diplomatic and political constraints made overt military force unpalatable.

To be sure, the use of lethal force by or at the direction of the CIA was not a 1990s novelty. Plots to kill Castro with exploding cigars and alleged plots to kill other Communist or Soviet-leaning political leaders in pursuit of foreign policy aims had, after all, played a central role in the embarrassing revelations and scrutiny of the 1970s (to which Carlucci alluded in his criticism of ISA, above), and had prompted a series of executive orders prohibiting "assassination" by executive branch employees (as described below in Part II.A.).[36] But the CIA's use of lethal force in the 1980s and thereafter in relation to terrorism was not just a matter of pursuing mere foreign policy. It was, rather, a question of circumstances involving threats to American lives. That is, it was a matter implicating the use of force in national self-defense, a justification ordinarily associated with military action.[37]

1. Using Lethal Force Against Hezbollah in 1984

The CIA's turn toward counterterrorism had its roots in a series of terrorist attacks resulting in American deaths in the early-to-mid-1980s, including the bombing in Beirut in 1983.[38] These events led to repeated

36. The CIA also has a long history of paramilitary activity. *See, e.g.,* Richard A. Best, Jr. & Andrew Feickert, *Special Operations Forces (SOF) and CIA Paramilitary Operations: Issues for Congress* (Cong. Res. Service RS22017), Jan. 4, 2005, at 3. For a discussion of the many ways in which questions of lethal force may arise in relation to CIA activities, entirely apart from operations specifically intended to cause death, see Jonathan Fredman, *Policy and Law: Covert Action, Loss of Life, and the Prohibition on Assassination*, 40 CENTRAL INTELLIGENCE AGENCY: STUDIES IN INTELLIGENCE 15 (1997).

37. *See, e.g.,* Abraham D. Sofaer, *Terrorism, the Law and National Self-Defense* 126 MIL. L. REV. 89 (1989). For a discussion of national self-defense concepts in relation to targeted killing and covert action after 9/11, see Kenneth Anderson, *Targeted Killing in U.S. Counterterrorism Strategy and Law*, in LEGISLATING THE WAR ON TERROR: AN AGENDA FOR REFORM 346-400 (Benjamin Wittes ed., 2009).

38. *See* STEVE COLL, GHOST WARS: THE SECRET HISTORY OF THE CIA, AFGHANISTAN,

debate within the Reagan administration over whether and when to use force to respond to or preempt terrorist attacks, including both the overt military option and the idea of instead using lethal force covertly (either directly by the CIA or through CIA-trained proxy forces).[39]

The lethal covert action option appears to have arisen first in the spring of 1984. A proposal drafted by Lieutenant Colonel Oliver North (then serving on the staff of the National Security Council) included language that would authorize covert action to "neutralize" terrorists with lethal force, using CIA-trained proxies in cases where the terrorists either already had attacked Americans or were planning to do so.[40] This drew fierce condemnation from the Agency's Deputy Director, John McMahon, who called North to berate him for forgetting the lessons of the 1970s relating to CIA involvement in assassination.[41] Director William Casey, already sympathetic to North's proposal, at this point turned to his General Counsel, Stanley Sporkin, to weigh in on McMahon's objection.[42] Sporkin concluded that there was a salient distinction between political assassination along the lines of the Castro plots of the 1970s and the exercise of force in national self-defense and that the task of preempting terrorist attacks fell on the proper side of that line.[43] Casey thereafter put his weight behind North's proposal, and a version of it appears to have prevailed in the end. National Security Decision Directive 138 (NSDD 138), which President Reagan signed that April, remains a classified document. It has been reported, however, that NSDD 138 included language authorizing "the use of sabotage, killing (though not "neutralization" or assassination), [and] preemptive and retaliatory strikes" against terrorists, and that it also included authorization for CIA officers to cooperate with SOF personnel in such missions.[44]

Noel Koch, a Pentagon official known as a major supporter of SOF, later lamented that NSDD 138 "was simply ignored. No part of it was ever implemented."[45] What happened? Within a few months of NSDD 138, Director Casey and Secretary of State George P. Shultz urged President

AND BIN LADEN, FROM THE SOVIET INVASION TO SEPTEMBER 10, 2001, at 137-138 (2004); *see also* DAVID C. WILLS, THE FIRST WAR ON TERRORISM: COUNTER-TERRORISM POLICY DURING THE REAGAN ADMINISTRATION (2003).

39. *See* TIMOTHY NAFTALI, BLIND SPOT: THE SECRET HISTORY OF AMERICAN COUNTERTERRORISM 145-147 (2005); *see also id.* at 148 ("The solution to the disagreement over using overt means was to choose covert action instead.").

40. BOB WOODWARD, VEIL: THE SECRET WARS OF THE CIA, 1981-1987, at 361 (1987).

41. *See id.* at 361-362. Interestingly, it does not appear from the public record that this proposal, or others akin to it described below, generated comparisons to or criticisms involving the Agency's involvement in the Phoenix program in Vietnam.

42. *See id.* at 362.

43. *See id.* at 362, 394.

44. WILLS, *supra* note 38, at 84.

45. *Id.* at 87.

Reagan to issue a finding that would seem to be in line with NSDD 138, as it

> would direct the CIA to train and support small units of foreign nationals in the Middle East which would conduct preemptive strikes against terrorists. When intelligence showed that someone was about to hit a U.S. facility, such as an embassy or a military base, the units would be able to move to disable or kill the terrorists.[46]

The preemptive strike proposal was developed by the National Security Council (NSC) and called for the CIA to "train and equip Lebanese 'hit men' who would be responsible for tracking down the people responsible for the terrorist attacks on U.S. facilities and the abduction of three U.S. citizens."[47] Not inconsistently, Woodward's account specifies that there would be two stages of authorization. An initial approval would authorize the creation and training of the unit itself, while a second and more specific approval would be necessary in order to authorize any specific operation by the unit.[48]

It appears that President Reagan approved this proposal in early November 1984, with a focus on as many as three separate Lebanese proxy units.[49] The CIA was thus put into the business of using lethal force via proxies as an alternative to an overt military response against terrorists including, at least, Hezbollah. Some at the time explicitly viewed this new CIA paramilitary capacity as "in competition with the Pentagon."[50]

Things did not proceed smoothly from there, however. Richard Helms, who had previously served as Director of Central Intelligence, got wind of the new program and, feeling that it smacked of the assassination programs that had gotten the CIA into such trouble in the past, reached out to Vice President George H. W. Bush (himself a former Director of the CIA) to express his concerns.[51] Internally, some senior CIA officials, particularly Deputy Director McMahon, felt much the same way, expressing concern that the CIA would be blamed for instigating an assassination program.[52]

What ultimately derailed the program, however, were doubts about the proxies themselves. The CIA and the State Department worked together to make it possible for a team of SOF personnel to inspect the Lebanese proxies on two occasions, and the resulting negative evaluations simply

46. WOODWARD, *supra* note 40, at 393.
47. NAFTALI, *supra* note 39, at 148.
48. WOODWARD, *supra* note 40, at 393.
49. *See* NAFTALI, *supra* note 39, at 148*;* WOODWARD, *supra* note 40, at 405.
50. *See* WOODWARD, *supra* note 40, at 362.
51. *See* NAFTALI, *supra* note 39, at 150-151.
52. *Id.* at 151. *See also* WOODWARD, *supra* note 40, at 394.

took the wind out of the program's sails.[53] Or at least it did so with respect to relying on Lebanese proxies. According to Woodward, Director Casey responded to the collapsing Lebanese effort by turning to the Saudi intelligence service with a request that they target Hezbollah's leader, Mohammed Hussein Fadlallah; and in Woodward's account, this occurred without the knowledge of McMahon or other internal CIA opponents, without any additional presidential authorization, and without notification to Congress.[54] Eventually, Casey's alleged Saudi initiative may have culminated in a massive car bombing in early 1985 near Fadlallah's Beirut residence. That attack, assuming it was indeed directed at Fadlallah, was a fiasco; dozens died, hundreds were wounded, Hezbollah made sure to blame America, and Fadlallah was unharmed.[55] In the aftermath, Casey told McMahon that he was going to "call the president . . . and tell him we have to rescind the finding and shut down the operation."[56]

These events underlined the level of aversion within the CIA and more broadly to anything that might be depicted as assassination, but also the strong desire to take whatever steps were possible in order to prevent further terrorist attacks. The latter force drove the CIA toward involvement in the use of lethal force in the name of self-defense, while the former acted as a check on that impetus.[57] The Fadlallah bombing for the time being tilted the balance in favor of caution, but so long as the underlying threat of terrorism remained – and so long as covert action through the CIA appeared to provide a politically-palatable alternative to the overt use of military force – the issue was bound to resurface.

2. Counterterrorism "Action Teams" in 1986

It did not take long. The terrorist attacks at El Al Airlines ticket counters in Rome and Athens in late 1985, which killed several Americans, prompted Casey to revisit the idea of a covert action capacity to use lethal

53. *See* NAFTALI, *supra* note 39, at 151-152.

54. *See* WOODWARD, *supra* note 40, at 395-397; NAFTALI, *supra* note 39, at 152.

55. *See* WOODWARD, *supra* note 40, at 397.

56. NAFTALI, *supra* note 39, at 152. Woodward asserts that Fadlallah was subsequently mollified by a $2 million Saudi bribe, in exchange for which he agreed to cease supporting attacks on U.S. and Saudi interests. *See* WOODWARD, *supra* note 40, at 397.

57. Another example of this tension arose in 1985 in connection with a covert action program directed at undermining the Muammar Gadhafi regime in Libya. Woodward reports that members of SSCI expressed concern to Director Casey that efforts to support Libyan dissidents and exiles could run afoul of the prohibition on assassination "since the exile movement wanted [Muammar Gadhafi] dead" and "support to potential murderers was murder, period." *Id.* at 419. Director Casey did not object to the proposition that it would be a problem if Gadhafi's death was sought, but rather responded that this was not the goal of the program. *Id.* The senators involved nonetheless protested in a letter to Reagan about the prospects of a CIA "assassination" program. *Id.*

force to preempt further attacks.[58] Casey had in mind "action teams that could put the CIA on the offensive in a global campaign against terrorist groups," and he tasked Duane R. "Dewey" Clarridge, a key figure in the CIA's Directorate of Operations (DO), with developing a proposal to that effect.[59] Clarridge recommended "formation of two super-secret 'action teams' that would be . . . authorized to kill terrorists if doing so would preempt a terrorist event, or arrest them and bring them to justice if possible."[60] Working with a new NSC-based interagency coordinating committee, Clarridge began developing a new covert action finding to authorize the "action team" model.[61] The NSC committee, notably, had a "founding directive" that grappled explicitly with the question of whether terrorism should be seen as an issue of law enforcement or national security, and whether, as paraphrased by Steve Coll, the CIA should "try to capture terrorists alive in order to try them on criminal charges in open courts, or should the goal be to bring them back in body bags[.]"[62]

In a National Security Decision Directive (NSDD 207) issued in January 1986, the Reagan administration endorsed a nuanced position. Terrorism was a law enforcement issue in some contexts, but capture for trial would not always be possible, and in some situations, a military-style response would be needed.[63] And in a covert action finding issued that same day, President Reagan made clear that the U.S. military was not the only instrument through which such force might be used.[64] The finding reportedly authorized the use of "action teams" as Casey and Clarridge had wished, including via foreign proxies or, apparently, CIA personnel.[65]

Once again, however, there was resistance. The "action team" concept "stirred nervous reaction on Capitol Hill," with "[s]ome privately label[ing] them 'hit teams.'"[66] Of particular concern were the boundaries of the authority to use lethal force. Apparently the finding authorized such action

58. *See* COLL, *supra* note 38, at 139.

59. *See id.*

60. *Id.* at 139-140. Clarridge also recommended establishing an integrated counterterrorism center to support these efforts, with integrated operational, analytical, and technical personnel. *See id*. at 140. Such a holistic approach ran counter to the traditional CIA model of strict separation between operations and analysis, not to mention its traditional emphasis on geographic regions. *See id.* at 139-140 The proposal encountered resistance because it violated the traditional model, and also because of a belief that counterterrorism was "'police work' best left to cops or the [FBI]." *Id* at 139-140. But Casey was persuaded, and this gave rise to CIA's Counterterrorist Center. *Id.* at 140-141.

61. *See id.* at 140-141.

62. *Id.* at 140-141.

63. *See id.* at 141.

64. *See id.* at 141.

65. *See id.* at 141.

66. *Id.* at 141.

only where an attack was imminent, for Robert Gates would later recall there was much debate about just where the line might lie in practical terms:

> [W]e got to the question of when you could kill a terrorist, and we had this almost theological argument. "Well, if the guy is driving toward the barracks with a truck full of explosives, can you kill him?" "Yeah." "Well, what if he's in his apartment putting the explosives together?" "Well, I don't know."[67]

The debate over how imminent a threat must be in order to warrant lethal force remains a central question – perhaps *the* central question – today.[68] The important point for now, however, was that the CIA in 1986 again was being asked to embrace the use of lethal force as an instrument of national self-defense, albeit in a context of discomfort about the underlying principle and uncertainty about the metes and bounds of the authority in question. The public record sheds no light on whether and to what extent the action team concept was put into practice over the next decade.

3. Lethal Force Against al Qaeda from 1998 until 9/11

By the fall of 1997, the CIA was well aware that Osama bin Laden and his al Qaeda organization constituted an increasingly important threat.[69] The Agency had established a special unit within its Counterterrorist Center to focus specifically on bin Laden, and a plan to locate him was in the works.[70] But the goal at that time was not to kill bin Laden. The idea, instead, was to capture him and render him to the United States or elsewhere to face prosecution.

Locating and capturing bin Laden was no simple task, however. The operation probably could not be executed by CIA officers. They would not be able to function effectively for this purpose in Afghanistan, at least not in comparison with Afghans. In any event, land-locked Afghanistan at the time was perceived as too remote and too hostile an environment to justify the risks, manpower, and resources that boots-on-the-ground American

67. *Id.* at 141.

68. *See., e.g.,* John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism, *Strengthening Our Security by Adhering to Our Values and Laws*, Address delivered at Harvard Law School's Program on Law and Security (Sept. 16, 2011) (discussing the role of imminence in targeting decisions outside the "hot" battlefield), *available at* http://www.whitehouse.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our-security-adhering-our-values-an; Robert Chesney, *Malinowski on IHL away from the Battlefield and on the Meaning of Imminence*, LAWFARE (Dec. 14, 2010), http://www.lawfareblog.com/2010/12/malinowski-on-ihl-away-from-the-battlefield-and-on-the-meaning-of-imminence/.

69. *See* COLL, *supra* note 38, at 367.

70. FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 110 (2004) [hereinafter 9/11 COMM. REP.].

involvement would entail. The plan, therefore, was to use an Afghan proxy force in a non-lethal variant of the action team concept.

Fortunately, a plausible proxy force was already in place. In connection with the hunt for Mir Aimal Kasi – a Pakistani man who had killed several CIA employees on the street outside CIA headquarters in Langley – other personnel at the Counterterrorist Center had been training and equipping a "family-based team of paid agents" to effectuate a similar locate-and-capture operation.[71] And after Kasi turned up in Pakistan, the team (known within the CIA as FD/TRODPINT, but referred to later in the 9/11 Commission Report simply as the "Afghan tribals") was available for a new project.[72]

The next question was whether a new presidential authorization would be necessary to undertake this operation or if instead it could be said to fall within the scope of the 1986 action team program described above.[73] Ultimately, the decision was made that this did fall within the scope of the 1986 program, and a Memorandum of Notification (MON) was duly issued to the congressional oversight committees explaining this new application of that existing authority. The process of drafting the MON, however, became the occasion for the reemergence of a familiar debate.

Despite the fact that the goal of the proposed operation was to capture rather than kill bin Laden, the fact remained that it was quite possible, if not likely, that the attempt would produce a shootout in which bin Laden would be killed. That prospect – the unintended but nonetheless foreseeable killing of bin Laden – revived the debates of the 1980s regarding lethal covert action, despite the fact that the 1986 action team decision might seem to have resolved such disputes in favor of even the *intentional* use of deadly force. "Discussion of this memorandum brought to the surface an unease about paramilitary covert action that had become ingrained at least among some CIA senior managers," according to the 9/11 Commission Report.[74] Echoing the position taken by Deputy Director McMahon and others in the 1980s, James L. Pavitt (who later became Deputy Director of

71. *See* Steve Coll, *A Secret Hunt Unravels in Afghanistan: Mission To Capture or Kill al Qaeda Leader Frustrated by Near Misses, Political Disputes*, WASH. POST, Feb. 22, 2004, at A1.

72. *Id*.

73. *See* 9/11 COMM. REP., *supra* note 70, at 113 (observing that a "1986 presidential finding had authorized worldwide covert action against terrorism and probably provided adequate authority," though "senior CIA managers may have wanted something on paper to show that they were not acting on their own"); COLL, *supra* note 38, at 423 ("The agency already had legal authority to disrupt and arrest terrorists under the 1986 presidential finding that established its Counterterrorist Center. . . . It seemed wiser to use a MON to amend the legal authority the center already possessed, to make it more specific.").

74. 9/11 COMM. REP., *supra* note 70, at 113.

Operations) "expressed concern that people might get killed; it appears he thought the operation had a least a slight flavor of a plan of assassination."[75]

As a result of these concerns, case officers were at pains to convey to the Afghan tribals that they were not supposed to kill bin Laden:

> CIA officers met with their TRODPINT agents in Pakistan to emphasize that their plan to capture bin Laden and hold him in the Afghan cave could not turn into an assassination. "I want to reinforce this with you," one officer told the Afghans, as he later described the meeting in cables to Langley and Washington. "You are to capture him alive."[76]

By this point, the project had come to focus on the prospects for capturing bin Laden while he stayed at the Tarnak Farms compound near Kandahar, a location where a large number of family members, including children, would be close by. There was considerable fear that the tribals would fire indiscriminately in the course of attempting the capture, causing collateral damage even if they succeeded in capturing bin Laden alive and then somehow extricating him and themselves from the compound.[77] The CIA's top leadership ultimately determined not to support the operation, as did key White House officials.[78] By the summer of 1998 the project was put on hold pending further developments.[79]

There things stood when two and a half months later al Qaeda struck the U.S. embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania. Overnight, the propriety of using lethal force against al Qaeda looked dramatically different on all the relevant dimensions.

Within a day of the bombings, an opportunity to attempt to kill bin Laden arose, and the Clinton administration seized it. The CIA informed the NSC principals that a large gathering of militants – including bin Laden – would take place in Afghanistan the following week. The principals accordingly recommended that the President order an overt strike – specifically, a cruise missile attack – with the "purpose to kill bin Laden and his chief lieutenants" at that meeting.[80] The President agreed, and ordered the attack – including notification to Congress "consistent with the War Powers Resolution."[81] Congress, notably, had not in the interim passed

75. *Id*. at 113. It is interesting to note that the article by Jonathan Fredman cited above at note 36, which expressly addresses scenarios such as this, was published in 1997, and thus may well have been written while such questions were being debated in connection with the plan to conduct a similar capture targeting Mir Aimal Kasi.

76. COLL, *supra* note 71.

77. *Id*.

78. *See id.*

79. *See id.; see also* 9/11 COMM. REP., *supra* note 70, at 114.

80. 9/11 COMM. REP., *supra* note 70, at 116.

81. Letter from President William J. Clinton to Congressional Leaders Reporting on

a statute to authorize the use of military force against al Qaeda, nor would it until after 9/11. But this did not stop the Clinton administration from resorting to such force, presumably (for domestic law purposes) pursuant to a claim of inherent authority under Article II of the Constitution to employ lethal force in national self-defense.

Ultimately, the August 1998 cruise missile attack in Afghanistan was only a partial success. Some militants were killed, but bin Laden himself left the scene hours before the missiles struck.[82] When he was located again, would the U.S. government still be willing, at least in principle, to attempt to kill him overtly? Would it at least be willing to kill him via covert action? Or would the willingness to resort to lethal force prove to be temporary, soon to be replaced by an insistence upon capture instead?

The Clinton administration's response to these questions was complex, and remains the subject of disagreement. First, overt lethal force did remain on the table throughout the years that followed, even though it was not actually employed.[83] The fact that no further strikes actually were launched did not reflect a belated conclusion that overt lethal force was not, or was no longer, a lawful option. Rather, the failure to launch reflected a persistent lack of actionable intelligence regarding bin Laden's location (though some, particularly within the CIA's Counterterrorist Center's unit focused on bin Laden, felt that the intelligence was good enough at various points), colored by grave concerns regarding the larger consequences of further strikes that if unsuccessful could make the United States appear feckless or that could in any event incur too much collateral damage.[84]

With those constraints in mind, it stands to reason that the *covert* rather than *overt* use of lethal force might have been viewed at the time as an attractive alternative to further cruise missile strikes. Depending on the instruments involved, after all, a covert use of force might be brought to bear more quickly than cruise missiles, and in any event deniability would allow the United States to circumvent some of the costs of a failed attack or one that caused collateral damage. Those features, in turn, might have lowered the threshold of reliability policymakers otherwise would insist upon, as a matter of policy preference, with respect to the intelligence on

Military Action Against Terrorists Sites in Afghanistan and Sudan (Aug. 21, 1998), *available at* http://www.gpo.gov/fdsys/pkg/PPP-1998-book2/html/PPP-1998-book2-doc-pg1464.htm.

82. *See* 9/11 COMM. REP., *supra* note 70, at 117. The attack in Afghanistan was accompanied by an attack against a suspected al Qaeda affiliated facility in the Sudan (the Al-Shifa pharmaceutical plant). There has been considerable controversy ever since regarding the accuracy of the intelligence depicting the latter as a chemical weapons facility. *See id.* at 118 n. 50.

83. *See id.* at 130-131 (discussing consideration given to a cruise missile strike in December 1998).

84. *See id.*

bin Laden's whereabouts. Yet the Clinton administration was less clear about its willingness to use lethal force covertly than about its continued willingness to launch cruise missiles.

In the aftermath of the embassy bombings, the Clinton administration changed its posture regarding the use of Afghan tribals to capture bin Laden, first proposed in 1998. There was now consideration given to allowing the tribals to kill in at least *some* circumstances.[85] The issue that has proven controversial is pinning down what those circumstances were and whether they changed over the course of the next two years. It appears that from the aftermath of the East African embassy bombings until the end of his term, President Clinton issued at least four separate MONs relating to bin Laden and that these memoranda varied in significant ways with respect to the extent to which they authorized use of lethal force.

The first MON issued after the embassy bombings in August 1998 revived the capture operation using Afghan tribals, and even though the Administration at that time was preparing a cruise missile strike to kill bin Laden, the tribals were, nevertheless, directed to use deadly force solely in self-defense, and in fact were warned that they would not be paid if bin Laden were killed.[86] This standard was changed, however, in the next MON in December 1998. The new MON still did not explicitly give the Afghan tribals open-ended authorization to kill bin Laden. But though they were to prioritize bin Laden's capture, this second MON provided that they would be permitted to use "lethal force" not just in self-defense but also in the event that they determined that the attempted capture "seemed impossible to complete successfully" – which was a distinctly foreseeable, perhaps even highly likely, eventuality.[87] The December 1998 MON, in short, was close to a de facto authorization to kill bin Laden.

For at least a brief period, then, the CIA's efforts were brought closer into line with the aims of the overt military alternative. It was a moment of convergence; both the CIA and the military were seeking to kill bin Laden, even if the CIA approach differed from the military's in that the CIA held out hope for a live capture. Indeed, the underlying legal rationale likely was the same regardless of which instrument was being used: echoing General Counsel Sporkin's 1984 analysis, the Clinton administration's lawyers apparently had concluded that "under the law of armed conflict killing a person who posed an imminent threat to the United States would be an act of self-defense, not assassination."[88]

The moment of convergence did not last, however. The December 1998 MON was relatively closely held, which the 9/11 Commission

85. *See id*. at 131. *See also* BENJAMIN WITTES, LAW AND THE LONG WAR: THE FUTURE OF JUSTICE IN THE AGE OF TERROR 19-21 (2008).

86. *See* 9/11 COMM. REP. *supra* note 70, at 126-127, 131-132.

87. *Id.* at 131.

