An Assessment of the Evolution and Oversight of Defense Counterintelligence Activities

Michael J. Woods & William King*

For more than thirty years, our country has struggled to delineate the boundaries of domestic intelligence operations. Americans tend to regard those government components exercising national security powers within the borders of the United States (whether under clear authority or not) with an inherent suspicion bolstered by historical experience. We tolerate the existence of such components but insist that they be highly regulated, particularly with respect to any activities that impinge upon civil society. Historical circumstances influence, but never erase, this regulatory imperative. Despite this imperative, components may occasionally escape regulation – at least for a time – because they are unknown, their missions remain mysterious or only partially understood, or because (intentionally or not) a convincing illusion of sufficient regulation is presented to the examining eye.

The aim of this article is to focus on the regulation of those components of the Department of Defense (DoD) empowered to conduct counterintelligence activities. We intend to explore the interlocking effects that statutes, intelligence oversight rules, internal DoD structure, and operational culture have on the conduct of counterintelligence.[1] In our view, these form a regulatory milieu that governs what DoD counterintelligence operators do, or are willing to attempt, in the context of domestic intelligence operations. Some parts of this environment, such as the varied cultures of the several organizations comprising DoD counterintelligence, are more difficult to describe than others. Some, such as the debate over the "wall" in the context of domestic electronic surveillance, occur almost entirely outside of the DoD.

However, we see most of the milieu as ultimately reducible to the underlying law. The legal definition of the term "counterintelligence," the placement of intelligence operations in the statutory structure of the Department, and the post-9/11 changes in the practice and law of

---

* Michael J. Woods is an attorney in the U.S. Department of Justice. He previously served as chief of the Federal Bureau of Investigations (FBI) National Security Law Unit