88. *Id.* at 132.

concluded contributed to the continued perception among many at the CIA that use of lethal force remained a taboo, justified only in cases of national self-defense.[89] Meanwhile, two additional MONs were issued over the course of the next year, and both retreated from the relatively flexible language of the December 1998 MON.[90] The first was designed primarily to extend the proxy force concept beyond the existing Afghan tribals to include Ahmed Shah Massoud's Northern Alliance forces.[91] The CIA proposed that Massoud's men be given authorization to use force under the same relatively flexible terms as provided in the December 1998 MON.[92] For reasons that are not clear, however, "[o]n this occasion . . . President Clinton crossed out the key language he had approved in December and inserted more ambiguous language."[93] And the second 1999 MON, which involved still another proxy force, went even further in constraining the lethal option, as it actually used the original capture language taken from the restrictive August 1998 MON, which predated the East African embassy attacks.

The December 1998 MON, of course, remained the controlling document for the original Afghan tribal proxy force. But the declining practical significance of that force, combined with the closely held status of its uniquely flexible grant of authority and the subsequent promulgation of a series of more restrictive MONs, left the impression among CIA officials that purposefully killing bin Laden was not truly part of the covert action alternative.

An incident involving a Northern Alliance attack on bin Laden in early 2000 underlines the gap between what the military was being asked to do overtly and what the CIA was permitted to do covertly through its proxies. The CIA had learned that bin Laden might be present at the Derunta training camp near Jalalabad and duly notified Massoud, whose men had established observation posts nearby.[94] But rather than merely confirm bin Laden's location or attempt a capture, Massoud took the initiative of dispatching a team armed with Katyusha rockets to bombard the camp. After Massoud reported this,

> CIA's lawyers convulsed in alarm. The White House legal authorities that provided guidance for the new liaison with Massoud had not authorized pure lethal operations against bin Laden.

89. *See id.* at 133.
90. *Id.* at 133.
91. *See id.*
92. *See id.*
93. *Id.*
94. *See* COLL, *supra* note 38, at 491-492.

> . . . The CIA was legally complicit in Massoud's operation, the lawyers feared, and the agency had no authority to be involved.[95]

The CIA directed Massoud to cancel the mission, but it was too late for him to recall the attack party.[96] "Langley's officers waited nervously" to see what would happen next.[97] "Some of them muttered sarcastically about the absurd intersections of American law and a secret war they were expected to manage."[98] In the end, weeks would pass without word as to what had happened before the CIA finally learned that the men claimed to have fired off their rockets without any discernible effect.[99]

The situation grew still more complex after the October 2000 bombing of the *USS Cole*. There was much discussion of launching a fresh round of overt military strikes against whatever al Qaeda-related targets could be found. But the intelligence linking al Qaeda to the *Cole* bombing was uncertain at best at that early stage, and President Clinton did not want to strike until al Qaeda's responsibility was established more clearly, notwithstanding the fact that al Qaeda already had been the authorized object for such attacks over the past two years.[100] And when the Bush administration took office in early 2001, it too was reluctant to launch missiles against al Qaeda-related targets in response to the *Cole* attack. For both administrations, this no doubt reflected at least in part the absence of substantial targets, above all bin Laden himself. Some Bush officials also emphasized, however, that "too much time had passed" and that the *Cole* bombing had become "stale."[101]

Yet even as the overt military option waned, the covert option for using lethal force unexpectedly waxed. By March 2001, the new Bush administration's NSC had directed the CIA to begin drafting new authorizations, including a MON that would entail "more open-ended language authorizing possible lethal action in a variety of situations."[102] A draft was in place by the end of that month, but things stalled at this point for two reasons.[103] One was that officials wished to embed the new authorities in the context of a broader regional policy review that was still underway.[104] The other was an ongoing debate about the way the expanded

95. *Id.*
96. *See id.* at 492-493.
97. *Id.* at 493.
98. *Id.*
99. *See id*
100. *See id.* at 193-195.
101. *Id.* at 202.
102. *Id.* at 210.
103. *See id.*
104. *See id.*

authority would relate to a new technology: armed unmanned aerial vehicles (UAVs), better known as "drones."[105]

The Air Force already had made the MQ-1 Predator available for use in Afghanistan for reconnaissance purposes, and its capacity to loiter in place while providing real-time video was a remarkable step forward in overcoming the intelligence gaps that had hampered the ability to project force within Afghanistan. To arm a Predator could have a game-changing impact, however, as this might collapse the time horizon for a missile strike from multiple hours to mere seconds once the decision to attack was made.[106] And by the spring of 2001 it was clear that this would soon be a viable option.

Operating armed Predators would remove the proxy element from the CIA's lethal operations, forcing attention to the functional convergence with the military that already was underway but which previously had been obscured by the intervening role of the proxies. Or so it seemed to the CIA Director George Tenet, at any rate. According to the 9/11 Commission report, Tenet clearly perceived this development in convergence terms:

> Tenet in particular questioned whether he, as Director of Central Intelligence, should operate an armed Predator. "This was new ground," he told us. Tenet ticked off key questions: What is the chain of command? Who takes the shot? Are America's leaders comfortable with the CIA doing this, going outside of normal military command and control? Charlie Allen [of the CIA] told [the Commission] that when these questions were discussed at the CIA, he and the Agency's executive director, A.B. "Buzzy" Krongard, had said that either one of them would be happy to pull the trigger, but Tenet was appalled, telling them that they had no authority to do it, nor did he.[107]

By August 2001, the NSC Deputies Committee had "concluded that it was legal for the CIA to kill Bin Ladin or one of his deputies with the Predator."[108] Questions remained as to when the armed Predator could be fielded and who would pay for it. But the path forward had been cleared of legal obstacles, and so the NSC again directed CIA to prepare new authorities including the use of lethal covert action.[109] It was the day before 9/11.

105. *See id.* at 211.

106. *Id.* at 421 (describing a four-hour window "from a presidential order to missile impact in Afghanistan").

107. 9/11 COMM. REP., *supra* note 70, at 211.

108. *Id.* at 212.

109. *See* COLL, *supra* note 38, at 212-214.

C. The CIA as a Combatant Command After 9/11

After 9/11, the U.S. government publicly asserted that a state of armed conflict existed between it and al Qaeda.[110] In the months that followed, the resulting kinetic action was concentrated in Afghanistan, where the bulk of al Qaeda's leadership and personnel happened to be and where the U.S. military acting through U.S. Central Command (CENTCOM) of course played the most visible role. But though CENTCOM remains deeply engaged in combat operations in Afghanistan to this day, the conflict is not (and from the beginning has not been) confined geographically to Afghanistan nor institutionally to CENTCOM. All along, there has been a "shadow" component to the conflict with al Qaeda, waged at times without formal acknowledgement by the U.S. government (though rarely without detection) in a variety of locations.

The CIA has played a central role in this shadow war, serving not only as a source of HUMINT and covert logistical support for the actions of the military but also as a warfighter – a veritable combatant command – in its own right.[111] This development marks a sharp break from the hemming and hawing over the propriety of the CIA's indirect involvement in the use of lethal force in the 1980s and 1990s and a substantial indicator of the post-9/11 convergence of military and intelligence operations.[112]

The change has been described as a "fundamental transformation" of the CIA as an institution.[113] The CIA's Counterterrorism Center (CTC), responsible for managing the CIA's kinetic operations, has grown immensely in terms of budget and personnel since 9/11, and today some twenty percent of the CIA's analysts function as "targeters," whose primary task is to identify or locate specific individual targets, who may then be attacked by a CIA-operated drone.[114] Some lament that the "CIA now functions as a military force" that lacks the accountability structures associated with the armed forces.[115] In the words of former Director Michael Hayden, "CIA has never looked more like its direct ancestor, the OSS, than it does right now."[116]

110. That determination has been the subject of considerable legal and policy controversy ever since. The merits of that debate are beyond the scope of this article.

111. *See, e.g.,* Miller & Tate, *supra* note 11.

112. *See id.* "One former senior U.S. intelligence official described the agency's paramilitary transformation as 'nothing short of a wonderment.' . . . 'You've taken an agency that was chugging along and turned it into one hell of a killing machine,' said the former official. . . ." *Id.*

113. *Id.*

114. *Id.*

115. *Id.* "'We're seeing the CIA turn into more of a paramilitary organization without the oversight and accountability that we traditionally expect of the military,' said Hina Shamsi, the director of the National Security Project of the American Civil Liberties Union." *Id.*

116. Siobhan Gorman, *9/11 A Decade After: Drones Evolve Into Weapon in Age of*

The transformation occurred quickly after 9/11. Tenet had presented what amounted to a CIA war plan to President Bush at a meeting at Camp David just four days after the attack. His proposal was sweeping, and included a request for "exceptional authorities" both to kill and to detain al Qaeda targets on a global basis. "It would give the CIA the broadest and most lethal authority in its history," Woodward wrote, "a secret global war on terror."[117] Significantly, Tenet requested that the authorization be broadly framed, providing programmatic approval rather than making it necessary to return to the President again and again to obtain specific authorizations for particular actions.[118] Bush agreed, reportedly signing an order on September 17th that formally modified Reagan's 1986 counterterrorism finding and superseded the interim modifications of the Clinton years discussed above.[119] Going forward, CIA was authorized "to *kill or capture* Qaeda militants around the globe," as paraphrased in media reports.[120]

In contrast to the uncertainties associated with the MONs issued between 1998 and 2000, after 9/11 the use of lethal force was unambiguous. "My last meeting with [the head of the CIA's Counterterrorism Center] before I left was interesting," said Gary Schroen, who spearheaded the initial CIA contingent to enter Afghanistan after 9/11.[121]

He basically said to me: "I want to make it clear what your real job is. All these other things – linking up with the Northern Alliance, preparing the battlefield, helping the special forces get in or whatever happens – is fine. But once the Taliban are broken, your job is to find bin Laden, kill him and bring his head back on ice."[122]

Terror – Intelligence Services Overcome Philosophical, Legal Misgivings Over Targeted Killings, WALL ST. J., Sept. 8, 2011, at A6.

117. BOB WOODWARD, BUSH AT WAR 76, 78 (2004).

118. *See id*. at 76.

119. *See id*. at 101.

120. Eric Schmitt & Mark Mazzetti, *Secret Order Lets U.S. Raid al Qaeda in Many Countries*, N.Y. TIMES, Nov. 10, 2008, at A1 (emphasis added). "A secret document known as a 'presidential finding' was signed by President George W. Bush that same month, granting the agency broad authority to use deadly force against bin Laden as well as other senior members of al-Qaeda and other terrorist groups." Joby Warrick, *CIA Assassin Program Was Nearing New Phase: Pannetta Pulled Plug After Training was Proposed*, WASH. POST, July 16, 2009, at A1; *see also* Joby Warrick & Ben Pershing, *CIA Had Program To Kill Al-Qaeda Leaders: Agency Didn't Tell Congress About Bush-Era Plan To Use Assassins*, WASH. POST, July 14, 2009, at A2.

121. Interview with Gary C. Schroen by PBS Frontline's The Dark Side, Jan. 20, 2006, *available at* http://www.pbs.org/wgbh/pages/frontline/darkside/interviews/schroen.html, [hereinafter Schroen].

122. *Id*. Schroen's colleague Gary Berntsen, who later took command of the CIA's paramilitary operations in Afghanistan, shared a similar story: "Gary Berntsen was working at the CIA's counterterroris[m] center in October 2001 when his boss summoned him to the front office and told him, 'Gary, I want you killing the enemy immediately.' Berntsen left

Notwithstanding the emphasis on lethal force, the looming war initially unfolded in a relatively conventional manner in terms of the CIA's role. CIA officers were the first Americans to enter Afghanistan after 9/11. The Agency had existing links to the Northern Alliance and had done extensive planning already with respect to a potential intervention on the Northern Alliance's behalf. The CIA was also far more nimble than the Pentagon, which had not planned for this situation and apparently had trouble agreeing on which component of the SOF community ought to take the lead initially.[123] But the immediate task for the CIA officers was distinctly in the nature of a support mission, involving efforts to leverage the capacities of Afghan allies and to prepare the way for the impending arrival of the military[124] (though CIA officers on an episodic basis did take a direct hand in the fighting, alongside U.S. military and Afghan forces, and the CIA did have armed Predator drones in theater).[125]

From this point of view, the broad authority in the September 17, 2001, order permitting the CIA to use lethal force against al Qaeda targets appeared more interesting on paper than in practice. Or at least that is how things looked from within Afghanistan. Beyond its borders, matters were different.

From the beginning of the war with al Qaeda, the CIA has acted under color of the September 17, 2001 finding in a wide variety of locations, covertly exercising three sets of powers that were identical to those contemporaneously being exercised overtly against the same enemy by the U.S. military: detention without criminal charge, the use of proxy forces to conduct lethal operations (in an extension of the model debated throughout

the next day for Afghanistan. . . . His primary target was bin Laden. . . ." *Tora Bora Revisited: How We Failed to Get Bin Laden and Why It Matters Today*: *Report to Members of the S. Foreign Relations Comm.* 111th Cong. 7 (2009), *available at* http://www.gpo.gov/fdsys/pkg/CPRT-111SPRT53709/html/CPRT-111SPRT53709.htm.

123. *See* Schroen, *supra* note 121. "I said: 'Reach out to these guys. Let's talk to the SEALs. Let's talk to Delta. Let's talk to SOCOM [Special Operations] Command. Let's talk to CENTCOM. Anybody you know, let's invite. We need to have a military officer, a special operations guy, come along with us.' Everybody that he talked to said: 'God, I want to go. I'd go myself, but we can't get the bosses to agree to even which special operations group is going to take the lead in this.' It just seemed like total confusion there, and so we packed up and got ready to go. . . . It took several weeks before that sorted itself out." *Id. See generally* GARY C. SCHROEN, FIRST IN: AN INSIDER'S ACCOUNT OF HOW THE CIA SPEARHEADED THE WAR ON TERROR IN AFGHANISTAN (2005) [hereinafter SCHROEN, FIRST IN].

124. Schroen, *supra* note 121.

125. On the episodic involvement of CIA officers in combat, see SCHROEN, FIRST IN *supra* note 123, at 253, 292. On the presence of CIA-operated drones in the Afghan theater, see WOODWARD, *supra* note 117, at 289. Note that it is unclear from Woodward's account whether or how often the CIA carried out drone strikes in Afghanistan, though it is clear that the strikes were used to collect intelligence in support of airstrikes carried out by the U.S. military. *See id.* at 211. Remarkably, the military was much slower to get Predators into the theater, and did not arm their Predators before sending them. *See id.*

the 1980s and 1990s), and the direct use of lethal force in the form of drone strikes.

Consider first the CIA's exercise of detention authority. At much the same time that the military was constructing a system for detention of "enemy combatants" (both within Afghanistan and at Guantanamo Bay), the CIA was constructing a parallel detention system at an array of undisclosed locations, a system that rested in an immediate sense upon the presidential finding described above but that ultimately relied upon the same law of war arguments that were used to justify the military's system.[126] Indeed, over time there appears to have been some traffic between those two systems. Detention is not the most vivid or lasting example of military-intelligence convergence, however. Many aspects of the CIA's post-9/11 detention practices remain secret, after all. In any event, President Obama ordered the termination of the CIA's detention program soon after taking office in January 2009.[127] (As of 2006, President Bush already had largely, if not entirely, ceased to rely on it.)[128] The CIA's involvement in the use of lethal force against al Qaeda, in contrast, has scaled upward dramatically in recent years.

As described above, the CIA's potential involvement in the use of lethal force against terrorists in the 1980s and 1990s seemed consistently to involve the use of a proxy force of indigenous allies, capable of acting with greater freedom of action in denied areas and entailing a degree of plausible deniability, perhaps, should their actions prove problematic. These advantages to the proxy force concept did not disappear after 9/11, no matter how free the CIA became (thanks to technological and other developments) to use deadly force in its own right. And thus it should not have come as a surprise when Bob Woodward asserted in 2010 that the CIA had evolved well beyond the counterterrorism action team concept of 1986,

126. For several years, the CIA detention program – involving at least some detainees captured and held outside of Afghanistan – was kept secret. But in November 2005, the *Washington Post* reporter Dana Priest exposed the existence of the "black sites" in a dramatic article. Dana Priest, *CIA Holds Terror Suspects in Secret Prisons: Debate Is Growing Within Agency About Legality and Morality of Overseas System Set Up After 9/11*, WASH. POST, Nov. 2, 2005, at A1. In 2006, in an address to the nation, President Bush ultimately acknowledged the existence of the CIA detention program and announced his decision to transfer the remaining detainees from CIA to military custody. *See* Dana Priest, *Officials Relieved Secret Is Shared*, WASH. POST, Sep. 7, 2006, at A17; Dafna Linzer & Glenn Kessler, *Decision To Move Detainees Resolved Two-Year Debate Among Bush Advisors*, WASH. POST, Sept. 8, 2006, at A1.

127. *See* Exec. Order No. 13,491, *Ensuring Lawful Interrogations*, 74 Fed. Reg. 4893 (Jan. 22, 2009) ("The CIA shall close as expeditiously as possible any detention facilities that it currently operates and shall not operate any such detention facilities in the future.").

128. *See* Priest, *Officials Relieved Secret Is Shared*, *supra* note 126 ("'Although there is no one in CIA custody today, it's our intent that the CIA detention program continue,' said a senior intelligence official. 'It's simply been too valuable in the war on terrorism to not allow it to move forward.'").

and had established a "3,000 man covert army in Afghanistan" consisting "mostly of Afghans, the cream of the crop in the CIA's opinion."[129] Called Counterterrorism Pursuit Teams (CTPT), according to Woodward, these forces "were a paid, trained and functioning tool of the CIA" that carried out "lethal and other operations" such as "kill[ing] or captur[ing] Taliban insurgents" or going into "tribal areas to pacify and win support."[130] In Woodward's account, the CTPTs amounted to a regiment-sized armed force operating under the ultimate command of the CIA Director, originally focused on combat and other operations in Afghanistan but later providing a rare capacity for projecting boots-on-the-ground force into Pakistan as well.[131]

All that said, the CIA's kinetic turn is best embodied by its creation of an extraordinary capacity to wage an air campaign using armed drones. The key development here was the timely maturation and proliferation of UAVs (first the MQ-1 Predator and then later the MQ-9 Reaper) equipped with increasingly reliable and discrete weapon systems (such as the AGM-114 Hellfire air-to-surface missile). This enables the CIA to project force in locations where it would be far more difficult, if not impossible, to carry out commando-style raids using either CIA officers or proxy forces. ArmedUAVs can be maintained and launched from more accessible areas, can loiter over potential targets for an extended period (thus providing better intelligence as well as the ability to tailor the precise moment of an attack in a manner that might reduce collateral damage), pose no risk to American or allied personnel (and thus no need to establish and maintain a combat search-and-rescue capacity), and may be perceived as less intrusive than ground troops from the perspective of host governments or populations (though that is not to say that they would not also cause sovereignty concerns). Drones may lack plausible deniability – particularly in contrast to the CTPTs[132] – but these other qualities over time have proven to be more than adequate compensation.

129. WOODWARD, *supra* note 117, at 8.

130. *Id.* at 8, 52; *see also id.* at 355 (asserting that the CTPTs were conducting "multiple raids every night around Kandahar"); Miller & Tate, *supra* note 11 ("[T]he purpose of the Counterterror Pursuit Teams is a source of disagreement among senior officials in government. 'They can fire in self-defense, but they don't go out to try and kill a target,' a U.S. official familiar with CIA operations in Afghanistan said. 'They're mostly arresting people and turning them over to' the Afghan security services. But the former senior U.S. military official said the teams' objectives were 'more kill-capture' than capture-kill. . . . In some cases, the pursuit teams used more indiscriminate means, including land mines, to disrupt insurgent networks, the former official said.").

131. *See* WOODWARD, *supra* note 117, at 367.

132. Miller & Tate, *supra* note 11 (noting, with reference to the CTPTs, that "[g]iven the scope of the CIA's paramilitary activities, human rights groups say the death toll over the past decade from CIA-directed operations undoubtedly exceeds the casualty count associated with strikes from drones. U.S. intelligence and congressional officials insist that the number of people killed in CIA operations outside the drone campaign is negligible, but say they

The first reported CIA drone strike occurred in November 2002, in Yemen. Al Qaeda had long had a substantial presence there, with its most notable operation being the attack on the *USS Cole* just two years earlier.[133] In this instance, the target was Qaed Salim Sinan al-Harethi (a.k.a. Abu Ali al-Harethi), the senior al Qaeda figure in Yemen and suspected mastermind of the attack on the *Cole.* Al-Harethi was traveling through a remote region of Yemen, packed into a vehicle with five colleagues including Kamal Derwish (a.k.a Ahmed Hijazi, an American citizen believed to have recruited the so-called Lackawanna Six to attend an al Qaeda training camp in 2001).[134] Unbeknownst to al-Harethi, he was entering a trap. A Predator drone circled overhead, transmitting a live feed both to CIA headquarters in Langley and to an operations center in the tiny east African nation of Djibouti, from which the Predator was controlled. Then-CIA Director George Tenet "gave a nod," the command was transmitted to the controllers in Djibouti, and the Predator fired.[135] All in the vehicle were killed.

This first drone strike made headline news, and U.S. officials were quick to offer legal justifications for the "covert" attack. It had taken place "with the approval and cooperation of Yemen's government," unnamed officials told reporters, and was appropriate both because al-Harethi and his colleagues were "'combatants' under international law" and the strike in any event could be viewed as an "act of self-defense . . . permitted under the international laws of war."[136] The unspoken premise, of course, was that the CIA was fighting war against al Qaeda with the military, relying on the same ultimate justifications for using lethal force. The CIA and the military found themselves targeting not only the same enemy using the same legal rationale, but also using the same weapons platform.

Nearly two years would pass before the CIA had the occasion to carry out another drone strike, at least insofar as we can tell from the public record. This might indicate that "assassination" concerns remained influential in the minds of the government's lawyers and policymakers. It might indicate a lack of access to the intelligence necessary to launch a similar strike, as the laborious process of developing a supporting network of on-the-ground HUMINT sources continued.[137] It might simply indicate

have never seen an agency-produced casualty count that includes other categories of operations").

133. For a review of al Qaeda's history in Yemen, see Robert Chesney, *supra* note 13, at 3.

134. *See* DINAH TEMPLE-RASTON, THE JIHAD NEXT DOOR: THE LACKAWANNA SIX AND ROUGH JUSTICE IN THE AGE OF TERROR 195 (2007).

135. *See id*. at 196.

136. *See* Dana Priest, *CIA Killed U.S. Citizen in Yemen in Missile Strike: Action's Legality, Effectiveness Questioned*, WASH. POST, Nov. 8, 2002, at A1.

137. On the necessity of strong HUMINT sources to inform drone operations, see WOODWARD, *supra* note 117, at 106-107 (describing critical role played by local informants

lack of access to armed UAVs in the right places and at the right times, or a lack of targets in locations where a drone strike would be deemed diplomatically or legally appropriate from the point of view of sovereignty concerns. Some or all of the above might be true. But whatever the case, the logjam began to break in the summer of 2004 with the killing of Nek Muhammad, a Pakistani extremist and former Taliban fighter who was in hiding in Pakistan's South Waziristan region.[138]

According to an analysis published by the New America Foundation, two more drone strikes in Pakistan's Federally Administered Tribal Areas (FATA) followed in 2005, with at least two more in 2006, four more in 2007, and four more in the first half of 2008.[139] The pattern was halting at best. Yet that soon changed. U.S. policy up to that point had been to obtain Pakistan's consent for strikes,[140] and toward that end to provide the Pakistani government with advance notification.[141] But intelligence suggested that on some occasions "the Pakistanis would delay planned strikes in order to warn al Qaeda and the Afghan Taliban, whose fighters would then disperse."[142] A former official explained that in this environment, it was rare to get permission and not have the target slip away: "If you had to ask for permission, you got one of three answers: either 'No,' or 'We're thinking about it,' or 'Oops, where did the target go?'"[143]

Declaring that he'd "had enough," Bush in the summer of 2008 "ordered stepped-up Predator drone strikes on al Qaeda leaders and specific camps," and specified that Pakistani officials going forward should receive only "'concurrent notification' . . . meaning they learned of a strike as it was underway or, just to be sure, a few minutes *after*."[144] Pakistani permission no longer was required.[145]

The results were dramatic. The CIA conducted dozens of strikes in

in supporting drone operations in Pakistan).

138. *See* David Rohde & Mohammed Khan, *Ex-Fighter for Taliban Dies in Strike in Pakistan*, N.Y. TIMES, June 19, 2004, at A6; *The Year of the Drone: An Analysis of U.S. Drone Strikes in Pakistan, 2004-2011,* NEWAMERICA.NET, http://counterterrorism.newamerica.net/drones#2011chart (attributing the attack on Nek Muhammad to a U.S.-operated drone) [hereinafter *U.S. Drone Strikes in Pakistan*].

139. *See U.S. Drone Strikes in Pakistan*, *supra* note 138.

140. JOBY WARRICK, THE TRIPLE AGENT : THE AL-QAEDA MOLE WHO INFILTRATED THE CIA 13 (2011); s*ee also* ERIC SCHMITT & THOM SHANKER, COUNTERSTRIKE: THE UNTOLD STORY OF AMERICA'S SECRET CAMPAIGN AGAINST AL QAEDA 118-119 (2011) (describing Director Hayden and DNI McConnell's efforts to persuade President Musharraf to permit an expanded U.S. combat presence in Pakistan, and Musharraf's agreement to permit CIA drones to strike targets beyond specifically-identified leaders).

141. *See* WOODWARD, *supra* note 117, at 4.

142. *See id.* at 4.

143. WARRICK, *supra* note 140, at 13.

144. WOODWARD, *supra* note 117, at 5 (emphasis in original).

145. WARRICK, *supra* note 140, at 13.

Pakistan over the remainder of 2008, vastly exceeding the number of strikes over the prior four years combined.[146] That pace continued in 2009, which eventually saw a total of 53 strikes.[147] And then in 2010, the rate more than doubled, with 188 attacks (followed by 56 more as of late August 2011).[148] The further acceleration in 2010 appears to stem at least in part from a meeting in October 2009 when President Obama granted a CIA request both for more drones and for permission to extend drone operations into areas of Pakistan's FATA that previously had been off limits or at least discouraged.[149]

Whatever the cause, the fact is that the CIA has directed the use of lethal force from armed drones in Pakistan more than 300 times over the past three years, or nearly once every three days. Thus it was no surprise to hear Director Panetta make such martial claims as his 2009 statement that the CIA is "the point of the spear" in the hunt for al Qaeda's top leadership.[150] Nor was it surprising, on this level at least, to find the director of the CIA's Counterterrorism Center (CTC) asserting that "[w]e are killing these sons of bitches faster than they can grow them now."[151] Such claims normally would be spoken by combatant commanders, if by anyone. But in light of the frontline role that the CIA and its CTC have come to play in the shadow war with al Qaeda, characterizing these officials as "combatant commanders" in their own right might not be too far off the mark.[152] With each additional sortie, the CIA's functional similarity to a conventional military conducting an air campaign has grown. Like a military commander, the CIA's Director now routinely decides whether to launch missiles to kill various targets, balancing the advantage to be gained with the risks (including the risk of collateral damage).[153]

146. *See id.* at 13.

147. *See U.S. Drone Strikes in Pakistan*, *supra* note 138.

148. *U.S. Drone Strikes in Pakistan*, *supra* note 138. The figure of 118 strikes in 2010 also appears in Miller & Tate, *supra* note 11.

149. *See* WOODWARD, *supra* note 120, at 208-209; WARRICK, *supra* note 140, at 91-92. It may also have mattered that Director Panetta in May 2010 urged the Chief of Staff of Pakistan's Army, Ashfaq Kayani, to consent to drone operations in a southern region of the FATA in which Pakistani armed forces were present. According to Woodward, Kayani replied that "he would see that they had some access." WOODWARD, *supra* note 117, at 366-367.

150. WARRICK, *supra* note 140, at 91.

151. *See* Miller & Tate, *supra* note 11. The quote was in response to a question from a fellow CIA officer inquiring about the pace of drone strikes in 2010. *See id*.

152. *See* SCHMITT & SHANKER, *supra* note 140, at 102-103 (describing the CIA Director as "America's combatant commander in the hottest covert war in the campaign against terror").

153. Warrick's account contains several vignettes in which former CIA Directors Michael Hayden and Leon Panetta exercise this authority. *See, e.g.,* WARRICK, *supra* note 140, at 15-16, 87-88.

To be fair, the CTC does far more than just drone strikes when it comes to counterterrorism, and its other operational activity is much less akin to military activity.[154] The drone program plainly has become a high-intensity operation, however, and is unlikely to abate much in the near term. Indeed, it is if anything likely to expand to other theaters, in some of which it will compliment or even replace existing military efforts.

Expansion to Yemen, in fact, has already begun. As noted above, the CIA did conduct a drone strike in Yemen in 2002. But in contrast to Pakistan, this attack did not mark the beginning of a sustained air campaign, let alone one commanded by the CIA. It was not until 2009, so far as the public record indicates, that the U.S. government began again to use lethal force in Yemen, and though it has done so on many occasions in the years that followed, it appears that these latest strikes were until recently carried out exclusively by the U.S. military (using a combination of manned aircraft, cruise missiles, and military-owned armed UAVs).[155]

This began to change in the summer of 2011. That August, *The Washington Post* reported that the CIA would soon resume drone strikes in Yemen as a supplement to the existing military air campaign,[156] supported by a new runway for drones at an unspecified location somewhere on the Arabian Peninsula. (This would reduce flight times, presumably, in comparison to launching from a military base across the Gulf of Aden in Djibouti, the approach in 2002.) Also in summer 2011, a new section within CTC was created focusing explicitly on the Yemen-Somalia theater (modeled on the existing Pakistan-Afghanistan Department, or PAD, which coordinates the air campaign in Pakistan).[157]

These plans bore their first fruit less than a month later, when a group of drones killed the American-born al Qaeda in the Arabian Peninsula (AQAP) member Anwar al-Awlaki while he traveled in a convoy in Yemen.[158] *The Washington Post* later reported that some of the drones involved included both CIA-controlled drones launched from the Agency's new facility in the Arabian Peninsula and others controlled by the military and launched from Djibouti – though all operated under "CIA authority" in this instance.[159] Quite accurately, Greg Miller described the operation as

154. *See* Miller & Tate, *supra* note 11 ("CIA officials insist that drone strikes are among the least common outcomes in its counterterrorism campaign. 'Of all the intelligence work on counterterrorism, only a sliver goes into Predator operations,' a senior U.S. official said. The agency's 118 strikes last year were outnumbered 'many times' by instances in which the agency provided tips to foreign partners or took nonlethal steps. 'There were investigations, arrests, debriefings . . . these are all operational acts,' the official said.").

155. *See* Chesney, *supra* note 13, at 31.

156. *See* Miller, *supra* note 11.

157. Miller & Tate, *supra* note 11.

158. *See, e.g.,* Greg Miller, *Joint Strike Is Latest Example of CIA-Military Convergence*, WASH. POST, Oct. 1, 2011, at A1.

159. *Id*.

"the latest, and perhaps most literal, illustration to date of the convergence between the CIA and the nation's elite military units in the counterterrorism fight."[160]

Expansion to other locations remains a distinct possibility. In recent years, the United States has repeatedly used deadly force in Somalia, in keeping with growing concern that Somalia's al-Shabaab movement is moving into the orbit of al Qaeda (or at least of al Qaeda's Yemeni operation, al Qaeda in the Arabian Peninsula). Based on the public record, these operations have been conducted by the military. But it is worth noting that the CTC's new Yemen-focused operation shares an orientation toward Somalia as well. Meanwhile, the prospect of an end to the overt American military presence in Afghanistan and Iraq highlights the possibility that CTC's drone strike portfolio might soon expand to those locations as well.[161]

None of which is to say that the traditional fear of CIA involvement in illegal (or at least unwise) "assassination" has entirely disappeared. On the contrary, that fear enjoyed a brief and incongruous resurgence in the summer of 2009. At the same time that drone strikes in Pakistan were increasing, the media reported that the CIA had for years been contemplating forming small teams to hunt down and kill al Qaeda leaders.[162]

Read in context with the developments already discussed in this section, it may be difficult to appreciate why this news was greeted with such surprise at the time. Here is what happened. A few months after he was sworn in as the CIA's Director in 2009, Panetta attended a briefing focused on new ideas in the hunt for Osama bin Laden.[163] Among other things, he was told of a program that would shortly become known to the public as an "assassination" plot, with all the negative legal and policy connotations that word entailed for the CIA.[164] Specifically, Panetta was

160. *Id*.

161. Michael Hirsh, *Slow Dance: Obama's Romance with the CIA*, THEATLANTIC.COM (May 2011), http://www.theatlantic.com/politics/archive/2011/05/slow-dance-obamas-romance-with-the-cia/238849/ ("As U.S. combat troops withdraw from Iraq and then, at least partially, from Afghanistan, senior CIA officials acknowledge that they will shoulder more of the war against the terrorists. The U.S. security presence in Iraq will center on clandestine action and surveillance overseen by the CIA. Afghanistan already has the agency's largest-ever presence in any one country, and when NATO evacuates in 2014, the agency will re-inherit a fight that it once owned. Even after U.S. forces depart, 'do not expect a significant drawdown in CIA resources in Afghanistan,' the senior administration official says. Currently, the CIA runs one drone program in Pakistan, and the U.S. military runs a separate one in Afghanistan; eventually, the agency will take up that burden as well.").

162. *See* Siobhan Gorman, *CIA Had Secret Al Qaeda Plan*, WALL ST. J., July 13, 2009, at A1, *available at* http://online.wsj.com/article/SB124736381913627661.html.

163. Warrick & Pershing, *supra* note 120.

164. Mark Mazzetti & Scott Shane, *C.I.A. Had Plan To Kill Qaeda Leaders*, N.Y.

told that the agency had "r[u]n a secret program for nearly eight years that aspired to kill top al-Qaeda leaders with specially trained assassins."[165] The program had been "active in fits and starts," having gone dormant in 2004 "because it was deemed ineffective" and then, after a brief revival in 2005, having been dormant again until 2009.[166] The program was resurfacing now, however, because of "new plans for moving forward with training for potential members of the assassination teams – activities that would have involved 'crossing international boundaries.'"[167]

In response, Director Panetta took two steps: He cancelled the program – which had proven over time to be infeasible or at least unduly difficult to operationalize, for reasons that are not clear from the public record – and he notified Congress for the first time about it.[168] It was soon headline news, and subject to withering criticism from many directions. Some objected to the cancellation of the program, pointing out that this was precisely what the CIA ought to be doing (and in various other ways, as we have seen, was in fact doing with other means). Others denounced the failure to notify Congress of the program earlier. Still others, however, denounced the idea of training "hit teams" to conduct "assassinations." Ultimately, nothing much came of it, as the program had in fact been cancelled. But the episode serves as a sharp reminder of the discomfort that many feel about the CIA's convergence-driven role as a veritable globe-spanning combatant command – and the possibility that this discomfort grows, the less military-like a particular use of force by the CIA appears to be.

Of course, there is an actual globe-spanning combatant command in the U.S. military proper: Special Operations Command (SOCOM), and its component the Joint Special Operations Command (JSOC). The parallels between the CIA's kinetic turn and the post-9/11 ascent of SOCOM and JSOC are striking. The next section takes up that ascent, teasing out the mirror-image elements of convergence it has entailed.

D. The Post-9/11 Evolution of JSOC

The SOF community has undergone an extraordinary transition over the past decade. Some aspects of the change have been highly visible. Events in Afghanistan in late 2001, for example, made clear that SOF played a critical role in the light-footprint combat model associated with Secretary Donald Rumsfeld, which aimed to leverage U.S. air power and indigenous

TIMES, July 14, 2009, at A1.

165. Warrick & Pershing, *supra* note 120.

166. Joby Warrick, *CIA Assassin Program Was Nearing New Phase*, WASH. POST, July 16, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/07/15/AR20 090715 03856.html.

167. *Id*.

168. Warrick & Pershing, *supra* note 120; Warrick, *supra* note 166.

ground forces so as to produce tactical and operational success without precipitating strategic failure through a large-scale, provocative, boots-on-the-ground U.S. presence.[169] Equally visible has been the role of SOF as a hunter-killer counterterrorism force in Afghanistan and Iraq in the phases following conventional combat operations. So too the DoD's decision in early 2003 to upgrade SOCOM from being a *supporting* command (providing personnel and material for operational control by regional combatant commands, such as CENTCOM) to being both a supporting and a *supported* command, one not limited to the concerns of a particular region and hence perhaps better suited to addressing trans-regional terrorist threats.[170]

In contrast, other aspects of SOF's evolution – particularly those most pertinent to the convergence trend – are less widely appreciated. Perhaps the most important development of this kind has to do with the Pentagon's decision to make JSOC the military's lead agency for counterterrorism, and the related issuance of a standing order authorizing an array of operations – including the use of lethal force – against terrorism targets outside of the "hot battlefields" of Afghanistan and Iraq.[171]

A word of caution: It is exceedingly difficult to examine JSOC's role in the conflict with al Qaeda based on the public record. It has maintained an extraordinary degree of secrecy over time with respect to both specific operations and larger institutional matters. In comparison with the CIA, it experiences far fewer leaks (whether of the semi-official or entirely unauthorized varieties), the prevalence of stories associated with the bin Laden raid being an understandable exception. But the publicly available information does suffice to demonstrate that the convergence between military and intelligence operations is not merely a matter of change within the CIA.

169. Whether the light-footprint model risks strategic failure instead by providing too little in the way of the capabilities needed to stabilize a society after conventional combat operations end is a different question, of course.

170. Secretary Rumsfeld explained at the time that "SOCOM will function as both a supported and a supporting command. The global nature of the war, the nature of the enemy and the need for fast, efficient operations in hunting down and rooting out terrorist networks have all contributed to the need for an expanded role for Special Operations forces. We are transforming that command to meet that need." MAJOR JAMES E. HAYES III, HONING THE DAGGER: THE FORMATION OF A STANDING JOINT SPECIAL OPERATIONS TASK FORCE HEADQUARTERS 1 (2006), *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA435896. *See also* Eric Schmitt & Thom Shanker, *Special Warriors Have Growing Ranks and Growing Pains in Taking Key Antiterror Role*, N.Y. TIMES, Aug. 2, 2004, at A8 ("'Since 9/11, we can no longer deal with this threat in pieces,' said a senior Defense Department official. 'You've got to have a global perspective, and that's what SOCOM is responsible for.'").

171. *See* Dana Priest & William M. Arkin, *Stealth Missions*, WASH. POST, Sept. 4, 2011, at A1 (describing a September 16, 2003, order from Secretary Rumsfeld); Schmitt & Mazzetti, *supra* note 120.

What exactly is JSOC? Bureaucratically, it is a sub-unified command under the aegis of SOCOM, meaning that it has independent authority to function and direct operations, rather like a combatant command in miniature. Substantively, it is a collection of numerous SOF special mission units, including Delta Force and SEAL Team Six, among others. Considering all of this, it is perhaps not surprising that it eventually was tasked with the lead role for the military in relation to counterterrorism.

Were this role to be performed solely in combat zones such as Afghanistan or Iraq, it would not necessarily be worth special attention in the context of a convergence discussion. What makes JSOC's role interesting for present purposes is that it is not confined to those locations.

Dana Priest and William Arkin of *The Washington Post* claim that in September 2003, JSOC was ordered to undertake a global campaign against al Qaeda, subject to a matrix specifying particular types of operations that could be conducted in various countries without need to go to the Secretary of Defense or even the President to obtain specific additional authorization.[172] Eric Schmitt and Mark Mazzetti of *The New York Times* had earlier described a similar order – known within the military, they said, as the "al Qaeda Network Exord" – that was issued in the spring of 2004.[173] The date discrepancy is irrelevant for present purposes. Both appear to be describing the same "execute order" (i.e., a military order to initiate operations), providing the rules of the road for JSOC to carry an array of operations against al Qaeda ranging from intelligence-gathering to killing.

It is not that the military could not act against al Qaeda or other targets outside of Afghanistan and Iraq prior to the al Qaeda Network Exord. But obtaining the requisite approval for the military to act in such circumstances may have been laborious and time consuming. The essential contribution of the al Qaeda Network Exord, it seems, was to streamline the authorization process as much as possible, tailoring it to the circumstances of specific anticipated locations of operations.[174] "Where in the past the Pentagon needed to get approval for missions [from the White House, presumably] on a case-by-case basis, which could take days when there were only hours to act, the new order specified a way for Pentagon planners to get the green light for a mission far more quickly. . . ."[175] In this way the Pentagon at last caught up, more or less, with the CIA, which, as noted above, had enjoyed broad authorization to conduct lethal operations against al Qaeda, even outside Afghanistan, since shortly after 9/11.

172. *See* Schmitt & Mazzetti, *supra* note 120.

173. *See id*.

174. *See* SCHMITT & SHANKER, *supra* note 140, at 34-35 (describing delays in obtaining specific authorizations to attack targets of opportunity prior to the al Qaeda Network Exord, and indicating that an interagency process managed via the NSC system ultimately produced the list of countries and conditions built into the "color-coded matrix" of pre-authorizations contained in the al Qaeda Network Exord).

175. Schmitt & Mazzetti, *supra* note 120.

According to Priest and Arkin, the al Qaeda Network Exord authorized operations in 15 countries.[176] The reins were loosest in Iraq and Afghanistan, not surprisingly. In those zones of active combat operations, JSOC had standing authority to employ lethal force against al Qaeda targets without need to seek permission from higher authorities in the chain of command.[177] The rules were more restrictive with respect to Somalia – a failed state with a friendly but largely powerless transitional government – where lethal operations require approval from the Secretary of Defense.[178] And if JSOC intended to use lethal force against an al Qaeda target in locations involving far greater geopolitical risks – such as Pakistan and Syria – approval had to come from the President himself.[179]

Schmitt and Mazzetti describe the al Qaeda Network Exord much the same as Priest and Arkin, except that Schmitt and Mazetti indicate the number of states encompassed as between fifteen and twenty (which, combined with the different date they give, suggests that Schmitt and Mazzetti might refer to a successor version of the original al Qaeda Network Exord).[180] Otherwise, the particulars are similar, except that Schmitt and Mazzetti's account suggests that Iran was left out of the al Qaeda Network Exord, whereas Priest and Arkin indicate that at least some kinds of operations were permitted in Iran under the version of the order with which they were familiar.[181]

There is an obvious functional convergence between the authority of the CIA and JSOC to use lethal force against al Qaeda targets in locations away from combat zones, even if the particulars of their respective permissions might vary to a degree from location to location.[182] Indeed, the degree of functional convergence is so apparent that the 9/11 Commission in its much-lauded report focused one of its recommendations on this very subject. "Lead responsibility for directing and executing paramilitary operations, whether clandestine or covert, should shift to the Defense Department," the Commission asserted, to be "consolidated with the capabilities . . . already being developed in the Special Operations

176. *See* Priest & Arkin, *supra* note 171.

177. *See id.*

178. *See id.*

179. *See id.* Other states listed in the order for approved operations against al Qaeda, according to Priest and Arkin, included Algeria, Iran, Malaysia, Mali, Nigeria, and the Philippines. *See id.*

180. Schmitt & Mazzetti, *supra* note 120.

181. *See id.* There may be no discrepancy, however, as the 2004 al Qaeda Network Exord might exclude Iran for kinetic or influence operations yet permit intelligence-gathering missions. Schmitt and Mazzetti do, after all, describe reconnaissance missions in Iran. *See id.*

182. *See id* (describing, for example, a decision by President Obama in 2010 to send "JSOC troops to Yemen to kill the leaders of [AQAP]").

Command."[183] Nothing ultimately came of these recommendations – during the 9/11 Commission Hearings the military's leadership was not enthusiastic,[184] and both the Pentagon and the CIA ultimately advised President Bush not to accept this suggestion[185] – but the very fact that it was made based on a perception of functional redundancy is instructive.

The military-intelligence convergence trend is not limited, however, to overlapping kinetic capacities beyond the hot battlefield. As described by Priest and Arkin, the al Qaeda Network Exord authorized JSOC to conduct not just lethal operations but also operations that looked like nothing so much as a traditional CIA covert action, including "psychological operations to confuse or trap al-Qaeda operatives."[186] Priest and Arkin also asserted that JSOC had taken on a host of other non-kinetic activities paralleling traditional CIA functions (whether under color of the Exord or not) "including tracing the flow of money from international banks to finance terrorist networks" and "send[ing] small teams in civilian clothes to U.S. embassies to help with what it calls media and messaging campaigns."[187] In addition, SOCOM since at least 2004 has had a budget for providing funds and other forms of support to foreign entities for use in counterterrorism and related operations, a form of aid that "has traditionally been handled by the CIA" in the eyes of some, though it might also be described as akin to SOF's traditional foreign internal defense (FID) mission.[188]

Intelligence collection is another point of convergence. Schmitt and Shanker contend that Donald Rumsfeld "was openly disdainful of the CIA's abilities" and therefore "set out to improve the Pentagon's own [HUMINT] network, including dispatching small intelligence teams abroad . . . sometimes . . . without the knowledge of the ambassadors and CIA station chiefs in various countries, causing turf battles."[189] Priest and Arkin assert

183. 9/11 COMM. REP., *supra* note 70, at 415.

184. When Commission member John Lehman raised the consolidation proposal at a hearing, both Secretary Rumsfeld and Deputy Secretary Wolfowitz suggested that their capacities were not entirely identical, but rather differed in light of the special expertise of particular personnel and also in light of what Wolfowitz referred to as "special authorities" that had been given to SOCOM. *See Day One Transcript, 9/11 Commission Hearings*, WASH. POST, Mar. 23, 2004, *available at* http://www.washingtonpost.com/wp-dyn/articles/A17798-2004Mar23.html. CJCS General Richard Myers added that "the teamwork is pretty darn good, actually." *Id*.

185. *See* JOHN J. LUMPKIN, PENTAGON, CIA OPPOSE TRANSFERRING PARAMILITARY OPERATIONS TO DEFENSE DEPARTMENT (2005) (noting DOD and CIA opposition to the 9/11 Commission's recommendation); *see also* Richard A. Best & Andrew Feickert, *Special Operations Forces (SOF) and CIA Paramilitary Operations: Issues for Congress* (Cong. Res. Service), Jan. 4, 2005 (discussing the 9/11 Commission's recommendation and noting arguments against following it).

186. Priest & Arkin, *supra* note 171.

187. *Id*.

188. LUMPKIN, *supra* note 185.

189. SCHMITT & SHANKER, *supra* note 140, at 259.

that JSOC has developed its "own intelligence division, its own drones and reconnaissance planes, even its own dedicated satellites."[190] These accounts call to mind the ISA experience of the 1980s, and in fact several sources suggest that some of these capacities may be delivered to JSOC by a unit that is a lineal or at least conceptual successor to ISA.[191]

More generally, the Pentagon has substantially expanded its HUMINT collection efforts in the post-9/11 period, raising questions about overlap with traditional CIA responsibilities and the need for deconfliction.[192] As late as 2010, that process continued to unfold. David Ignatius wrote in March 2010 that "the U.S. military has long been unhappy about the quality of CIA intelligence in Afghanistan," and that acting "[u]nder the heading of 'information operations' or 'force protection,'" the Pentagon has responded by "launch[ing] intelligence activities that, were they conducted by the CIA, might require a presidential finding and notification of Congress."[193] Ignatius adds, moreover, that the military has done this not simply by developing its own in-house capacities, but also by turning to private contractors for intelligence support services.[194] More specifically, it has turned in particular to a firm operated at the time by Dewey Clarridge, the legendary former CIA official referred to above as instrumental in founding the CTC and adopting a more aggressive CIA position in connection with counterterrorism in 1986.[195] The symbolism of convergence in that example is strong.

These developments have not gone unnoticed. As early as 2004, we find indications that they generated diverse reactions within the military itself. "[S]ome senior military officers are calling for transformation [of SOF] around the imperative for a new, secretive, and ethnically diverse intelligence cadre capable of tracking down [terrorists]," wrote Ann Scott Tyson in the *Christian Science Monitor*.[196] Tyson quoted Lieutenant General

190. Priest & Arkin, *supra* note 171.

191. *See* David Ignatius, *Get Ready for the American Ninjas*, WASH. POST, Feb. 25, 2003, at A23; Kibbe, *supra* note 7, at 110 (asserting that ISA, under the name Gray Fox, was "recently transferred from the intelligence command to SOCOM. It is the JSOC units and Grey Fox that are to play the key role in Rumsfeld's plans for 'hunter-killer' teams that will pursue 'high-value targets' (terrorists) around the world.").

192. *See, e.g.,* Walter Pincus, *CIA, Pentagon Seek To Avoid Overlap*, WASH. POST, July 4, 2005, at A2 (describing the proposed Memorandum of Understanding between CIA and DoD addressing, among other things, the substantial expansion of DoD's intelligence-collection efforts). Note too that Congress in 2004 appropriated funds to the Defense Department for the specific purpose of paying intelligence sources.

193. David Ignatius, *When the CIA's Intelligence-Gathering Isn't Enough*, WASH. POST, Mar. 18, 2010.

194. *See id.*

195. *See id.*

196. Ann Scott Tyson, *Boots on the Ground, Now Also the Eyes*, CHRISTIAN SCIENCE MONITOR, Mar. 11, 2004, http://www.csmonitor.com/2004/0311/p01s02-usmi.html.

Norton Schwartz, then Director of Operations for the Joint Chiefs of Staff, as calling for "operations-intelligence fusion . . . in direct support of counterterror."[197] She also noted, however, that such arguments were "stirring controversy over what some military analysts view as the potential pitfalls of blurring traditional lines between Special Operations and the CIA, especially in the realm of covert action."[198]

In the final analysis, the military's JSOC and the CIA's CTC appear to have developed parallel counterterrorism capacities spanning: the collection, analysis, and exploitation of intelligence; non-kinetic operations to influence events; and kinetic operations up to and including the use of lethal force outside of combat zones. This development has a range of legal implications, which I will examine in Part II. But the story of convergence still is not complete, for I have not yet acknowledged still another aspect of the CIA-military convergence, one that involves a rather literal element of convergence: the operational integration of CIA and military units in the field.

E. Joint CIA/JSOC operations and Cooperative Convergence

To this point, the convergence narrative to this point describes a substantial amount of institutional competition between the CIA and the military with respect to the conflict with al Qaeda and its allies. Each is maximizing its capabilities to locate, assess, and capture or kill such targets, often in the same locations. But if we focus solely on institutional competition, we would miss the crucial role that institutional *cooperation* simultaneously plays in the convergence process.

In many operational contexts, the CIA and the military in fact are highly cooperative. In pursuit of the same counterterrorism goals, they share information and personnel, and both construct and execute operations jointly – toggling between operating under CIA or military authorities as circumstances may dictate, as I discuss in Part II.B.[199]

Such cooperative convergence is, in part, a matter of co-locating or even assigning personnel from one entity to work under the direction of the other.[200] Joby Warrick's account of the CIA's facility at Khost in

197. *Id*.

198. *Id*.

199. *See, e.g.,* Azmat Khan, *JSOC Using Captured Militants to Analyze Intel*, PBS FRONTLINE (Sept. 6, 2011), http://www.pbs.org/wgbh/pages/frontline/ afghanistan-pakistan/jsoc-using-captured-militants-to-analyze-intel/ ("Much of what goes on here is a fusion operation. JSOC people [work] with CIA, and CIA people with JSOC. They have access to each other's system. They are by and large an integrated operation in the level of targeting and sharing of information about targets.").

200. *See, e.g.,* Priest & Arkin, *supra* note 171 (observing that JSOC brought in up to one hundred CIA operators to work out of JSOC's headquarters at Balad, Iraq, and sent some seventy-five officers to serve four-month rotations with various agencies in

Afghanistan illustrates this point,[201] as does the following passage in Greg Miller and Julie Tate's more recent account of CIA-military integration:

The comingling of the CIA and military at remote bases is so complete that U.S. officials, ranging from congressional staffers to high-ranking CIA officers, said that they often found it difficult to distinguish CIA from military personnel. "You couldn't tell the difference between CIA officers, Special Forces guys and contractors," said a senior U.S. official after a recent tour through Afghanistan. "They're all three blended together."[202]

Summarizing this state of affairs, a senior DoD official stated that "[w]e are in each other's systems, we speak each other's languages."[203] Nothing symbolizes this better than the fact that General David Petraeus (previously the military's commander in both Iraq and Afghanistan) has become the CIA's new director, while Leon Panetta (the former CIA director) has moved to the Pentagon to replace Robert Gates (himself a former CIA director) as the Secretary of Defense.

But convergence runs deeper than the blending of personnel, which might be written off as a mere matter of *secondment*, of little larger significance. The blending also is thoroughly operational.

Operational integration is not entirely a post-9/11 novelty. The "relationship between special-operations units and the C.I.A. dates back to the Vietnam War."[204] But whatever its history, the degree of operational integration today is remarkable. Post-9/11 operational coordination began as early as the opening weeks of the U.S. intervention in Afghanistan, as the CIA and special forces A-Teams collaborated to great effect in support of Northern Alliance ground operations and coalition air operations.[205] Operational coordination has not been limited to the combat zone setting, however. Describing JSOC operations outside of Afghanistan and Iraq, Schmitt and Mazzetti observe that "[s]ome of the military missions have been conducted in close coordination with the CIA," while "in others, like the Special Operations raid in Syria on Oct. 26 of [2008], the military commanders acted in support of CIA-directed operations."[206] Schmitt and Mazzetti also report that Defense Secretary Gates at some point issued an

Washington).

201. *See* Warrick, *supra* note 120.

202. Miller & Tate, *supra* note 11.

203. *Id*

204. Schmidle, *supra* note 4.

205. Schroen, *supra* note 121 (stating that "once they got on the ground, the relationship between CIA and those special forces A-teams was superb; it was seamless"); *see also* SCHMITT & SHANKER, *supra* note 140, at 259 (describing refinement of "tactical cooperation" between CIA and JSOC in Iraq).

206. Schmitt & Mazzetti, *supra* note 120. *See also* SCHMITT & SHANKER, *supra* note 140, at 259 (discussing "seamless operational cooperation . . . on a smaller scale in Yemen, Pakistan, and other shadowy battlegrounds").

order, distinct from the al Qaeda Network Exord, "that specifically directed the military to plan a series of operations, in cooperation with the CIA, on the Qaeda network and other militant groups linked to it in Pakistan."[207]

Miller and Tate add further detail, reporting that "[h]ybrid units called "omega" or "cross matrix" teams have operated in Afghanistan, Iraq, and Yemen."[208] These integrated CIA-military teams "wore civilian clothes and traveled in Toyota Hilux trucks rather than military vehicles. They were designed to develop sources and leads" but also to "be prepared if necessary to be the front end of a more robust lethal force."[209] On several occasions, they penetrated Pakistan in what Miller and Tate describe as a virtual test-run of the Abbottabad raid.[210]

Operational convergence even extends to the CIA drone program. According to Miller and Tate, the CIA's current structure for conducting drone strikes in Pakistan involves a fleet of thirty Predators and Reapers commanded by the CIA but flown – in the sense of hands-on-the-joystick – by *Air Force* personnel working from a *military* base in the United States.[211]

F. Cyberoperations

Though the narrative to this point has been wholly dominated by the aspects of convergence associated specifically with the CIA and JSOC, the convergence trend is in fact a broader phenomenon, and it is by no means limited to counterterrorism concerns. Any conversation about convergence and its legal consequences would be incomplete without at least touching upon its relationship to the emergence of cyberspace as a significant operational domain.

The first way in which cyberspace is especially prone to convergence has to do with the sheer difficulty of categorizing activity in cyberspace. Traditional categorical distinctions among intelligence collection, covert action, and military activity are hard to bring to bear on computer network operations, particularly if the question must be decided ex ante – i.e., before a particular line of code is put to use in a particular way. The code at issue may have simultaneous utility as a tool to collect intelligence and an instrument to influence events. And even under the latter heading, "influence" could mean something as innocuous as the generation of false information, or it could entail kinetic consequences on a scale similar to a conventional armed attack.

Cyberspace can also pose confounding difficulties with respect to the geography of the government's actions. Recall the discussion above of the

207. Schmitt & Mazzetti, *supra* note 120.
208. Miller & Tate, *supra* note 11.
209. *Id*
210. *See id.*
211. *Id.*

varying restrictions placed on JSOC under the al Qaeda Network Exord, depending on the state in which JSOC might be acting. Now imagine mapping a similarly nuanced set of constraints onto computer network operations, coupled with knowledge that a given operation might (but not certainly) have indeterminate collateral consequences on servers located in various locations around the world. One can readily imagine the obstacles this could produce to quick and decisive action.

Complicating matters further, there is substantial degree of physical, personnel, and institutional convergence between the leading military and Intelligence Community entities that actually engage in computer network operations. The military has long had various entities focused on cyberoperations. Today they are concentrated in U.S. Cyber Command (CYBERCOM), a sub-unified command of U.S. Strategic Command. The Intelligence Community, for its part, has long had perhaps the premier cyber capacities in the world in the hands of the NSA – which is a component of the DoD, but with a substantial civilian workforce and a capacity for operating under color of non-military authorities. CYBERCOM and NSA today are deeply intertwined, reflecting a sound instinct against attempting to duplicate NSA's truly unique (and no doubt extraordinarily expensive) capacities within CYBERCOM. Thus CYBERCOM and NSA are co-located at Fort Meade, they share some personnel (many of whom are trained in procedures meant to preserve a distinction between their actions as CYBERCOM personnel and their potentially-identical actions wearing their hats as NSA personnel), and both are (and must be) headed by the same official (currently General Keith Alexander).[212] Small wonder, in light of all this, that convergence has proven especially disruptive to the legal frameworks associated with computer network operations.

The convergence trend described above is no accidental occurrence. It is the product of numerous factors that have been driving convergence over the long term. Perhaps most notably, the notion of a sharp line between contexts of war and of peace – and thus between war-fighting and whatever one might call lesser forms of force – has proven increasingly untenable over time, and not just since 9/11.[213] Since at least the 1980s, if not earlier,

212. *See* Ellen Nakashima, *NSA Chief Faces Questions About New Cyber-Command: Alexander Set To Testify Before Senate Panel on His Stalled Nomination,* WASH. POST, Apr. 14, 2010, at A19.

213. The controversies associated with the Obama administration's position that the U.S. military intervention in 2011 did not constitute "war" as that term is defined in the Constitution or "hostilities" as defined in the War Powers Resolution nicely illustrates just how incoherent these distinctions have become in a world in which government uses of force spread across a broad spectrum rather than across binary, on-off categories. *See, e.g.,* Trevor Morrison, *Libya, 'Hostilities,' the Office of Legal Counsel, and the Process of Executive Branch Legal Interpretation*, 124 HARV. L. REV. F. 62 (2011).

terrorism and other unconventional threats have with increasing insistence demanded (or at least enabled) government responses that blur such distinctions, all the more so insofar as these responses take place in the shadows – i.e., secretly, or at least with deniability.[214] This strategic trend has led the U.S. government to (i) expand the manpower and resources of both the CIA and the military's SOF, (ii) adopt legal positions that facilitate assertions of the right to use lethal force against terrorist targets, and (iii) task both the CIA and the military with missions involving the use of force in contexts requiring secrecy and even deniability (particularly where the mission will be executed in the territory of a state that is unwilling to consent to U.S. forces operating on its territory, or at least unwilling to acknowledge such consent in public). This in turn has resulted in institutional competition as well as cooperation between the CIA and the military.

Technological trends also help drive convergence. The maturation and proliferation of UAVs is a case in point. Of course, it is not just a matter of technological progress, but also budgetary opportunities made possible by changing strategic priorities associated with terrorism. But however they arrived, UAVs not only have simultaneous utility as weapons and collection platforms (and in that sense physically embody the convergence trend) but, critically, do not necessarily require military personnel to operate; the CIA can use them too. As a result, they have greatly expanded the capacity of not just the military but also the CIA to engage in collection and kinetic operations in denied or partially denied areas.[215] It is, in a sense, an accident of history that the CIA was in a position to exploit this first, thus establishing a certain path dependency that helped explain why the CIA continued to grow a drone fleet; had the CIA not been engaged in the long-term pursuit of bin Laden in Afghanistan prior to 9/11, it would have been more difficult perhaps to envision the move to establish what amounts to a robotic CIA Air Force. Then again, it may be that the domestic and

214. Kenneth Anderson has convincingly argued that it is time to recognize a distinction between truly "covert" activity and merely "deniable" activity, that rigid insistence on playing dumb about transparent activity such as the CIA drone program ultimately reduces legitimacy. *See, e.g.,* Kenneth Anderson, *Petraeus and the Culture of the CIA*, OPINIO JURIS (Aug. 26, 2011), http://opiniojuris. org/2011/08/26/petraeus-and-the-culture-of-the-cia/. It may be that solving that particular puzzle would require legislative clarification that the CIA is in fact permitted to engage in covert action-style operations even when the operation will not in fact be denied once detected. I have been told by a number of sources that the existence of such authority – referred to as the "third way" – has been the subject of intense disagreement within the government, notwithstanding that the language of the so-called "Fifth Function" in the National Security Act does not appear to require that an operation be covert in order to come within the CIA's competencies.

215. *See generally* Kenneth Anderson, *Targeted Killing and Drone Warfare: How We Came to Debate Whether There Is a 'Legal Geography of War, in* FUTURE CHALLENGES IN NATIONAL SECURITY AND LAW (Peter Berkowitz ed., 2011), *available at* http://media.hoover. org/sites/default/files/documents/FutureChallenges_Anderson.pdf.

diplomatic sensitivities of states like Pakistan might have driven the CIA into the drone business, at least so long as the military was unable or unwilling to carry out identical operations on an unacknowledged basis.

Is there in fact some legal account that might explain why the CIA can operate drones in some locations while JSOC may not? That is a pressing question, and a good segue to an examination of the legal consequences of convergence.

II. THE LEGAL CONSEQUENCES OF CONVERGENCE

The convergence trend has a disruptive impact on the complex legal architecture that governs U.S. intelligence and military activities, but that impact is not well-understood outside of the government itself. My aim in this Part is first to give a deep account of that architecture, to describe the problems convergence generates for it, and to make modest recommendations meant to retailor the architecture to account for (rather than resist) the convergence trend.

I am specifically concerned with the domestic law rules relating to the military and intelligence activities of the U.S. government. These can be grouped into three categories.

One category concerns the internal executive branch decisionmaking process. Specifically, there are rules mandating that certain decisions be made only by the President or at least a cabinet-level official, thus ensuring a degree of democratic accountability (and, theoretically, encouraging caution) before certain actions are taken. For the sake of convenience, I will call these "process rules."

A second category of rules concerns information-sharing between the executive branch and Congress. Again, the effect is to supply a degree of democratic accountability, this time horizontally, and to encourage caution. I will refer to these as "information-sharing rules," which is unoriginal but perhaps usefully clear.

A third category of rules covers "substantive rules," concerning either affirmative authorization to carry out particular actions or specific constraints prohibiting certain actions. The rules that particularly interest me in this category are standing rules – meaning that authority has been provided or denied on a sustained basis, rather than ad hoc or temporarily.

Many elements of this framework have been the subject of extensive discussion and debate over the past decade. That is true, for example, with respect to the substantive constraints imposed on the United States (or at least arguably imposed) via the laws of war and by various federal statutes (such as the Torture Act, the War Crimes Act, the USA PATRIOT Act, the Military Commissions Act of 2006, and the Military Commissions Act of 2009). Here I assume the reader's familiarity with those issues, and focus instead on aspects of the legal architecture that are more specifically

impacted by the convergence trend: process rules relating to the decision to conduct covert action or to engage in certain military activities, information-sharing rules requiring notification to Congress of covert action and of deployment of the armed forces into hostilities, and substantive rules relating to whether and how particular government agencies might vary in terms of how they are externally constrained from acting or, conversely, how they might lack affirmative domestic law authority to act in the first instance.

A. The Domestic Legal Architecture of National Security

For most of its history, the United States has relied on a combination of thinly specified constitutional default rules regarding the decisionmaking process and case-by-case statutory or executive branch authorizations to act for certain ends and with certain means. We do not have a long tradition of a statutory framework purporting to impose standing rules of process, information-sharing, or substance. But this pattern changed in the latter half of the twentieth century, hand in hand with the emergence of a vastly bigger establishment of standing military and civilian institutions actively engaged with national security and foreign affairs. The edifice is still relatively sparse – and not always as effective as its proponents hope or its opponents fear – but for better or worse Congress and various Presidents since World War II have constructed a domestic legal architecture that speaks along all three dimensions.

1. Origins

For the first two centuries of U.S. history, the legal architecture governing America's overseas national security activities was quite limited. There was, of course, the Constitution's partial allocation of war and foreign affairs powers, which to a limited and contested extent speaks to the broad procedural question regarding the allocation of decisionmaking authority between the elected branches. And there has long been an overlay of international law considerations impacting, at least to some degree, the substantive discretion of the United States to act abroad in certain ways; both *jus ad bellum* and *jus in bello* norms, after all, can be thought of as substantive constraints impacting discretion to engage in certain national security activities, as can the subsequent emergence of the U.N. Charter system and international human rights law. But beyond these considerations, there was little else by way of standing rules for most of U.S. history. When Congress got involved, it generally did so on an episodic basis involving funding measures or the occasional declaration of war or authorization of force, rather than default framework rules.

There was little incentive for Congress to do more. It is true that, throughout this era, the United States engaged in both full-blown wars and

many low-intensity uses (or threats) of military force abroad, and no small amount of intelligence activity as well (including what we would today call covert action).[216] But the capacity to engage in such conduct was not deeply *institutionalized* in those years. There was no large-scale standing army, no sustained overseas deployment of our armed forces, and no stand-alone intelligence agencies tasked with covert action or collection responsibilities. And aside from a small number of relatively substantial armed conflicts, the quantity and strategic significance of low-intensity conflict and overseas intelligence-related activity was limited. As a result, there was little occasion for or interest in enacting framework legislation in that long era.

This state of affairs began to change in late nineteenth and early twentieth centuries as the United States began to assert itself as a powerful actor in international affairs. Yet for a time other factors continued to weigh in favor of the thinly specified status quo legal framework. Prior to the mid-twentieth century, mass communication technology was limited; trust in government with respect to national security and foreign affairs was relatively high; journalists were not oriented toward the exposure of secret government activities in the realms of foreign affairs or national security; and the civil liberties-human rights community of non-governmental organizations and related actors had not yet come into its own as an influential – and deeply skeptical – government watchdog network. These conditions collectively limited the information about national security activities that came to the public's attention as well as the concern such activities might generate once known, and together this sustained a climate in which Congress was unlikely to press for change.

All of these conditions flipped by the end of the twentieth century. By the early 1950s, the United States was a superpower. It possessed a massive military apparatus deployed across the globe. It was developing a growing array of intelligence agencies beyond the intelligence arms of the service branches, including the technology-oriented NSA within the newly organized DoD and the civilian, institutionally independent CIA (authorized by Congress to engage not only in collection and analysis of intelligence but also "such other functions and duties related to intelligence" as the might be directed, interpreted by the Truman administration and all its successors to include covert action). And underlying it all, the United States had adopted a grand strategy contemplating the sustained and extensive use of these instruments, and many others besides, to project power and influence abroad – both overtly and covertly – in hopes of containing communism while avoiding nuclear annihilation.[217] As a result,

216. *See* STEPHEN F. KNOTT, SECRET AND SANCTIONED: COVERT OPERATIONS AND THE AMERICAN PRESIDENCY (1996).

217. *See, e.g.,* NICHOLAS THOMPSON, THE HAWK AND THE DOVE: PAUL NITZE, GEORGE KENNAN, AND THE HISTORY OF THE COLD WAR (2009).

both the quantity and the potential strategic significance of overseas national security activities – and above all, the *risks* – had become far greater than had generally been the case in the past.

Meanwhile, the capacity of the government to control information relating to national security affairs – and the way in which the public perceived those affairs – changed rapidly during the 1960s and early 1970s. Technological change played a key role, as illustrated by the manner in which television brought foreign affairs – such as the Vietnam War – into American living rooms in an unprecedented manner.[218] So too did the broader sociocultural trend involving a decline in trust in the government – a decline reinforced by a steady stream of revelations about previously secret and decidedly controversial activities undertaken overseas for national security, not to mention the domestic fiasco of Watergate. In this climate, journalists became ever more inclined toward exposure of falsehood, mistakes, or illegality on the government's part, while non-governmental advocacy groups began to grow more effective as watchdogs – capable of marshaling indignation or litigation, or both – thanks to the other developments listed above, to which they too then contributed (for example, by acting as engines for exposing and highlighting government misconduct).

In retrospect, it was perhaps predictable that these developments would eventually produce legislative efforts to craft a standing set of rules attempting to constrain or regulate the overseas activities of the military and the Intelligence Community.

2. The Emergence of the Current Framework

The first step, arguably, in the construction of a framework of statutory default rules for military and intelligence activities occurred in 1947, when Congress through the National Security Act transformed President Harry Truman's Central Intelligence Group into the CIA, as we know it today. The National Security Act specified that the CIA was to perform a series of functions, most of which were predictable and relatively self-explanatory (such as collecting and analyzing intelligence). But the National Security Act also granted the CIA an authority that was decidedly less clear: "it shall be the duty of the Agency, under the direction of the National Security Council – . . . (5) to perform such other functions and duties as the National Security Council may from time to time direct."[219]

From the beginning, the executive branch has construed the generic terms of the "fifth function" to include authority to engage in covert action:

218. Consider also the impact of such prosaic technologies as the office photocopier, without which Daniel Ellsberg would have had a hard time exfiltrating a copy of the Pentagon Papers.

219. National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495, §102(d).

i.e., efforts to influence events overseas without the sponsoring role of the U.S. government being detected or acknowledged. In December 1947, citing the fifth function, for example, the Truman administration directed the CIA "to initiate and conduct . . . covert psychological operations designed to counteract Soviet and Soviet-inspired activities which constitute a threat to world peace and security,"[220] and the next year did the same in directing the CIA to establish an "Office of Special Projects . . . to plan and conduct covert operations" to respond to the "covert activities of the USSR, its satellite countries and Communist groups. . . ."[221] Subsequent administrations followed suit, tasking the CIA under the fifth function to engage in covert actions ranging from mild forms of information manipulation abroad to high-intensity paramilitary operations.[222] Eventually, a combination of sustained legislative acquiescence over time and subsequent legislation that expressly assumes that the CIA conducts covert action put to bed any debate as to this provision of the National Security Act.

Meanwhile, the second step in the construction of a statutory legal framework for military and intelligence activities came in 1973, when Congress passed (over President Richard Nixon's veto) the War Powers Resolution (WPR). This time the primary concern was military rather than intelligence activity, and the main thrust of the statute was not to empower the executive branch but to constrain it.

The WPR concerns the armed forces of the United States and their involvement (or potential involvement) in activities relating to hostilities or potential hostilities. In relevant part, the WPR imposes a pair of information-sharing requirements along with a rather complex decision-making rule that attempts to ensure Congress's voice in such deployments. As to information-sharing, the WPR through both its consultation and notification provisions obliges the executive branch to make Congress aware within a short time period when the armed forces are deployed into hostilities, circumstances in which hostilities are imminent, or circumstances involving deployments into foreign territory, waters, or airspace "while equipped for combat." As to the decision-making process itself, the WPR's "clock" mechanism attempts to force the executive branch to terminate such operations after sixty days if Congress does not provide affirmative authorization in the interim (though the president may invoke a thirty-day extension to facilitate withdrawal).

220. Memorandum from Exec. Sec'y Sidney W. Souers to the Members of the Nat'l Sec. Council, Enclosure 5 (Directive to Dir. of Cent. Intelligence Roscoe H. Hillenkoetter) (Dec. 9, 1947).

221. National Security Council Directive on Office of Special Projects, NSC 10/2 (June 18, 1948), *available at* http://www.state.gov/www/about_state/history/intel/290_300.html

222. *See, e.g.,* National Security Council Directive, Document 250 NSC 5412, *available at* http://history.state.gov/historicaldocuments/frus1950-55Intel/d250.

What the WPR does *not* do is impose any form of constraint – substantive, procedural, or informational – on military activity that does not implicate the WPR hostilities triggers, nor any constraints of any sort with respect to the overseas activities of any non-military personnel. And thus the WPR had nothing to say about CIA activity abroad, however war-like that activity might be,[223] nor about at least some forms of low-intensity military activity.

In short order, however, Congress took steps to extend certain aspects of the emerging statutory framework to the realm of CIA covert action. The tipping point came in the fall of 1974, when Congressman Michael Harrington revealed to the media that the Nixon administration had directed the CIA to spend millions in an effort to prevent Salvador Allende from winning a presidential election in Chile.[224] The story broke just a month after President Nixon's resignation over Watergate – a fiasco in which a domestic form of covert action had played an important role – and in the aftermath of great controversy and debate just a few years earlier about the role of covert action in war in Southeast Asia. In this tinderbox, Harrington's revelation "provoked a firestorm of criticism," prompting calls for legislation that might prohibit the use of covert action altogether[225] or at least require information-sharing with Congress.[226] Ultimately, using its power of the purse, Congress not only adopted an information-sharing rule, but also imposed a decisionmaking rule of process.

The thrust of this pathbreaking legislation – known as the "Hughes-Ryan Amendment" – was that no funds could be spent by or on behalf of the CIA to conduct covert action unless certain procedural and information-sharing conditions were satisfied.[227] In that respect the law was quite like the WPR, albeit much simpler. First, the statute forbade the CIA from engaging in covert action without a written "finding" from the President stating that the action was "important to national security." This was not a

223. Congress considered but did not pass Senator Thomas F. Eagleton's proposal that the WPR also encompass scenarios involving paramilitary entities "employed by, under contract to, or under the direction of" the United States. *See, e.g.,* W. MICHAEL REISMAN & JAMES E. BAKER, REGULATING COVERT ACTION: PRACTICES, CONTEXTS, AND POLICIES OF COVERT COERCION ABROAD IN INTERNATIONAL AND AMERICAN LAW 121 n.43 (1992).

224. *See* L. BRITT SNIDER, THE AGENCY AND THE HILL: CIA'S RELATIONSHIP WITH CONGRESS, 1946-2004, at 271-273 (2008); s*ee also* Seymour M. Hersh, *CIA Chief Tells House of $8 Million Campaign Against Allende in '70-73*, N.Y. TIMES Sept. 8, 1974, at A1.

225. SNIDER, *supra* note 224, at 273.

226. David Binder, *Watchdog Panel Proposed,* N.Y. TIMES, Sept. 20, 1974, at A11.

227. The Hughes-Ryan Amendment altered §662 of the Foreign Assistance Act of 1961, which appears as amended at 22 U.S.C. §2422. Interestingly, the legislation did not define covert action; in fact, it did not use that phrase at all. Instead, it referred vaguely to CIA "operations in foreign countries, other than activities intended solely for obtaining necessary intelligence." This excluded collection and left covert action, and perhaps much else besides; it was not a model of statutory clarity, and though its main purpose was clear to everyone concerned, the fact remained that this "definition" created room for substantial debates as to just what would now be subject to the new constraints.

true *substantive* constraint, of course; no genuine proposal for covert action would fail to pass such a vague standard. The real impact of the finding requirement, instead, was its *procedural* aspect, in that obliging the President to take this step eliminated the possibility of denying knowledge in the event of failure – thus harnessing presidential self-interest more directly to the task of ensuring against unduly risky or ill-conceived covert action projects (which is not to suggest that such proposals typically emanated from the CIA itself).

Second, the Hughes-Ryan Amendment also included an information-sharing measure requiring that certain congressional committees receive "timely notice" of activities for which a finding was required. This was not an authority to formally approve or disapprove covert action proposals, yet the information-sharing obligation nonetheless would have some checking effect. It would provide still further reason for the executive branch to self-police, and it would put at least some members of Congress in a position to take action should they take a dim view of the activity about which they received notice. Such action might include simply the solicitation of more information, but it also might extend to formal or informal efforts to stop the covert action in question.

This information-sharing activity could not be done *easily,* of course, but it could be accomplished, with sufficient motivation, through measures including use of the power of the purse to terminate the action, undermining the action through a leak of information to the press (or outright disclosure on the public record in Congress) in hopes of bringing political pressure to bear against the program in question. Both options were more likely to succeed with respect to a mere covert action as compared to an overt armed conflict; one of the curious facts about covert action is that the secrecy associated with it both makes it easier to initiate and easier to terminate, relative to the political consequences of either authorizing or terminating overt hostilities involving the military. This perhaps helps us understand why the WPR included a clock mechanism while Hughes-Ryan did not.[228]

The Hughes-Ryan Amendment had quick impact. Some of that impact was apparent to the public, as when notification to Congress of a covert action program in Angola led to legislation cutting all funding for the operation. But behind closed doors, there were issues with the implementation of the new information-sharing requirement.

One problem that arose concerned the tricky question of how to define the set of actions that truly required notification under the law. The statute's plain language was rather sweeping, and seemed to encompass a large quantity of relatively minor, small-bore activities that as a practical matter simply could not be processed through the findings-and-notification

228. Notably, the information-sharing regime also undermined plausible deniability for Congress, decreasing its capacity to criticize a program only after its public revelation.

regime given limited presidential bandwidth. Ultimately, a solution was found in a creative interpretation of the presidential-finding requirement. The newly-established Senate Select Committee on Intelligence (SSCI) and House Permanent Select Committee on Intelligence (HPSCI) agreed with the executive branch to distinguish between relatively significant operations – defined as those "involving high-risk, large-resource commitments or the possibility of harm to the participants or embarrassment to the United States" – for which specific findings would indeed be required, and relatively insignificant operations for which it would suffice that there be a "'general,' omnibus finding" specifying various kinds of activities that would then be undertaken (without further individual findings) on a programmatic basis.[229] It was a sensible distinction to draw – even if the statute itself had not drawn it – and one that would seem to cut in the other direction, decades later after the convergence trend began to shift ever more significant operations out of the reach of Hughes-Ryan.

In the interim, the reputation of covert action in the eyes of the public – and hence its political vulnerability in Congress – declined further in the years following the Hughes-Ryan Amendment, thanks to media reports and legislative investigations conducted by the Church and Pike Committees, which combined to expose the most sordid aspects of the CIA's history of covert action. The general thrust of the Church Committee's assessment was that covert action often failed, and in any event tended to undermine rather than advance U.S. foreign policy objectives. This contributed to a climate of increasing skepticism regarding covert action, as did the committee's revelation of various unsavory – and unsuccessful – plots involving the use of lethal force against foreign leaders (thus giving rise to the idea, mentioned in Part I, of the "lessons of the 1970s" with respect to assassination). Ultimately, the Church Committee called for enhanced congressional oversight and other constraints beyond those imposed as recently as by the Hughes-Ryan Amendment,[230] such as a new substantive rule prohibiting the use of covert action to "subvert democratic governments or provide support for police or other internal security forces which engage in the systematic violation of human rights."[231]

No such legislation would be forthcoming, however, as Presidents Gerald R. Ford and Jimmy Carter moved via executive order to impose voluntary substantive and procedural constraints on covert action, thereby deflating momentum in Congress for more permanent (and potentially more drastic) intervention. The first such effort was Executive Order 11,905, issued by President Ford.

Executive Order 11,905 did not actually speak explicitly of covert action as such, but rather referred to "special activities" (other than

229. SNIDER, *supra* note 224, at 280.

230. *Id*. at 275-278.

231. S. REP. NO. 94-755, at 159-161, ¶2 (1977) (CHURCH COMMITTEE REPORT).

intelligence collection and production) in which the goal was to further official policies abroad without the role of the U.S. government being "apparent or publicly acknowledged."[232] But it was much the same thing. With respect to the covert action decisionmaking process, Executive Order 11,905 revised the internal executive branch screening system, making the Attorney General into an observational participant.[233] With respect to substance, Executive Order 11,905 expressly prohibited such activities as "political assassination" and "experimentation with drugs on human subjects" without informed consent.[234]

President Carter largely reaffirmed Ford's procedural and substantive rules when in 1978 he issued Executive Order 12,036, but he also added an expanded information-sharing regime vis-a-vis SSCI and HPSCI. Whereas Hughes-Ryan effectively concerned only covert action, Executive Order 12,036 called for the Intelligence Community to keep SSCI and HPSCI "currently informed concerning intelligence activities, including any significant anticipated intelligence activities. . . ."[235] This expanded the obligation of congressional notification beyond covert action to include collection activities – a requirement that would later become a statutory obligation as well.

The new substantive, procedural, and information-sharing constraints associated with Executive Orders 11,905 and 12,036 did much to blunt legislative momentum towards further statutory refinement of the emerging legal architecture governing covert action. Perhaps more significantly, though, the geostrategic climate in the meantime changed in a manner that disinclined Congress to push for further constraints. In the aftermath of the Iranian Revolution and the Soviet invasion of Afghanistan in 1979, national security concerns were waxing and the impetus for civil liberties-oriented reforms was waning. As a result, the sole additional framework statute to emerge from the legislative ferment of the 1970s – the Intelligence Oversight Act of 1980 – did little more on this front other than to entrench Executive Order 12,036's expanded information-sharing requirements.[236]

Against this backdrop, the Reagan administration in 1981 replaced Carter's Executive Order 12,036 with a new Executive Order 12,333 – an iconic designation, with the order known to government lawyers today as simply "twelve-triple-three." For present purposes, Executive Order

232. Exec. Order No. 11,905, *United States Foreign Intelligence Activities*, §2(c), 41 Fed. Reg. 7703 (Feb. 18, 1976).

233. *Id*. at §3(c).

234. *Id*. at §§5(d), (g).

235. Exec. Order No. 12,036, *United States Intelligence Activities,* §3-401, 43 Fed. Reg 3674 (Jan. 24, 1978). Carter did drop the word "political" from the phrase "political assassination." *Id*. at §2-305.

236. Intelligence Authorization Act for Fiscal Year 1981, Pub. L. No. 96-450, §407(b)(1), 94 Stat. 1975, 1981 (1980).

12,333 was most notable for requiring that *any* agency engaged in covert action comply with the Hughes-Ryan rules for presidential findings, though the statute itself only encompassed the CIA. At least for a time, this raised the question as to whether all unacknowledged military operations had to be supported by a presidential finding – a question which, as I discuss below, came to a head a few years later.

There things stood with respect to covert action when the Iran-Contra Affair emerged in the mid-1980s. Not surprisingly, that scandal revived interest in new legislative constraints on covert action, and by 1987, a multi-year debate was underway concerning whether and how to further constrain covert action. The main bone of contention in that debate was whether to set a forty-eight hour deadline for covert action findings to be reported to the oversight committees.[237] But from the convergence perspective, the more interesting part of the negotiation concerned the effort to more clearly define the set of government actions that would be considered as "covert action" in the first place – including the extent to which that should include unacknowledged military operations.

3. Defining Covert Action

Recall that the Hughes-Ryan Amendment did not define "covert action" as such, but instead simply attached the finding-and-notification obligations to all CIA activity undertaken for purposes other than intelligence collection. If applied literally, this would encompass – and render extraordinarily burdensome – a vast array of relatively minor yet frequent CIA activities such as counterintelligence activities and run-of-the-mill support to diplomats and other government officials.[238] Understandably, the executive branch for years had taken the view that such matters were not intended by Congress to be encompassed by the oversight regime, and SSCI and HPSCI appear to have agreed. As a result, a course of action emerged consistent with that understanding, and to some extent the Ford, Carter, and Reagan executive orders with their definitions of "special activities" can be understood as efforts to entrench that course. Predictably, perhaps, not everyone agreed at all times regarding the metes and bounds of this implied exception for routine, low-risk activity.[239] "The result," the SSCI later

237. For a sampling of that debate at an early stage, see UNITED STATES CONG. HOUSE PERMANENT SELECT COMM. ON INTELLIGENCE SUBCOMM. ON LEGISLATION, H.R. 3822, TO STRENGTHEN THE SYSTEM OF CONGRESSIONAL OVERSIGHT OF INTELLIGENCE ACTIVITIES OF THE UNITED STATES: HEARINGS BEFORE THE SUBCOMMITTEE ON LEGISLATION OF THE PERMANENT SELECT COMMITTEE ON INTELLIGENCE, HOUSE OF REPRESENTATIVES, ONE HUNDRETH CONGRESS SECOND SESSION, FEBRUARY 24 AND MARCH 10, 1988 (1988) [hereinafter H.R. 3822].

238. *Id*. at 10 (testimony of DCI Webster).

239. AUTHORIZING APPROPRIATIONS FOR FISCAL YEAR 1991 FOR THE INTELLIGENCE ACTIVITIES OF THE U.S. GOVERNMENT, THE INTELLIGENCE COMMUNITY STAFF, THE CENTRAL

wrote, "has been a sometimes confusing list of exceptions and case-by-case determinations that have left both the Executive and Legislative branches uncertain as to the outside parameters of covert action."[240]

Against this backdrop, and with the spur provided by the Iran-Contra Affair, Congress in late 1987 took up the challenge of defining covert action more precisely by statute.[241] Its initial attempt to accomplish this failed, as the proposed definition did nothing to address the underlying problem of over-inclusiveness described above.[242] And for two years Congress did not touch the issue. In 1990, however, Congress at last took up the task seriously.

This time, it appears, Congress aimed to address not one but two overbreadth concerns. As before, there was a concern about subjecting routine, low-risk activity to the finding-and-notification system. Now, however, there also was a concern about encompassing activities that might well be significant and even risky, but which nonetheless should be exempted from the finding-and-notification system because they were conducted by the U.S. *military*, on the theory that at least some military activity had not previously been and should not now become subject to SSCI and HPSCI oversight.[243]

The solution proposed by SSCI in its 1990 bill involved two steps. First, the bill defined covert action in broad terms, including any activity that satisfied three conditions: (1) it must be conducted by an element of the U.S. government; (2) it must be meant to "influence political, economic, or military conditions abroad;" and (3) the "role of the United States Government" in sponsoring the activity must not be intended "to be apparent or acknowledged publicly."[244] This was a broad definition, taking no account of which agency conducted the operation in question. But SSCI's proposal went on to pare it back considerably by enumerating a series of exemptions. And therein lies the complexity of the definition.

The 1990 bill stated that an otherwise qualifying activity would not be categorized as covert action after all – and hence would not trigger the finding-and-notification regime – if it fell into a list of categories including, most notably, intelligence collection, "traditional military activities," and

INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM, AND FOR OTHER PURPOSES, S. REP. NO. 101-358, at 50 (1990) (accompanying S. 2834).

240. *Id*.

241. H.R. 3822, *supra* note 237.

242. *Id*. at 9-11; s*ee also* PERMANENT SELECT COMMITTEE ON INTELLIGENCE, REPORT AND MINORITY VIEWS OF REPRESENTATIVES HYDE, LIVINGSTON, SHUSTER, COMBEST, BEREUTER, ROWLAND, AND DORNAN, H.R. REP. NO. 101-725, at 34 (1990).

243. S. REP. NO. 101-358 (1990), at 50 ("The new definition would generally reflect current practice . . .").

244. S. 2834, 100th Cong. §503 (1999) (proposing amendment to §503 of the National Security Act).

"routine support" to traditional military activities. Critically, however, SSCI did not propose to define these categories in the statutory text itself. Rather, the idea was to explain their intended meaning in the accompanying committee report. As a result, the definitional language of the original committee report, and the language in successive reports, became the focus of intense scrutiny and negotiations among legislators and the White House. Ultimately, the actual text of the 1990 bill became law without alteration from SSCI's original proposal, but the definitions contained in the underlying committee reports changed in important ways en route.

Some of the proposed exemptions were relatively clear, or at least generated little pushback from the George H. W. Bush administration.[245] The first proposed exemption, for example, encompassed "activities the *primary* purpose of which is to acquire intelligence."[246] The idea here, plainly, was to distinguish collection from covert action, and to keep the former from becoming subject to a presidential-finding requirement (though not to spare it from an obligation to keep SSCI and HPSCI currently informed of collection operations; recall that the 1980 act extended that information-sharing obligation to all "significant" collection activities). Of course, the Hughes-Ryan Amendment had excluded intelligence-collection activities from the presidential finding requirement. But note that it did so

245. The "administrative activities" exemption is relatively clear as SSCI explained it. S. 2834 §503. Exemptions for "traditional diplomatic ... activities" and "routine support" thereto also generated little controversy. According to the explanation offered in SSCI's report, "tradition" does little work here; it is the meaning of "diplomacy" that counts instead. In SSCI's account, "diplomacy" is at bottom a matter of passing messages and conducting negotiations, as distinct from other forms of international interaction such as an arms sale or a "financial transaction." *See* S. REP. NO. 101-358, at 53. Proposed exemptions for "counterintelligence activities" (CI) and "activities to improve or maintain the operational security of the United States Government programs" (OPSEC) posed more difficulty. In both cases, the activity would have to be "traditional" to qualify. SSCI's report first explained, unhelpfully, that "traditional" was to be "understood in the sense of being usual, accepted customary practice – practice that is acknowledged and understood to fall within accepted parameters." *Id.* at 52. But the report then went on to offer something a bit more useful. First, there need not be an "exact precedent" in order for an activity to count as "traditional" CI or OPSEC. Second, what mattered at bottom was instead that the action "hew to the *purpose* of" CI and OPSEC. *Id*. That is to say, if the operation pursues "purposes other than those that are described as [CI or OPSEC]," then it could not be deemed "traditional" and the exemption would not apply. *Id*. Underlining the point, the SSCI report added that an activity could not be considered "traditional" CI or OPSEC if it "could have a significant effect on the perceptions, policies or actions of [a] foreign power beyond the ordinary objectives of counterintelligence operations." *Id*. Thus the "tradition" test in practice turned out to be not so much a matter of historical comparisons, but rather a question of the purpose and the impact of the operation in question. All of which might have been helpful, except that it is unclear what result should control in circumstances involving a dual purpose: a simultaneous desire both to achieve CI or OPSEC goals and to influence events abroad in the manner of a covert action. Unfortunately, SSCI's explanation left that matter unaddressed in the CI-OPSEC setting, in contrast to how it confronted the question expressly with respect to the exemption for collection. *Id*. at 53.

246. S. 2834 §503 (emphasis added).

only insofar as "collection" was the *sole* purpose of the activity in question. In actual practice, neither the executive branch nor the oversight committees had held to that strict line. Instead they focused on whether collection was the *primary*, even if not sole, purpose of the activity.[247] One might question whether it is coherent in all cases to say that one purpose is primary when the government does something that enables it both to collect information and influence events – particularly in cyberspace. Coherently or not, however, SSCI now proposed to entrench the primary purpose test.

One exemption, in contrast, did generate significant disagreement, in the sense that it failed to address concerns that the broad definition of covert action raised. The issue was whether and to what extent the broad definition of covert action in the 1990 bill would encompass operations conducted by the armed forces. The bill appeared to address this subject by explicitly exempting "traditional military activities" (TMA) from the covert action definition, thus shielding TMA from the finding-and-notification regime. The text of the bill did not actually define TMA, however. One had to look to the committee report for the definition that SSCI had in mind. And upon close inspection, that definition proved to be quite narrow.

The report's discussion of TMA opened on a broad note. SSCI explained that it intended that TMA "encompass almost *every* use of uniformed military forces,"[248] including not only "actions taken in time of declared war or where hostilities with other countries are imminent or ongoing," but also low-intensity scenarios such as "military contingency operations to achieve limited military or political objectives" such as "operations to rescue U.S. hostages held captive in foreign countries, to accomplish other counterterrorist objectives (i.e. the extraterritorial apprehension of a known terrorist), or military actions in support of counternarcotics operations in other countries."[249] In short, the proposed TMA exemption to the covert action definition appeared at first blush to be a sweeping exemption turning solely on whether the action was performed by the military. But there was a catch. The report went on to make clear that SSCI assumed that U.S. government responsibility "would be apparent or acknowledged at the time of the military operation."[250] When that was not the case – i.e., when "military elements *not* identifiable to the United States [are] used to carry out an operation abroad without ever being acknowledged by the United States" – the operation could *not* constitute TMA.[251] Thus an *undetected* military operation could fall within the TMA category, but an *unacknowledged* one never would. On this view, the TMA

247. S. REP. NO. 101-358, at 52.

248. *Id*. at 54.

249. *Id.*

250. *Id*.

251. *Id*. (emphasis added).

exemption did no work, as the definition of covert action already excluded operations in which the U.S. role was intended to be acknowledged.

As we shall see, this was far from the end of the matter. The military and the White House would push back on this definition, seeking to broaden it so as to encompass at least some unacknowledged military activities. Before turning to the outcome of that negotiation, a word about the distinct exemption for "routine support" to TMA is in order.

The 1990 SSCI bill also proposed to exempt activity amounting to routine support for TMA. The accompanying report explained that "activities undertaken by U.S. agencies, including non-DoD agencies," may constitute routine support for TMA even though "they are not acknowledged publicly by the United States."[252] But what counted as routine support?

SSCI first made clear that the exemption could attach even if the support in question was provided for an operation that never actually occurred. Indeed, the report stated that routine support to TMA could involve support merely for the "planning . . . of a military operation" rather than just its "execution."[253] This introduced indeterminacy with respect to the scope of the "planning" concept. That was not the most open-textured element in the routine support exemption, however. The biggest question concerned the meaning of "routine."

The committee conceded that this "will inevitably involve a subjective element," but suggested that the analysis might be guided by reference to a series of examples.[254] The "routine" category would include various forms of logistical support that might be useful in placing personnel inside a denied area and enabling them to act without detection, including false documents, communications gear, safe houses, transportation, and information.[255] Attempts to provide such support in Tehran for Operation Eagle Claw come to mind as a paradigm of what SSCI likely had in mind here: unacknowledged efforts both by Intelligence Community and military personnel not just to gather information but also to facilitate travel within Tehran, in aid of an anticipated military operation. In contrast, support for TMA along the lines of recruiting or training foreign supporters, influencing foreign public opinion, or inducing foreign persons to take certain actions would all be considered *non*-routine.[256] The latter set of situations, the committee explained, simply posed more serious risks for the United States.[257]

252. *Id*.
253. *Id*.
254. *Id*.
255. *Id*. at 54-55.
256. *Id*. at 55.
257. *Id*.

The Pentagon objected to SSCI's proposal. "Senior Defense Department officials became concerned about the Senate Bill's broadly phrased definition language," fearing that it "might be interpreted as encompassing . . . certain types of rather sensitive traditional Defense Department activities which neither the Department, the rest of the Executive Branch nor Congress had previously considered covert action."[258] These activities apparently included "strategic deception operations, certain peacetime psychological operations, some advance support contingency operations, and certain elements of some counterintelligence operations."[259]

The Senate and House did not alter the text of the legislation itself, despite this opposition. When the Senate and House bills were reconciled in conference that fall, however, conferees sought to address the Pentagon's concerns by altering the definition of TMA in the new conference committee report.[260] They wrote in a new report that they did "not intend that the new definition . . . include any activity not heretofore understood to be a covert action" (nor did they mean to *exclude* anything previously understood to be *covered*).[261] Turning to the key dispute over unacknowledged military operations and the meaning of TMA, the conferees abandoned the narrow interpretation of TMA that SSCI had offered in its original report, and in its place offered a new standard focusing on the institutions and personnel involved. Specifically, they proposed that an unacknowledged operation could qualify as TMA so long as two conditions were met. First, the operation had to be conducted "by military personnel under the direction and control of a United States military commander."[262] Second, the operation had to be collateral to an overt U.S. military operation occurring either at the same time or at least immediately after.[263] The conferees added that a CIA-commanded operation obviously could not qualify as TMA on this understanding, though it could constitute "routine support to TMA" subject to the degree-of-risk test for "routine" described above in SSCI's original report.[264]

This did not entirely mollify the White House and the Pentagon. President George H. W. Bush vetoed the bill, and though his objections largely concerned distinct matters, his veto message did note his continuing concern that the effort to define covert action might expand the concept in a manner that interfered with "the historic missions of the armed forces." [265]

258. H.R. REP. NO. 101-725, at 34 (1990) (statement of minority views contained in a report accompanying the House version of the bill).

259. *Id*.

260. H.R. REP. NO. 101-928 (1989).

261. *Id*. at 27.

262. *Id*. at 28-29.

263. *See id*.

264. *Id*. at 29.

265. Memorandum of Disapproval for the Intelligence Authorization Act, Fiscal Year

By early 1991, however, the White House and Congress were back to the negotiating table. The looming Persian Gulf War (ground operations began in the midst of these negotiations, on February 23) made the Bush administration still more sensitive to ambiguities associated with the covert action definition, presumably by providing concrete examples of war-related activities that might or might not qualify as TMA or routine support to TMA.[266] The Pentagon was specifically concerned that various forms of "strategic deception," "psychological operations," and "advanced force" might not be exempted with sufficient clarity.[267] And thus an initial round of meetings involving senior White House officials and leaders from the oversight committees grappled with the question of how best to refine the TMA exemption so as to address these concerns. Those initial meetings were followed by a round of staff meetings to work out the details.[268] By April, HPSCI's leadership concluded that there was not likely to be an agreement, and therefore moved forward with a version of the bill that simply dropped the effort to define covert action. SSCI, meanwhile, held out for continued progress in the negotiations.[269]

The logjam was broken a few weeks later. The revived bill preserved the same text as earlier (i.e., the broad definition of covert action and the listing of exemptions), and it was accompanied by a report that for the most part carried forward the earlier conference report language explaining the intended meaning of each of the exemptions.[270] But there was new language in the report concerning the meaning of TMA, language that appeared at last to resolve the White House and Pentagon objections.

The earlier conference report had altered the TMA exemption so as to encompass some unacknowledged military activity, but only so long as the operation was conducted and commanded by military personnel and carried out contemporaneous with or at least *immediately preceding* an overt military operation. Now, the exemption was much expanded by modifying that strict temporal element (while retaining the requirement of military command-and-execution).[271] Under the revised understanding

1991 (Nov. 30, 1990), *available at* http://bushlibrary.tamu.edu/research/public_papers.php?id=2520&year=1990&month=11.

266. H.R. REP. NO. 102-37 (1991), at 48 (accompanying H.R. 1455) (statement of minority views, recapping negotiations with the White House). We cannot say with any precision what sorts of activities the military or other agencies undertook to facilitate Operation Desert Storm before it got underway, but one can imagine any number of kinetic and non-kinetic possibilities involving CIA and special operations personnel.

267. *Id*. at 48.

268. *Id*. at 48.

269. *Id*. at 48-49.

270. S. REP. NO. 102-85, at 42-48 (1991) (accompanying S. 1325).

271. SCI's report underlined that this was an exemption meant to extend solely to forces under military command: "Activities that are not under the direction and control of a military commander should not be considered" TMA. *Id*. at 46.

hammered out between SSCI and the White House, an unacknowledged operation would now qualify as TMA so long as it:

> 1) was commanded and executed by military personnel, and
>
> 2) took place in a context in which overt hostilities either were
>
> (a) ongoing, or
>
> (b) "anticipated (*meaning approval has been given by the National Command Authorities for [i] the activities and for [ii] operational planning for hostilities*)."[272]

This was a subtle bargain. On one hand, the temporal scope of the TMA exemption was *far* broader under this understanding thanks to the "operational planning" language, as I will explain below. On the other hand, that expanded scope came with a string attached, in the form of a new decisionmaking rule pursuant to which the President or Secretary of Defense would have to approve the operation in order for the operation to qualify as TMA under the "operational planning" prong and hence avoid triggering finding-and-notification requirements.

The key to understanding all of this is to appreciate just what it means for "operational planning" to be authorized. This is not demanding in any sort of temporal sense. Operational planning can and normally will begin far earlier than the eve of conflict or even the eve of a deployment in anticipation of combat. The military has developed a rather elaborate process for the production of operational plans, embodied in a decisionmaking system called the Joint Operation Planning Execution System (JOPES).[273] And while JOPES does anticipate crisis planning in which unexpected circumstances greatly or entirely collapse the period between the authorization of planning and the onset of hostilities, this is the exception rather than the rule. The rule, in contrast, is "contingency planning" (previously called "deliberate planning") in which an operational plan is developed for contingencies specified in advance in documents such as the Secretary of Defense's annual Contingency Planning Guidance. As

272. *Id*. at 46 (emphasis added).

273. *See* USER'S GUIDE FOR JOPES (1995), *available at* http://www.dtic.mil/doctrine/doctrine/other/jopes.pdf; CJCSM 3122.01, JOINT OPERATION PLANNING AND EXECUTION SYSTEM (JOPES), VOL. I (PLANNING POLICIES AND PROCEDURES) (2001), *available at* http://publicintelligence.info/CJCSM_3122.01_JOPES_Vol_1.pdf; CJCSM 3122.02, TPFDD DEVELOPMENT AND DEPLOYMENT EXECUTION; CJCSM 3122.03, JOINT OPERATION PLANNING AND EXECUTION SYSTEM (JOPES), VOL. II (PLANNING FORMATS AND GUIDANCE) (1999), *available at* http://info.publicintelligence.net/CJCSM_3122.02a_JOPES _Vol_2.pdf. The JOPES system has been, or soon will be, superseded by the APEX system. *See, e.g.,* JOINT ADVANCED WARFIGHTING SCHOOL, OPERATIONAL ART AND CAMPAIGNING PRIMER AY 09-10, at 2, http://www.jfsc.ndu.edu/schools_programs/jaws/Campaign_Planning_Primer_2010v-4.pdf. The shift does not alter the main point in the text, however.

explained in a joint publication, "a contingency is an anticipated situation that likely would involve military forces in response to natural and man-made disasters, terrorists, subversives, military operations by foreign powers, or other situations as directed by the President or SecDef."[274] Suffice to say that the nature of the process is to anticipate circumstances that, though potentially quite unlikely, might foreseeably result in an order from the President to use armed force. From this perspective, the "operational planning" standard included in SSCI's explanation is not nearly as restrictive, in the temporal sense, as the casual reader might assume.

But the executive branch did not get this expansion of the TMA concept without giving Congress something in exchange. The language in SSCI's report quoted above refers not just to the National Command Authority having authorized operational planning for hostilities, but also having authorized the unacknowledged operation in question. An unacknowledged military operation covered by this part of the TMA exemption thus would not have to be reported to SSCI and HPSCI or supported by a covert action finding as such, but it would require either the President or the Secretary of Defense to approve the operation. This is a somewhat milder form of decisionmaking rule than the one imposed for covert action by the Hughes-Ryan Amendment – it does at least give the option for secretarial rather than presidential involvement – and it is not paired with an information-sharing rule requiring that authorization be shared with Congress. Yet it mandates a level of internal executive branch authorization that would preclude, for example, a decision by a combatant commander or anyone lower in the chain of command from engaging in an unacknowledged operation other than during times of overt hostilities (though it might yet qualify as "routine support" to TMA, depending upon the particulars).[275]

In any event, the House was quick to go along with this compromise by the Senate and White House. By mid-summer, a conference committee produced a bill that once again stated the proposed covert action definition and its exemptions, along with an accompanying conference report that closely tracked the Senate report just described.[276]

President Bush was not entirely mollified, it seems, but ultimately he was not willing to veto the bill on this basis. He argued that there was no need to define covert action in the first place, and implied that he would keep his own counsel when determining "whether particular military activities constitute covert actions," including "activities preparatory to the

274. JOINT PUBLICATION 5-0, JOINT OPERATIONAL PLANNING (2006), at xi (the Joint Operational Planning manual largely concerns a distinct but related planning system, but addresses JOPES concepts as well), *available at* http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.

275. S. REP. NO. 102-85, at 47.

276. H.R. CONF. REP. 102-166 (1991).

execution of operations."[277] But he nonetheless signed the bill in the end, making H.R. 1455, the Intelligence Authorization Act for Fiscal Year 1991, law of the land.[278] Its definition of covert action, and the aforementioned exemptions, now appear as 50 U.S.C. Section 413B(e).[279]

For the better part of two hundred years, the United States got by with relatively few standing rules regarding overseas national security activities involving military force or intelligence operations. By the end of the twentieth century, however, much had changed. Congress in fits and starts had established a complex set of decisionmaking and information-sharing rules, amounting to an architecture for national security activities. That architecture from the beginning has been shot through with gaps, and due to the convergence trend these gaps are growing in scale and significance. I turn now to a discussion of the specific impact of convergence along various dimensions of this architecture, beginning with the rules relating to executive branch decisionmaking procedures.

B. Executive Branch Decisionmaking Procedures

As described above, the current domestic legal architecture for national security activities imposes a presidential authorization obligation on activity constituting covert action, as well as a requirement of presidential or at least secretarial authorization for a subset of TMA (involving unacknowledged military operations carried out in connection with mere "operational planning" for hostilities). With these decisionmaking rules, Congress in theory harnessed White House self-interest more directly to the task of vetting proposals to undertake such actions. How well those rules serve that purpose today is increasingly unclear, however, as a result of the convergence trend.

1. Counterterrorism Actions

The problem stems in part from the interaction between definitions of covert action and TMA, on one hand, and uncertainties introduced by the

277. Presidential Statement on Signing the Intelligence Authorization Act, Fiscal Year 1991, 27 WEEKLY COMP. PRES. DOC. 1137 (Aug. 14, 1991).

278. Intelligence Authorization Act for Fiscal Year 1991, Pub. L. No. 102-88, 10 Stat. 429.

279. 50 U.S.C. §413B(e) (2006). One could argue for disregarding all of the preceding discussion on the ground that it simply was not included in the statute itself, and that TMA should instead be given its plain meaning without reference to the executive-legislative history. But TMA's meaning is hardly plain, whatever connotations "traditional" might have. And in any event, the question is unlikely to arise in a litigation context, but will instead arise continually in the context of executive branch and legislative decision-making and interactions in which both the aforementioned history and the subsequent course of practice building upon it will most likely be given priority.

adoption of an armed conflict model for counterterrorism, on the other. This interaction exposes the indeterminate aspects of the definitions, but it also very likely shifts a substantial amount of high-risk unacknowledged activity beyond the reach of the decisionmaking rules reviewed above.

Consider first the track of the TMA definition that exempts unacknowledged military operations conducted collateral to *overt* hostilities. We can say with confidence that this applies to at least *some* terrorism-related military operations. But it proves to be exceptionally difficult to draw boundaries around that set. The problems involve uncertainty as to (i) what counts as "hostilities" for purposes of TMA; (ii) who counts as the enemy at the organizational and individuals levels; (iii) what geographic boundaries, if any, cabin the hostilities; and (iv) what temporal boundaries cabin the concept.

First, there is a threshold question about the meaning of hostilities in the context of TMA. That word has been the object of fierce definitional debate over the past year as a result of the Obama administration's position that its military role in the Libyan civil war – including the use of armed drones carrying out periodic strikes, as well as the provision of various forms of logistical and intelligence support to the strike aircraft of other states – did not constitute participation in "hostilities" or deployment into a context in which "hostilities" were imminent for purposes of the WPR.[280] *If* the same standard were applied to "hostilities" as used in the executive-legislative history relevant to TMA, one can readily see how it would (ironically) serve to constrict the scope of TMA. But it is not obvious that the word should receive the same interpretation in both contexts. The Obama administration, after all, asserts its narrow understanding of hostilities in the WPR setting based on a claim about a long-standing executive branch view about its meaning in that specific context, as opposed to a claim about the meaning of hostilities more generally. Still, the comparison at least serves to draw attention to the essential indeterminacy of the word (as well as to foreshadow an apparent gap in the information-sharing rules of the legal architecture, as I discuss in more detail in Part II.C.).

Second, even if we had a firm grasp of what hostilities means in the TMA context, we must then grapple with the question of precisely who the enemy is. The position of the Obama administration is that the United States in at least some locations is engaged in armed conflict with al Qaeda, the Taliban, and associated forces.[281] That easy formulation masks

280. *See* Morrison, *supra* note 213. The Administration did issue a WPR notification to Congress at the outset of the operation, at a point when manned combat aircraft were involved. *See* Letter from the President to the Speaker of the House of Representatives and the President Pro Tempore of the Senate (Mar. 21, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/03/21/letter-president-regarding-commencement-operations-libya.

281. *See, e.g.,* Brief for Respondents, Hamlily v. Obama, 616 F. Supp. 2d 63 (D.D.C.

significant definitional problems, however. At the organizational level, it is unclear which precise set of groups are sufficiently associated with al Qaeda or the Afghan Taliban so as to come within the scope of this understanding (either on the theory that a group is part-and-parcel of al Qaeda itself, or that it is distinct yet still an enemy in the sense of being a co-belligerent entity).[282] And even if one had a clear sense of which entities count at the group level, a similar set of questions arises when it comes to defining the organizational boundaries of these groups at the individual level. These groups are not necessarily best viewed as hierarchical organization with fixed and objective distinctions between members and non-members.[283]

Third, questions also arise as to whether there are geographic boundaries to any hostilities that may be underway.[284] The past decade has seen protracted debate regarding whether "armed conflict" can be said to exist at all outside of Afghanistan and Iraq, given the relatively episodic nature of violent exchanges between the United States and al Qaeda in other locations. The same question arises, of course, with respect to the "hostilities" element of the TMA definition, though the answer need not be the same in both cases. Even if one can answer that question with precision, however, there is a further wrinkle. The TMA definition does not refer to any hostilities, but specifically to *overt* hostilities. It probably is common ground that there have been and continue to be overt hostilities in Afghanistan, for example, but where else in late 2011 is this true? The world is aware of the drone program in Pakistan, for example, but the U.S. government persistently refuses to acknowledge it officially – making it what Kenneth Anderson aptly describes as deniable-but-not-truly-covert.[285] Arguably, the same is true with respect to both CIA and JSOC operations in Yemen and Somalia as well. As a result, it is unclear both whether these should be considered examples of overt or covert hostilities, and, if the latter, whether this reinforces the view that only Afghanistan counts in geographic terms.

Fourth, the militarization of counterterrorism also exposes an element of temporal uncertainty in the TMA definition. Iraq illustrates the point. There is no doubt that overt hostilities were underway there at least for

2009) (No. 05-0763) (using this formulation to describe in a general way the scope of the government's detention authority under color of the laws of war).

282. *See* Robert Chesney, *Who May Be Held? Military Detention Through the Habeas Lens*, 52 B. C. L. REV. 769 (2011).

283. *See id*.

284. *See generally* Anderson, supra note 215.

285. *See* Kenneth Anderson, *Washington Post Stories on the CIA and JSOC – and My Prediction of Harold Koh's Legacy as Legal Adviser*, OPINIO JURIS (Sept. 3, 2011), http://opiniojuris.org/2011/09/03/washington-post-stories-on-the-cia-and-jsoc-and-my-prediction-of-harold-kohs-legacy-as-legal-adviser/.

some period beginning in March 2003. But is that still the case in late 2011? We lack metrics for stating with precision when hostilities start and stop for TMA purposes.[286]

Next, consider the second track of the TMA definition, which extends the exemption for unacknowledged military operations to actions that are not collateral to *current* overt hostilities, but that are related to overt hostilities for which operational planning has been authorized.

Whatever the boundaries of the first track of the TMA definition turn out to be, there is very little doubt that this second track manages to pick up a substantial amount of additional terrorism-related operational activity. It seems quite likely, after all, that a great deal of operational planning for overt operations against an array of transnational terrorist entities has been authorized. Recall that soon after 9/11, President Bush stated before Congress that "[o]ur war on terror begins with Al Qaeda" but "will not end until every terrorist group of global reach has been found, stopped and defeated."[287] Given this assertion, it would be surprising to learn that no operational planning for overt hostilities against some terrorist organizations beyond the scope of the AUMF ever was authorized.[288]

In fact, there is some evidence that a great deal of activity might be categorized by the Pentagon as TMA under this second track of the definition. In an unclassified section of a report issued in 2009, HPSCI observed that the military

> frequently labels [its clandestine activities] as "Operational Preparation of the Environment" (OPE) to distinguish particular operations as traditional military activities and not as intelligence functions. The Committee observes, though, that *overuse of the term has made the distinction all but meaningless. . . .* DOD has shown a propensity to apply the OPE label where the *slightest nexus of a theoretical, distant military operation might one day exist*.[289]

Assuming that this characterization is accurate, it suggests that the second track of the TMA definition has run riot under the loose label of OPE. Yet it is in the nature of the second track standard to make such expansion possible, insofar as it relies on nothing more than the "operational planning" test as a restricting device.

---

286. *Cf.* MARY DUDZIAK, WAR TIME: AN IDEA, ITS HISTORY, ITS CONSEQUENCES (forthcoming 2012).

287. President George W. Bush, Address to a Joint Session of Congress and the American People (Sept. 20, 2001).

288. *Cf.* SCHMITT & SHANKER, *supra* note 140, at 25-26 (describing debate within the Bush administration in late 2001 with respect to how broadly to define the enemy).

289. INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2010, H.R. REP. NO. 111-186 (2009) (accompanying H.R. 2701) (emphasis added).

Having said all that, it is not clear that the OPE "bubble" presents a major issue in terms of the decisionmaking rules, the focus of this section, as opposed to the information-sharing rules, discussed below. Recall that the second track of the TMA definition comes with a string attached: such operations must be authorized at the presidential or at least the secretarial level. This is a decisionmaking rule in its own right, of course, one that partially replicates the rule for covert action findings. The only question is whether one should be troubled by the fact that this rule permits secretarial approval to suffice.

It is certainly a lesser form of accountability. The Secretary of Defense has an institutional commitment to the military's interests, not those of other agencies or the government as a whole, and as a result might not have an incentive to police for, say, potential diplomatic risks associated with a proposed operation. The Secretary of Defense also is insulated to a greater degree from political accountability, being an appointed-and-confirmed rather than elected official. Yet requiring the Secretary's authorization is no small matter, and certainly much superior to leaving discretion to conduct unacknowledged operations entirely in the hands of combatant commanders or their subordinates.

The first track of the TMA definition, as noted above, does not provide even this much accountability. But before leaping to the assumption that lower level military commanders therefore may conduct unacknowledged operations at their discretion, it is worth recalling that statutes are not the only mechanisms for imposing decision-making rules. The military does have its own self-imposed constraints with respect to just this scenario, designed in no small part to address the same sorts of risks that motivated Congress to insist upon presidential accountability for covert action. Specifically, the Exords that govern military operations may specify an obligation to obtain approval from various officials – ranging from the President to the Secretary of Defense to combatant commanders – before certain operations may be conducted in certain locations. They can and sometimes do replicate the presidential accountability system required by Congress for covert action and for second-track TMA. It is just that they do not *have* to do this, and sometimes they do not do so.

Nothing illustrates this better than the series of post-9/11 Exords relating to the war on terrorism itself. The al Qaeda Network Exord appears to have created a system in which certain operations in certain states cannot be conducted without presidential approval or at least the approval of the Secretary of Defense. For operations that would qualify under the second track of the TMA definition, this might duplicate (or perhaps more accurately, operationalize) a statutory obligation. For operations that would qualify under the first track of the TMA definition, however, this becomes the only source for the decisionmaking rule. The questions then become whether the Exord is sufficiently strict on this

dimension and whether this approach ought to be codified rather than left to executive branch discretion.

According to Schmitt and Shanker, Secretary of Defense Robert Gates during his tenure had long been concerned by the prospect of kinetic operations undertaken without prior presidential approval (suggesting that the arrangement described above dated from the tenure of his predecessor Donald Rumsfeld).[290] They quote Gates as stating that:

> It has been my practice since I took this job that I would not allow any kind of lethal action by U.S. military forces without first informing the president or getting his approval. . . . I can't imagine an American president who would like to be surprised that his forces were carrying out an attack someplace around the world without him knowing about it. So I decided that we should change all of the ExOrds to make them conform in policy with my practice – that, in essence, before the use of military force, presidential approval would be sought.[291]

This apparently did not mean that commanders always had to reach back to the president before attacking in particular instances; that would cause problems in striking targets of opportunity.[292] Rather, "Gates created a system where options for potential types of missions were discussed with the president in advance so that he [as] commander in chief could delegate authority beforehand to strike specific fleeting targets."[293]

This was a wise arrangement, all the more so if the circumstances involved an unacknowledged operation. The risks to the United States are at their zenith when it comes to kinetic operations undertaken in locations where the United States is not already involved in overt hostilities. This is so without respect to whether and how one defines the geographic boundaries of whatever armed conflict with al Qaeda or its associates may be underway; the question is an entirely independent one having to do with the prospects of retaliation against the United States upon another state's discovery that U.S. military forces have conducted an operation involving the use of force on their territory.

Congress accordingly should entrench a version of the Gates decisionmaking rule in statute. At a minimum, it should require presidential authorization (or at least secretarial authorization) for the use of

290. *See* SCHMITT & SHANKER, *supra* note 140, at 246.

291. *Id.* at 246.

292. *See id.* at 246.

293. *Id.* at 246. That in turn highlights a further complicating element in this discussion: the question of broad versus specific authorizations, whether in the form of an Exord or a Finding or MON. The utility of requiring an authorization from a particular official arguably decreases in proportion to the breadth of the ex ante authorization that official might issue.

lethal force by *any* U.S. government-controlled entity, if the force will be used in the territory of a state where no overt hostilities involving U.S. armed forces already are underway. Congress might also consider a broader approach, requiring presidential (or at least secretarial) authorization for *all* unacknowledged operations occurring on the territory of a state where hostilities are underway or imminent, thus more perfectly matching responsibility to the magnitude of the consequences entailed by such operations. From the decisionmaking rule perspective, it would then no longer be necessary to parse through the definitional morass described above.

2. Computer Network Operations

Whether a presidential finding is required in connection with an unacknowledged operation is not simply a problem generated by the war on terrorism. It is a question that arises with special complexity in connection with computer network operations (CNOs). Whether a given CNO constitutes a covert action subject to the finding requirement is especially difficult to come to grips with, particularly given the literal convergence of personnel, equipment, and capabilities associated with the partial integration of NSA and CYBERCOM.

There are at least three issues under this heading, all suggesting that CNOs pose a particularly difficult challenge to the coherence of the categorical distinctions employed in the covert action definition.

First, it may be very difficult to determine whether a given CNO qualifies for the intelligence collection exemption to the covert action definition. Particularly from an ex ante perspective, a CNO might have equal potential for use as a platform for collection activities and for "influence" operations (up to and including those with significant physical effects). The Stuxnet worm provides a case study (though no state has yet acknowledged responsibility for that attack and hence one should not simply assume it was an American project). In that case, the code apparently was intended all along to make its way into specialized industrial-control software from Siemens known to be employed in an Iranian nuclear facility, and then to cause (and disguise) destructive physical consequences inside that facility. But it is not difficult at all to imagine that the worm with minor modifications could have been designed to afford its originator with merely the *option* of causing such an impact on demand, while in the meantime providing the originator with a flow of data regarding the facility's ordinary operations. Indeed, this may well have been a feature of the actual Stuxnet worm.

If that had been the case, and if it was an American operation, the analysis provided in Part II.A. suggests that in such scenarios categorization would turn on which purpose was "primary." Yet neither or both might be

primary at the same time. That scenario of course can arise with human agents as well, though it may well occur with greater frequency in the CNO setting.

Next, let us assume for the sake of argument that a given CNO is not best viewed as "primarily" a matter of collection, and hence does not qualify for that exemption. Two further questions then arise. Might the operation instead qualify as TMA? And if not, might it at least qualify as "routine support" thereto?

The question as to whether to classify CNO as TMA is difficult for several reasons. First, the fact that there has been a rather literal form of convergence between NSA and CYBERCOM might make the inquiry especially difficult. As a result of this institutional convergence, the same personnel might be trained for and authorized to conduct operations under color of both Title 10 and Title 50 authority as circumstances dictate. In that situation one could not simply identify the institutional affiliation of the personnel involved in order to inform the inquiry as to the nature of the action. Then again, it might also be the case that the procedural formalities adopted in order to facilitate this hat-switching capacity might themselves constitute a relatively objective marker as to the nature of the operation. In any event, it seems strange to allow such formalisms – rather than a functional assessment of the risks involved – to determine whether a given CNO will be subject to a presidential authorization requirement.

But let us assume that we are dealing with an operation commanded and executed by military personnel, such that it is at least possible for the operation to constitute TMA. The next issue, as we have seen, is whether the operation is collateral to ongoing overt hostilities under the first TMA track, or at least to anticipated overt hostilities for which operational planning has commenced under the second TMA track. The latter scenario in theory might sweep a vast array of unacknowledged cyber activities into the realm of TMA; one can readily imagine the arguments for treating just about any sort of activity relating to computer systems in China, for example, as a form of OPE in the event of some future conflict for which contingency planning has been authorized. But in that case the operation must be approved by the President or Secretary of Defense. The more interesting question, then, is how broad the TMA concept might be in cyberspace in connection with first TMA track, involving ongoing overt hostilities.

The question of conflict geography looms especially large. We have already noted the debate and uncertainty surrounding the question of whether there are geographic limitations to the war with al Qaeda such that ongoing overt hostilities should be said to exist for TMA purposes only in Afghanistan (and in Iraq as well). If we assume for the sake of argument that a strict approach should be taken to this issue, hard questions still arise with respect to the intersection of hostilities in Afghanistan and cyberspace.

This question appears to have generated a great deal of internal government debate over the past six years, and it is not clear from the public record how, if at all, the matter has been resolved. Complicating matters, it is quite clear that the issue is intertwined with – and probably greatly outweighed by – a policy dispute about the tradeoff between shutting down servers that facilitate insurgent or terrorist communications or allowing those servers to continue to operate in order to facilitate intelligence collection and other interests.[294] There also are significant policy concerns relating to the collateral consequences of shutting down such servers.[295] All that said, the legal question is an important one.

The issue is summarized aptly in an explanatory statement generated by the House Armed Services Committee in connection with the draft National Defense Authorization Act for Fiscal Year 2012:

The committee notes that al Qaeda, the Taliban, and associated forces are increasingly using the internet to exercise command and control as well as to spread technical information enabling attacks on U.S. and coalition forces in areas of ongoing hostilities. While these terrorist actions often lead to increased danger for U.S. and coalition forces in areas of ongoing hostilities, terrorists often rely on the global reach of the internet to communicate and plan from distributed sanctuaries throughout the world. As a result, military activities may not be confined to a physical battlefield, and the use of military cyber activities has become a critical part of the effort to protect U.S. and coalition forces and combat terrorism globally.[296]

The drafters of that language no doubt had in mind, among other things, the long-running concerns of CENTCOM commanders regarding use of the Internet by insurgents in Afghanistan and Iraq.[297] According to Schmitt and Shanker, CENTCOM was pressing as early as 2005 for action to "take down" four jihadist websites, but ran into opposition because the servers supporting those sites "were in Western Europe and Southeast Asia," with "huge amounts of digital data and communications flowing through legitimate servers in the United States" as well.[298]

This issue is intertwined with questions regarding substantive constraints on military and intelligence operations, and in particular with the question of whether there are geographic constraints that apply to one form of operation but not the other – questions I will discuss in Part II.E. Here the issue is simply whether one can fairly apply the TMA label to

294. *See* SCHMITT & SHANKER, *supra* note 140, at 132-151.

295. *See id.* at 132-151.

296. *See Summary of Bill Language*, in H.R. 1540 – FY12 NATIONAL DEFENSE AUTHORIZATION BILL CHAIRMAN'S MARK, at 16, *available at* http://armedservices.house.gov/index.cfm/ files/serve?File_id=61e9d0d1-581b-4204-ba0e-f601878bc710.

297. *See* SCHMITT & SHANKER, *supra* note 140, at 133-135.

298. *Id.* at 134.

operations involving a server located in, say, Europe, if that server is being used to facilitate communications among insurgents in Afghanistan and one has adopted a geographically strict understanding of where overt hostilities are occurring for TMA purposes.

There is no obviously correct answer to this question. On one hand, the scenario presupposes a relatively direct impact between the extraterritorial activity (i.e., the work performed by the server located in some third country) and the conduct of hostilities inside the combat zone. On the other hand, the scenario seems far removed from the paradigm of activities relating to overt hostilities insofar as it contemplates potentially significant impacts in third countries that would not expect such consequences given their physical remoteness from the combat zone. That last point supports the conclusion that there are unusual risks associated with this fact pattern, risks of the kind that support application of a decisionmaking rule requiring presidential or cabinet-level approval.

This may explain why the government reportedly has developed a relatively elaborate interagency screening process for this situation, with at least the prospect of presidential involvement in the final decision.[299] Given the novelty and evolving nature of CNOs, and the government's limited experience dealing with the issues they present, it may be that the wisest course of action in confronting the aforementioned difficulties is to leave the executive branch on its own with respect to decisionmaking. Solutions such as the interagency vetting system just mentioned might flourish or fail, and others might emerge in their place. Accordingly, it might be more important, for the short term at any rate, to focus on ensuring that Congress has some understanding of what the problems are and what the executive branch is doing about them. This brings us to our next topic.[300]

C. Sharing Information with Congress

There are several information-sharing rules that oblige the executive branch to inform Congress – or at least some subset of Congress – of military and intelligence activities. There are gaps among them, however, and those gaps are growing at least in part because of the convergence trend.

299. *See id.* at 145-146.

300. There is a further question as to whether CNOs might escape categorization as covert action on the ground that they constitute "routine support" to TMA. In some cases, CNOs no doubt can be reasonably easily analogized to the examples offered in the original SSCI explanatory statement. A Stuxnet-style attack that causes physical damage, for example, would surely not qualify. But just how to analogize to the examples of logistical support in the physical world is far less clear. If, for example, an operation were conducted to manipulate data in another state's computer systems in order to facilitate the surreptitious entry into or travel within that state by military personnel engaged in TMA, it is not at all obvious how that manipulation ought to be characterized.

One of these rules is the oversight requirement for activity constituting covert action. The executive branch must give notice of such activities to SSCI and HPSCI, or at least to the Gang of Eight leadership, consisting of the chair and ranking members of those committees and the majority and minority leaders of both Houses. If the activity is "intelligence collection," as opposed to covert action, notification to SSCI and HPSCI is required, and in this case, notification cannot be limited to the Gang of Eight.[301] Meanwhile, the WPR's consultation and notification requirements call for Congress as a whole to be notified should the armed services be deployed into hostilities or circumstances where hostilities are imminent.

The fundamental problem convergence presents for this framework is embodied by the OPE concept described above. When in 2009 HPSCI publicly complained about the overexpansive application of OPE, in fact, it was not primarily concerned with circumvention of the covert action system's requirement of presidential authorization.[302] Rather, it was concerned with its own prerogatives in terms of oversight over intelligence-collection activity. Specifically, HPSCI objected that the profligate invocation of the OPE label was being used to shield intelligence collection activity from being categorized as such, thereby providing a fig leaf for avoiding reporting to SSCI and HPSCI.[303] HPSCI went so far as to warn that "if DOD does not meet its obligations to inform the Committee of intelligence activities, the Committee will consider legislative action clarifying the Department's obligation to do so."[304]

HPSCI's argument is well taken, assuming that the military did in fact use the OPE label to cast intelligence collection activities in terms of TMA, for categorization as TMA simply does not speak to the question of whether an action must be reported to SSCI and HPSCI as an intelligence collection activity. TMA is no more and no less than an exception to the procedural rules associated with *covert action*, and using the TMA label to avoid those rules does nothing to justify avoidance of the distinct information-sharing requirement attaching to all U.S. government collection activity. Put simply, OPE activities may well qualify as TMA rather than covert action, but it does not follow that those activities are not also *collection* activities that must be notified to SSCI and HPSCI. Congress can and should stand

301. According to 50 U.S.C. §413a, all government agencies involved in "intelligence activities" must keep SSCI and HPSCI "fully and currently informed of all intelligence activities," including "any significant anticipated intelligence activity and any significant intelligence failure." 50 U.S.C. §413a(a)(1) (2006). The obligation is restated, moreover, in another section that emphasizes that the president has ultimate responsibility for ensuring compliance with this notification obligation. *Id.*

302. *See* H. R. REP. NO. 111-186 (2009).

303. *Id.*

304. *Id.*

firm on this position; no statutory changes should be needed to justify that course.

Not all military activity grouped under the TMA label is in the nature of collection, however. On the contrary, a range of operations would plainly qualify as covert action if not conducted and commanded by the military in relation to current or anticipated hostilities. These examples of TMA by definition are not subject to the notification regime for intelligence collection, and the whole point of defining them as TMA is to exempt them as well from the covert action regime. The only remaining question – in terms of mandatory information-sharing rules – is whether a given instance of TMA of this variety might require notification to Congress as a whole pursuant to the WPR's consultation and notification rules.

The Obama administration on at least one occasion has referenced a "classified annex," under the general heading of military operations against al Qaeda and its allies in connection with a WPR report to Congress.[305] In theory this might encompass some activity that would not separately be reported to SSCI or HPSCI due to the TMA exemption. But even assuming that at least *sometimes* TMA gets notified to Congress in this manner, it is doubtful this mechanism closes much of the oversight gap generated by the TMA exemption and the breadth of activity that might fall within it in light of convergence related trends.

The Obama administration famously takes a very narrow view of the meaning of "hostilities" as that word is used in the WPR,[306] and as a result it is quite possible, if not probable, that a substantial amount of TMA would fall below the WPR threshold and hence generate no notifications to Congress. Even if the WPR threshold were construed more broadly, moreover, the fact that TMA encompasses not just activity in support of ongoing overt operations (track one), but also activity collateral to operations that are merely *anticipated* (track two), means that some TMA almost certainly would not trigger the WPR threshold. And though under track two, TMA must be supported by authorization from the President or the Secretary of Defense, there is no corresponding obligation to notify Congress. Finally, although the WPR does require at least semiannual updates regarding qualifying deployments, it is far from clear that this reporting obligation requires a level of detail comparable to that required for covert actions; the executive branch might plausibly discharge its obligations with relatively generic descriptions.

Setting aside the WPR, one might expect the Senate and House Armed Services Committees (SASC and HASC, respectively) to exercise a degree of oversight over TMA roughly comparable to that which SSCI and HPSCI

305. *See* Letter from the President on the War Powers Resolution (June 15, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/06/15/letter-president-war-powers-resolution.

306. *See* Morrison, *supra* note 213.

exercise over covert action. But though some reporting does occur, nothing analogous to the covert action notification is required by statute for DoD. The closest example might be 10 U.S.C. Section 119, which provides that DoD may not initiate new Special Access Programs (SAPs, which strictly limit access to knowledge about classified programs) without notification to SASC and HASC, including descriptions of the programs and milestones for them.[307] Insofar as an activity categorized as TMA falls within a DoD SAP, it might therefore be brought to the attention of SASC and HASC as a statutory obligation. Yet it is not clear that Section 119 would require the degree of granularity that would prompt discussions of particular operations.[308] Whatever reporting of TMA does occur, therefore, is probably better understood to be a function of information sharing typical of a department and its authorizing committees, rather than an obligation to be followed in all circumstances.

The result is problematic, especially with respect to unacknowledged military operations taking place in states where no overt hostilities are occurring or imminent (and especially if such operations would involve the use of lethal force). Whether anything can be done to rectify the situationis far from clear.

In 2003, there was an attempt to amend the TMA definition, and it failed utterly. SSCI tried negotiating with the Undersecretary of Defense for Intelligence, Stephen Cambone, about amending the TMA definition to limit its scope.[309] Believing it had reached an understanding with Cambone, SSCI apparently articulated a new approach in a classified annex to a report.[310] According to *Washington Times* reporter Bill Gertz, the "new restrictions on the use of Special Operations Forces" would "for the first time . . . require a presidential order before deploying commandos in routine but hidden activities."[311] Specifically, "Cambone understanding" would have modified the TMA definition by adding a new condition: an unacknowledged activity could qualify as TMA only if the U.S. military simultaneously had an overt presence in the country in question, whereas "those same activities when carried out in a nation where the presence of U.S. military forces is kept secret are to be treated as covert actions and require a presidential finding" – and, by extension, notification to SSCI and HPSCI.[312]

307. *See* 10 U.S.C. §119 (2006).

308. Section 119(e), moreover, permits the Secretary of Defense to report certain information only to the chair and ranking members of SASC and HASC, rather than the full committees, upon a determination by the secretary that "inclusion of that information in the report would adversely affect the national security." *Id.* §119(e).

309. Gertz, *supra* note 6.

310. *See id.*

311. *Id.*

312. *Id.*

The Pentagon, supported by SASC and HASC, resisted the change.[313] At least one "senior U.S. intelligence official" argued that the language in the report reflected a misunderstanding of conversations between Cambone and certain senators, was not by any means an agreed position, and in fact was "opposed by most U.S. intelligence and defense officials."[314] An official explained that "[i]f you put a clandestine agent inside Iran to prepare for a hostage rescue, that's traditional military activity, not covert action."[315] Secretary of Defense Rumsfeld "told a town hall meeting at the Pentagon in August [of 2003] that [SASC] had assured him that no new restrictions on special operations had been enacted."[316] Indeed, the conference report accompanying the ultimate version of the intelligence authorization bill in November 2003 not only did not indicate any change to the understanding of TMA, but affirmatively repudiated the possibility.[317]

This may well have been the right decision at the time, barely two years after the 9/11 attacks and in the earliest stage of the ascent of JSOC and operations under the al Qaeda Network Exord. Eight years later, however, it might be wise to revisit the question, particularly in light of two factors: the diffusion of the terrorist threat associated with al Qaeda in the form of geographically dispersed franchises and like-minded groups and individuals, and the looming drawdown of overt combat operations in Afghanistan. At the same time, it would be foolish to assume that either the Pentagon or SASC and HASC would acquiesce in, let alone support, an attempt by Congress to give SSCI and HPSCI considerably more oversight over JSOC operations. For this reason, that responsibility should be thrust upon SASC and HASC.

I do not mean to suggest that such oversight should be established for activities conducted within states where overt hostilities are underway, such as Afghanistan today or Iraq in previous years. I am concerned, rather, with unacknowledged operations functionally equivalent to covert action that occur in states remote from combat or imminent combat that escape categorization as covert action due to the expanding scope of TMA. At an absolute minimum, this change should be pursued for any such operations involving the use of lethal force.[318]

313. *See* Kibbe, *supra* note 7, at 107.

314. Gertz, *supra* note 6.

315. *Id*.

316. Kibbe, *supra* note 7, at 107.

317. *See* Kibbe, *supra* note 7, at 107 (writing that "the intelligence committees reaffirmed the 'functional definition of covert action'" and that the bill further indicated that "[n]either the Administration nor the Conferees have sought or agreed to modify, amend, or reinterpret the scope of the Act, or approval and notification requirements under the Act").

318. It is worth emphasizing that oversight is not merely a means for disciplining the executive branch through external accountability. Disclosure to Congress also protects the executive branch by reducing risk of Congressional backlash should an operation later go badly. The more complete the disclosure, the better for all. *See* John Rizzo, *9/11: Three*

It may be that SASC and HASC already have, in practice, substantial insight into JSOC's activities, TMA or otherwise, and that statutory entrenchment of a reporting requirement would have little or no practical effect. In that case, of course, there is no harm in codifying the practice, and at least some benefit in terms of the optics of democratic accountability in relation to JSOC's increasingly important role.

Legislation could and probably should establish a mechanism for reporting such activities to SASC and HASC, modeled on the Gang of Eight process. Congress should also take the opportunity to make a critical change to all such Gang of Eight reporting mechanisms. Currently, the Gang of Eight receives briefings without their professional staff present, and there is reason to believe that this substantially hinders their capacity to form judgments about the information. That process should be modified, possibly by permitting the chief majority and minority counsels for the relevant committees to attend as well (creating a Gang of Twelve).[319]

D. The Title 10/Title 50 Debate and the Intersection of Domestic and International Law

The decisionmaking and information-sharing issues described above are not the only issues raised by the convergence trend. Indeed, they may not be the ones that have most troubled government lawyers in recent years. That honor likely goes, instead, to the question of whether different substantive legal constraints apply depending on whether an action is conducted under color of Title 10 or Title 50 authority.

1. The Meaning of Title 10 and Title 50 Authority

It is worth pausing to clarify the meaning of Title 10 and Title 50 authority. Title 10 of the U.S. Code contains the bulk of the statutes that regulate the armed services, and the phrase accordingly is routinely used as a shorthand for the proposition that the military has domestic law authorization to carry out certain activities. That usage in fact is imprecise. Regarding the use of military force, as in the context of the conflict with al Qaeda, the actual domestic law source of the military's authority is found not in Title 10 but, rather, in either statutory authorizations for using such force (such as the AUMF) or the executive branch's inherent authority (and duty) to use force in national self-defense (founded in Article II of the Constitution). Nonetheless, Title 10 authority is commonly used in the

Major Mistakes, DEFINING IDEAS: HOOVER INSTITUTION JOURNAL (Sept. 8, 2011), http://www.hoover.org/publications/defining-ideas/article/91992.

319. *See* Kathleen Clark, *Congress's Right to Counsel in Intelligence Oversight*, U. ILL. L. REV. 915 (2011).

argot of national security law as a way of referring to quintessentially military activity.

Title 50 is a portion of the U.S. Code that contains a diverse array of statutes relating to national security and foreign affairs. These include the standing affirmative grants of authority through which Congress originally empowered the CIA to carry out its various functions. That set in turn includes the sweeping language of the so-called fifth function, which the executive branch has long construed to grant authority to engage in covert action. Separately, Title 50 also contains the statutes that define covert action, require presidential findings in support of them, and oblige notification of them to SSCI and HPSCI. As a result, Title 50 authority has also become a shorthand, in this case one that refers to the domestic law authorization for engaging in quintessential intelligence activities such as intelligence collection and covert action.

While this seems clear, note that the notion of a Title 10-Title 50 distinction tends to obscure the possibility that some actions ought to require justification, based on domestic law, under *both* titles. The strongest case for this is seen in the CIA drone campaign in Pakistan: a covert operation governed by Title 50, but one that involves the intentional use of lethal force on a sustained basis in relation to an enemy with which the U.S. government claims to be at war. It is far from obvious that the only relevant domestic law question is whether Congress has given the CIA standing authority to engage in covert action. The more important question, arguably, is whether the CIA's action has a sufficient domestic law foundation in terms of either an AUMF or a legitimate claim of inherent constitutional authority for the use of force under Article II. It is easy to answer in the affirmative with respect to this particular example; the AUMF provides a relatively strong foundation for resolving such Title 10 concerns. The important point, however, is that the drone program probably requires justification under both headings, and thus that it can be a bit misleading to ask *solely* about authorization under Title 10 or Title 50.

This possibility – that a given operation may require dual justification – almost invariably goes unremarked in Title 10-Title 50 debates.[320] On the contrary, there is typically an assumption that only one or the other authority applies in a given case, and debate generally focuses on a different question: do Title 10 and Title 50 differ in terms of whether and to what extent operations conducted under each heading are subject to the constraints of international law?

320. For a rare counterexample, see CURTIS A. BRADLEY & JACK L. GOLDSMITH, FOREIGN RELATIONS LAW (4th ed. 2011).

2. Does Title 50 Confer Discretion To Act in Violation of International Law?

Over the course of the past few years, government officials have repeatedly suggested that different substantive legal constraints attach depending on whether activity occurs under Title 10 or Title 50, and that this distinction has an impact on decisions regarding which entities are tasked with which operations in which locations. The claim has arisen most often in connection with the CIA, JSOC, and the use of lethal force in the form of drone strikes.[321] The killing of Anwar al-Awlaki, a U.S. citizen, by a combination of CIA and military drones operating under the CIA's Title 50 authority is but the latest example,[322] one that echoes the previous decision to have CIA "command" the SEAL Team Six attack on bin Laden. Similar claims have been made in relation to the conduct of CNOs, moreover.[323]

Some might suspect that such claims are just cover for non-legal considerations for favoring one agency or another to have the lead in a given operation. Such considerations might include diplomatic sensitivities (Pakistani officials, for example, might prefer to be able to say that the U.S. military never formally operates on its territory, other than in run-of-the-mill liaison capacities), turf fights (the CIA, for example, might reasonably demand a share of the spotlight when it came to the culmination of a decade's worth of searching for bin Laden), budget concerns, considerations of relative practical capacities and experience, or some combination of all these considerations. Others, in contrast, might fear that the claim of differential legal constraints is all too real, and that it might involve a claim that Title 50 authority entails permission in domestic law to act in violation of international law.

Neither of those skeptical accounts is entirely correct, yet both contain elements of truth. Some or all of the non-legal considerations just listed no doubt play a significant if not preponderant role when it comes to the allocation of responsibility for various operations among government entities, yet there are also legal and quasi-legal distinctions that may influence such decisions as well. On the other hand, Title 50 authority does not provide *carte blanche* to act in violation of international law. Most

321. *See, e.g.,* Josh Gerstein, *Sept. 11 Panel's Forgotten Concern: "Paramilitary" CIA*, POLITICO.COM (Sept. 10, 2011), http://www.politico.com/news/stories/0911/63155.html (noting the claim that "U.S. laws . . . made it easier for the [CIA] to quickly ramp up [paramilitary operations] and to operate secretly overseas"); Barnes & Entous, *supra* note 11; Miller, *supra* note 11; Miller & Tate, *supra* note 11.

322. *See* Miller, *supra* note 158 ("The attack on Aulaqi blended capabilities from both sides and was carried out under CIA authority that allowed for greater latitude in conducting lethal operations outside conventional war zones.").

323. *See* Nakashima, *supra* note 9.

significantly, Title 50 provides no justification for disregard of the laws of war. Whether Title 50 authority differs from Title 10 authority in relation to international law protections for the sovereignty of other states is, however, a more complex question.[324]

a. Title 10, Title 50, and the Laws of War

Does the Title 10-Title 50 distinction have any bearing on whether a U.S. government action must comply with international humanitarian law (IHL)? In theory, there are two senses in which the answer might be yes. First, it might be that the field of application of IHL is best understood to exclude covert action. Second, it might be that Title 50, as a matter of U.S. domestic law, is best read to provide implicit authority to act in violation of IHL. Neither of these arguments bears scrutiny.

Consider first the applicability of IHL on its own terms. It does not provide exemptions based on the nature of the agency or entity involved in a given operation, nor does it do so based on whether the operation is acknowledged or denied.

The major IHL treaties, such as the Geneva and Hague Conventions, purport to bind the parties to a conflict as a whole, not just those entities belonging to each party that happen to be regular armed forces. It is the U.S. government, not just the U.S. military, which must comply with the principles of necessity, proportionality, and distinction. If IHL applies to an activity, in other words, there is no basis for setting IHL aside merely because of the identity or nature of the particular organization or entity through which the party is acting. Indeed, the United States could hardly argue otherwise in the post-9/11 era, given the consistency with which it has advanced the position that non-military actors, such as al Qaeda members, are bound by IHL and may be prosecuted for war crimes for their IHL violations. Nor is there any reason to believe that the customary law of war differs in this respect. The same can be said about IHL in relation to the overt-covert distinction; nothing in IHL suggests that actors conducting operations on an unacknowledged basis in any way exempts them from compliance with IHL constraints.

The more interesting question is whether this lack of distinction carries through into U.S. domestic law. The "dualist" nature of the American legal system as it relates to international law, after all, opens the door to the

324. I set aside the possibility of an institutional distinction relating to international human rights law (IHRL). For better or worse, the United States does not accept that its IHRL treaty obligations apply outside the United States in the first place, and in any event believes that under the principle of *lex specialis* these obligations do not govern where the law of armed conflict also is in play. Both of these views are fiercely contested. There is no reason to believe, however, that this contestation manifests within the government in the form of a perceived distinction in how operations may be conducted under Title 10 or Title 50.

possibility that IHL might be incorporated into domestic law in a manner that differentially impacts overt and covert action. There is little reason to think that the domestic legal system actually does this, however.

There is some degree of explicit incorporation of IHL into domestic law, and none of it suggests an overt-covert distinction. To begin, the Constitution considers treaties – including IHL instruments such as the Geneva and Hague Conventions – the law of the land. Beyond this, statutes such as the War Crimes Act explicitly incorporate various aspects of IHL into domestic criminal law, with no mention of the relevance of the institutional affiliation of a defendant or of the overt-covert distinction.

Then there is the question of *implicit* incorporation, which arises most obviously in connection with the AUMF relating to al Qaeda. In granting the President the authority to use military force, the AUMF does not explicitly require compliance with IHL. However, nor does it purport to grant the power to act in violation of IHL, either by acting overtly or even covertly. At least since 2009, the executive branch has taken the position that the AUMF is best read to implicitly condition its grant of authority upon compliance with applicable IHL rules.[325]

None of this would matter, perhaps, if Title 50 were read as providing standing authority to act in violation of IHL. Title 50 obviously does not do so explicitly, however, and there is nothing in the legislative history or subsequent practice under the Title 50 system (whether one focuses on the fifth function, the covert action definition, or both) suggesting that Congress intended that the CIA (or any other entity engaging in covert action) be exempted from IHL compliance in relation to armed conflict.

There is one final wrinkle that requires discussion in relation to IHL. The DoD as a matter of *policy* applies and conforms to IHL standards at *all* times, even when IHL does not apply.[326] This explicitly includes compliance with the requirements of military necessity, distinction, and proportionality.[327] CIA has no comparable policy, insofar as the public record indicates. Strange as it sounds, then, one can say that the military is more constrained than the CIA with respect to IHL standards, but only when IHL does not actually apply.

It is not clear that anything turns on this policy distinction. Where it might matter most is in the context of drone strikes conducted in locations where arguments *might* be made that IHL has no application. But from the public record, there is considerable reason to believe that the CIA does

325. *See, e.g.,* Brief for the Respondents, *supra* note 281.

326. As stated in Joint Publication 1-04, "[i]t is DOD policy that members of the DOD Components comply with the law of war during all armed conflicts, however such conflicts are characterized, *and in all other military operations*." JOINT PUBLICATION 1-04, LEGAL SUPPORT TO MILITARY OPERATIONS II-2 (2011), *available at* http://www.fas.org/irp/doddir/dod/jp1_04.pdf (emphasis added).

327. *See id.*

indeed follow the DoD practice of applying IHL concepts of necessity, distinction, and proportionality in all settings – even those that might not amount to armed conflict.

The closest thing to an official confirmation of this came in State Department Legal Adviser Harold Koh's speech delivered at the American Society of International Law conference in March 2010. Koh took up the question of the use of force via drones. He was careful not to refer to the CIA or to drone strikes in Pakistan in particular, but taken in context most in the audience came away understanding that they had just heard a defense of the legality of the CIA drone program.[328] "[T]here are obviously limits to what I can say publicly," Koh noted.[329] But he was able to assert "that it is the considered view of this Administration . . . that U.S. targeting practices, including lethal operations conducted with the use of unmanned aerial vehicles, comply with all applicable law, including the laws of war."[330] Koh went on to assert specifically that "the principles of distinction and proportionality . . . are implemented rigorously throughout the planning and execution of lethal operations to ensure that such operations are conducted in accordance with all applicable law," including contexts that might involve "self-defense" separate and apart from "armed conflict."[331]

This suggests that, as a matter of law and policy, there is no substantial difference between the military and the CIA with respect to whether and how IHL constrains kinetic operations.[332] That is not to say the military and the CIA are likely to operationalize these constraints with equal efficacy. The military's training regimens and doctrinal structures have long been premised on the relevance of IHL, after all, while the same has not traditionally been true for the CIA. This no doubt could produce variation in the sophistication and thoroughness with which IHL concepts are brought to bear in particular cases, though any such gap could be reduced over time through enhanced training and legal oversight within the CIA.[333]

328. *See, e.g.,* Adam Serwer, *Did Harold Koh also Provide Legal Justification for Targeted Killings of Americans Suspected of Terrorism?*, THE AMERICAN PROSPECT, Apr. 12, 2010, *available at* http://prospect.org/csnc/blogs/tapped_archive?month=04&year=2010&base_name=did_koh_also_provide_the_legal.

329. Harold Hongju Koh, *The Obama Administration and International Law* (Mar. 25, 2010), *available at* http://www.state.gov/s/l/releases/remarks/139119.htm.

330. *Id.*

331. *Id.* Other less formal accounts – such as the detailed descriptions of drone strike decisions by then-Director Panetta, provided by Joby Warrick in his book, *The Triple Agent* – are consistent with this understanding of Koh's speech at least insofar as they reveal a constant focus on the question of collateral damage. *See* WARRICK, *supra* note 140. *See also* Tara Mckelvey, *Inside the Killing Machine*, NEWSWEEK (Feb. 13, 2011), http://www.thedailybeast.com/newsweek/2011/02/13/inside-the-killing-machine.html.

332. Again, institutional culture might well be a different matter. The military's training and doctrinal structures have long been premised on the assumption that IHL applies, while the same has not historically been true for the CIA.

333. For a skeptical view of this question, see Alston, *supra* note 13.

In the meantime, one of the most useful steps that the executive branch and Congress could take would be to state in no uncertain terms that operations authorized under Title 10 and Title 50 alike comport with IHL norms at all times, or at least whenever the use of lethal force is intended.

b. Title 10, Title 50, and Sovereignty

Is there a Title 10-Title 50 distinction with respect to international law's protection of state sovereignty? That is a decidedly more complicated question.

As with the IHL inquiry, one must distinguish between arguments about the content of international law itself and arguments about the potentially variable reception of that content into domestic law. The first question concerns the range of extraterritorial actions that actually are prohibited (or otherwise constrained) as a matter of international law. A good place to begin that analysis is with Article 2(4) of the U.N. Charter.

Article 2(4) forbids "the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations" (which include the goal of maintaining "international peace and security").[334] That prohibition is not an absolute. One state may act on another's territory without raising Article 2(4) concerns if it has the latter's permission, for example, and force may be used against another state even without its consent if the U.N. Security Council authorizes it or if the circumstances implicate the right of self-defense referenced in Article 51.[335] Where one of these exceptions applies, of course, no question would arise as to whether Article 2(4) applies differentially to activity conducted under Title 10 or Title 50.

The interesting question, then, is whether there are situations involving unacknowledged activity on the territory of another state that Article 2(4) does not forbid in the first instance. It is helpful to distinguish between run-of-the-mill intelligence-gathering activities – i.e., spying – and covert action.

Spying of course will normally violate the domestic laws of the host state. But it is far from clear that spying itself is a violation of international law, either as a general matter or in connection with Article 2(4) in particular. Spying ordinarily does not involve the use or threatened use of force, of course, and hence is a poor fit with the language of Article 2(4).

334. U.N. Charter art. 1(1), 2(4).

335. That right of self-defense, moreover, at least arguably extends to circumstances in which the host state is unable or unwilling to suppress a non-state actor that is carrying out armed attacks on another state while harboring within the host state's territory. *See, e.g.*, Ashley Deeks, *Pakistan's Sovereignty and the Killing of Osama bin Laden*, ASIL INSIGHTS (May 5, 2011), http://www.asil.org/insights110505.cfm.

More generally, the prevalence of spying and the lack of sustained claims that spying violates international (as opposed to domestic) law when it is detected militates against recognition of any customary norm against the practice.[336]

If that conclusion is correct, then there is no need to consider whether Title 50 is properly read to authorize violations of sovereignty via spying. If, on the other hand, spying is construed to be forbidden by international law, it is very hard to escape the conclusion that Title 50 must be read to provide domestic law justification for breaking that rule.

Covert action is a different kettle of fish. It spans a spectrum of intensity, ranging from relatively innocuous activity, to operations disruptive to the political independence of other states, all the way to activity amounting to armed attack. It is unclear whether and to what extent international law purports to forbid covert actions that fall short of the "use of force" standard mentioned in Article 2(4). Some contend that customary international law includes a general prohibition to the effect that "[e]very State has the duty to refrain from intervention in the internal or external affairs of any other State."[337] Whether that is so, and just how far such a prohibition might run, is a difficult and significant question. But the important point for present purposes is that at least some covert action might constitute a "use of force" within the meaning of Article 2(4), and there is neither a textual basis for construing Article 2(4) to contain an exception for covert operations, nor a good case for construing Article 2(4) to have such an exception (as it would run fairly sharply against the grain of the objects and purposes of the Charter in general and that article in particular).

This is enough to compel consideration of the second question: whether Title 50 should be construed to permit covert action contrary to whatever sovereignty protections international law might provide.

If the proper reading of international law is that *all* such operations are prohibited, separate and apart from Article 2(4) problems, Title 50 would almost certainly have to be construed to authorize breach of that general rule. It is clear, after all, that Congress is well aware of the fact that the

336. *Cf.* A. John Radsan, *The Unresolved Equation of Espionage and International Law,* 28 MICH. J. INT'L L. 597 (2007); REISMAN & BAKER, *supra* note 223. One might argue that the very fact that such activities are conducted on a secret and unacknowledged basis evidences awareness on the part of states that they are not lawful, but that argument is difficult to maintain in the face of the much more obvious explanation that they are kept secret so that they can actually succeed and remain unacknowledged in order to minimize retaliation and embarrassment.

337. *See, e.g.,* Craig Forcese, *Spies Without Borders: International Law and Intelligence Collection*, 5 J. NAT'L SEC. L. & POL'Y 179, 198 (2011) (quoting "Draft Declaration on Rights and Duties of States," 1949 Y.B. INT'L L. COMM'N 287, art. 3). The Draft Declaration was never adopted, though Forcese contends that "many of its provisions reflect core precepts in modern international law." *See id.* at 185 n.15. *See also id.* at 198 (quoting a General Assembly declaration to similar effect).

CIA does carry out covert action, and far from stopping the practice, Congress has passed statutes explicitly regulating it and thus implicitly approving of it. One could not escape the conclusion, in that case, that Congress intended the CIA to engage in at least some forms of covert action regardless of international law constraints.

The question would remain, however, whether the same conclusion should follow as to covert action that would violate Article 2(4). The most plausible answer is no, as there is nothing in the text, legislative history, or subsequent course of practice under Title 50 that suggests Congress intended or has acquiesced in the use of covert action to carry out acts amounting to the use of armed force without a justification such as a legitimate claim of self-defense or host state consent. Thus, it seems true that whether acting under Title 10 authority or Title 50 authority, U.S. government entities are comparably situated with respect to Article 2(4) and the use of force without adequate justification.[338]

There is one glaring problem with this analysis. If it is correct, then why have government officials repeatedly suggested in the context of drone operations that Title 50 operations as a legal matter can be carried out in foreign states without host government consent more readily than can Title 10 operations? The answer is that these should not be understood as claims about a Title 50 international law override, but rather as claims about the distinct constraints the executive branch has imposed on Title 10 activity via the al Qaeda Network Exord and any of its successors, on one hand, and various al Qaeda-related covert action findings and MONs, on the other.

As described in Part I.B, the public record suggests the following: A series of Exords both authorize and constrain JSOC's operations in relation to al Qaeda and its associated forces, just as various findings and MONs do for the CIA. At least as of 2003, it was clearly the case that under the then-applicable framework, the CIA had greater freedom of action to carry out counterterrorism operations outside of Afghanistan and Iraq than did the military. Secretary Rumsfeld was eager to close that gap, and near this time a new or modified Exord paved the way for JSOC operations in a range of locations – with the level of approval necessary to conduct particular

338. None of which is to deny that the CIA and the military might have distinct *cultures* with respect to respect for the sovereignty of other states, or that such cultural variation can in turn interact with legal questions. Most significantly, the culture of an institution may impact the willingness of its leadership to support participation in activities that present close calls in terms of their legality under Article 2(4) (or any other sovereignty-oriented rule that might exist). Specifically, it may well be that the CIA as an institution is more comfortable than the military with operations that raise difficult legal questions under this heading. Or at least that is a plausible hypothesis as to the military writ-large. Whether the comparison is as plausible when we focus on SOF units such as those associated with JSOC is not as obvious.

operations dependent on the identity of the country in which the operation would take place.

The question is whether this development, or others related to it, wholly aligned the military's freedom of action with that which the CIA enjoyed under its governing findings and MONs. There is some reason to doubt that this is so, notwithstanding the fact that the al Qaeda Network Exord apparently broke new ground in its relatively open-ended approach to the geography of hostilities.[339] More specifically, there is reason to believe that the military may be more constrained than the CIA when it comes to conducting operations without seeking consent from or at least providing notification to the host government.

Ongoing media coverage of evolving drone operations in Yemen has repeatedly hinted at this possibility. To cite specific examples, in fall 2010, Julian Barnes and Adam Entous reported that the Obama administration was considering a shift from JSOC stand-alone operations to hybrid operations in which JSOC units would operate under CIA authority.[340] Such a shift would permit "unilateral" operations "without the explicit blessing of the Yemeni government."[341] Similar hybrid arrangements had been used in other locations including Iraq, Barnes and Entous explained, "in order to get around restrictions *placed on military operations*."[342]

This past summer, journalists reported that the Obama administration planned to have the CIA join JSOC in conducting drone operations in Yemen. Several reporters emphasized that distinct legal frameworks having to do with host state consent helped to explain the shift (in addition to more practical concerns, such as the sheer number of drones available to the CIA and the possibility that CIA drones are more often equipped with smaller missiles suitable for decreasing collateral damage). Greg Miller, for example, wrote that "Because it operates under different legal authorities than the military, the CIA may have greater latitude to carry out strikes if the political climate shifts in Yemen and cooperation with American forces is diminished or cut off."[343] And Siobhan Gorman and Adam Entous observed that "[t]he U.S. military strikes have been conducted with the permission of the Yemeni government. The CIA

339. *See* SCHMITT & SHANKER, *supra* note 140, at 128 (quoting a former administration official for the proposition that this "was a fundamental legal difference from past 'ExOrds' written to deal with a specific nation-state adversary").

340. Julian Barnes & Adam Entous, *Yemen Covert Role Pushed: Foiled Bomb Plot Heightens Talk of Putting Elite U.S. Squads in CIA Hands*, WALL ST. J. (Nov. 1, 2010), at A1.

341. *Id*. The report indicates various other reasons for the shift, including the notion that "[a] shift to the CIA would . . . giv[e] the White House more direct control over day-to-day operations." *Id*.

342. *Id*. (emphasis added). Barnes and Entous also wrote that "when the military conducts missions in a friendly country, it operates with the consent of the local government." *Id*.

343. *See* Miller, *supra* note 158.

operates under different legal restrictions, giving the administration a freer hand to carry out strikes even if Yemeni President Ali Abdullah Saleh, now receiving medical treatment in Saudi Arabia, reverses his past approval of military strikes or cedes power to a government opposed to them."[344] More recently, Miller and Julie Tate wrote in that the decision to expand CIA drone operations into Yemen "was driven" not just by the CIA's capabilities but also by its "unique authorities," which apparently contrast with "conventional military authorities that require permission or at least a level of acquiescence from Yemen."[345] Miller and Tate explained that "[t]he CIA is in a better position to keep flying even if that cooperation stops."[346] Notably, when the United States finally succeeded in killing Anwar al-Awlaki of AQAP in a drone strike on September 30, 2011, it did so in an operation "carried out by Joint Special Operations Command, under the direction of the CIA."[347]

These references to "legal" variations related to host state consent almost certainly do not have to do with international law constraints, for the reasons set forth above. The variation, instead, almost certainly stems entirely from the distinct scope of the relevant Exords, findings, and MONs.[348]

E. CNOs and the Title 10-Title 50 Debate

The final topic to be addressed concerns CNOs in the context of the foregoing discussion.

The public record makes clear that this has been the topic of pressing debate for some time as between the CIA and the military, yet the nature of that debate is unclear (perhaps reflecting the limits of the public record, miscommunication, or misunderstanding among those involved). The record suggests at times that the issue has to do with the covert action-TMA distinction, though not so much because of the findings-and-notification regime but rather because that categorization might result in one agency or the other having the lead for conducting such operations (and, by extension, the power to resist or support the actual execution of the operation). In Section II.B.2., I addressed this possibility. At other times, however, there

344. *See* Gorman & Entous, *CIA Plans Yemen Drone Strikes: Covert Program Would Be a Major Expansion of U.S. Efforts To Kill Members of al Qaeda Branch*, WALL ST. J. (June 14, 2011), at A8.

345. Miller & Tate, *supra* note 11.

346. *Id*.

347. Jennifer Griffin & Justin Fishel, *Two U.S.-Born Terrorists Killed in CIA-Led Drone Strike*, FOXNEWS.COM (Sept. 30, 2011), http://www.foxnews.com/politics/2011/09/30/us-born-terror-boss-anwar-al-awlaki-killed/.

348. *See* Kenneth Anderson, *DOD or CIA in Yemen?*, THE VOLOKH CONSPIRACY (June 15, 2011), http://volokh.com/2011/06/15/dod-or-cia-in-yemen/.

are hints in the record that the issue instead is a matter of international law protection for sovereignty, and hence I conclude by taking up the CNO topic.

In late 2010, Ellen Nakashima wrote that a dispute was raging with respect to whether the CIA or the military should have lead responsibility for CNOs against al Qaeda-related targets, with the CIA arguing that such operations would be "covert action" and hence "traditionally its turf" and the military replying that "offensive operations are the province of the military and are part of its mission to counter terrorism, especially when, as one official put it, "al-Qaeda is everywhere."[349] But "[t]he real issue," according to one anonymous official quoted in Nakashima's story, was the difficulty of "defining the battlefield."[350]

> Operations in the cyber-world can't be likened to Yorktown, Iwo Jima or the Inchon landing," he said. "Defining the battlefield too broadly could lead to undesired consequences, so you have to manage the potential risks. Getting to the enemy could mean touching friends along the way.

Ultimately, the question was put to the Justice Department's Office of Legal Counsel (OLC) in an effort to settle the interagency debate, and OLC responded with a draft opinion in spring of 2010 "that avoided a conclusive determination on whether computer network attacks outside battle zones" amounted to covert action or TMA, "but that nonetheless concluded that "[o]perations outside a war zone would require the permission of countries whose servers or networks might be implicated."[351]

This approach received reinforcement in the spring of 2011, when the Pentagon completed a "weapons-review" of various CNO instruments. All weapons in the arsenal of the DoD are subject to a legal review, typically focused on ensuring their compliance with considerations such as IHL rules regulating the means and methods of warfare – and possibly also other international law considerations, such as the legal principles relating to the protection of sovereignty discussed above. Depending on the weapon, that review might result in approval for use subject to certain conditions, such as a requirement that high-level approval be obtained before particular weapons are used. Cyberweapons are no different in this regard.

In May 2011, Nakashima reported that the DoD had developed a "list of cyber-weapons and – tools, including viruses that can sabotage an adversary's critical networks, to streamline how the United States engages in computer warfare."[352] Nakashima explained that the list entailed a

349. *See, e.g.,* Ellen Nakashima, *Pentagon Is Debating Cyber-Attacks,* WASH. POST, Nov. 6, 2010, at A1.

350. *Id*.

351. *Id.*

352. Ellen Nakashima, *Defense Dept. Develops List of Cyber-Weapons*, WASH. POST,

complex set of conditions on CNOs,[353] including conditions suggesting that sovereignty concerns – whether of legal or simply diplomatic – weighed heavily on the process.

"[T]he use of any cyber-weapon outside an area of hostility or when the United States is not at war is called 'direct action' and requires presidential approval," Nakashima wrote, whereas "in a war zone, where quick capabilities are needed, sometimes presidential approval can be granted in advance so that the commander has permission to select from a set of tools on demand. . .."[354] She added that this structure was created "in part out of concerns that deciding when to fire in cyberspace can be more complicated than it is on traditional battlefields," particularly insofar as "targets can include computer servers in different countries, including friendly ones."[355] Citing a 2010 dispute between the CIA and CYBERCOM over whether to conduct a CNO to take down the website of AQAP, Nakashima added that the debate "rekindled a long-standing interagency struggle over whether disrupting a terrorist Web site overseas was a traditional military activity or a covert activity – and hence the prerogative of the CIA."[356]

The issue driving this debate is international law's protection for the sovereignty of other states, and thus the Title 10-Title 50 debate as applied to CNO clearly intersects with the discussion immediately above. There I concluded that Title 10 and Title 50 operations are similarly situated with respect to conduct constituting the "use of force" under Article 2(4). Insofar as a CNO's impact on a third-country server or system amounts to a "use of force," then, it would follow that there is nothing to be gained by proceeding under Title 50 rather than Title 10 in terms of legal flexibility (there might be practical, diplomatic advantages to a Title 50 approach, if this increased the capacity of governments involved to act as if the United States had no responsibility for the operation).

But if the impact on the third-country server or system falls below that threshold, then one would confront two contested questions: what international law actually forbids in the first place, and whether Title 50 should be construed to override any such objections. The law is simply not sufficiently clear on either point to enable conclusive answers, which may be why former DNI Dennis Blair lambasted this debate as "infuriating" and "over-legalistic," concluding that "[t]he precedents and the laws on the books are just hopelessly inadequate for the complexity of the global information network."[357]

May 31, 2011, at A3.

353. *See id.*

354. *Id.*

355. *Id.*

356. *Id.*

357. Nakashima, *supra* note 349.

Blair is correct, but it is not entirely clear how best to improve the situation. Nakashima notes that there is pending legislation at least partially intended to respond to the problem – Section 962 of the National Defense Authorization Act for Fiscal Year 2012.[358] That provision would "affirm" the Title 10 authority of the "Secretary of Defense . . . to conduct military activities in cyberspace," including "authority to carry out a clandestine operation in cyberspace" so long as the CNO is "in support of military operations" authorized by "9/18/01 AUMF" or "to defend against a cyberattack against an asset of the Department of Defense."[359] According to Nakashima, the bill's sponsor in the House intends this to "establish that [CNOs] to deny terrorists the use of the Internet to communicate and plan attacks from throughout the world are a 'clandestine' and 'traditional military' activity."[360]

A proper reading of the covert action definition *ought* to make it clear already that a CNO under color of the AUMF (a context in which overt hostilities certainly are underway already) constitutes TMA, with all the consequences that follow in terms of not requiring a finding or notification to SSCI and HPSCI, and, it seems, permitting the military rather than the CIA to function as lead agency. If experience shows that this is the subject of continuing disputes, however, legislation to clarify the matter would indeed be desirable.

Or at least it would be desirable if it matched that clarification with a layer of decisionmaking and information-sharing rules appropriate to the risks associated with CNOs affecting servers and systems in neutral (or even friendly) states. The proposed Section 962 in fact contains such an information-sharing obligation, calling for periodic reporting to SASC and HASC in such cases. Nakashima's reporting suggests that appropriate decisionmaking structures have been adopted within the executive branch as well, and though it would be wise eventually to entrench those in statute, the novelty of the situation in this instance gives reason to live with the current regime of executive branch self-constraint – thus facilitating experimentation in the quest to craft a structure that best balances the need for speed and the necessity of high-level accountability.

None of this speaks to the potentially significant sovereignty concerns that might play a role in driving the turf battle between the CIA and the military. That may be for the best, given the uncertainty as to what, if anything, international law actually forbids below the "use of force" threshold.

358. *See* Nakashima, *supra* note 352.

359. *See* §962(a) & (b), *available at* http://armedservices.house.gov/index.cfm/files/serve?File_id=61e9d0d1-581b-4204-ba0e-f601878bc710.

360. *See* Nakashima, *supra* note 352.

CONCLUSION

How significant are the Title 10-Title 50 debate and other legal issues raised by the convergence phenomenon? Speaking in the context of drone strikes, Michael Leiter, former Director of the National Counterterrorism Center, recently offered a skeptical view:

> Whether it's . . . CIA or JSOC, to me frankly in the end it doesn't matter that much. Which is why I would prefer not to get caught up on Title 10, Title 50, and Washington debates. I don't think it matters to the countries where we're conducting the strikes or the people we're killing if it was a Title 10 or Title 50. . . . I'd like to avoid some of these legal debates that don't matter, and have the . . . real debates that do matter.[361]

It is tempting to agree with Leiter when considering the question from the perspective of the persons whom the United States may target or the states on whose territory the United States might act. But on closer inspection the issue looks quite different.

The various issues collected under the heading of the "Title 10/Title 50" debate go to the heart of our still evolving national security legal architecture. That architecture aims to reconcile the need for secrecy and discretion in the pursuit of national security aims, on one hand, with the need to subject the resulting powers as much as possible to mechanisms that enhance accountability and compliance with the rule of law, on the other. The current architecture is by no means perfect. Whatever utility it does have, however, will fade if the structure fails to evolve concurrently with fundamental changes in the institutions it purports to regulate. The story of convergence set forth above is the story of just such a significant change, a salutary one involving seemingly successful adaptation to strategic and operational challenges. The question now is whether any serious steps will be taken to retailor the legal architecture accordingly.

361. Interview with Michael Leiter by the Aspen Institute's Security Forum (July 28, 2011), *available at* YouTube.com.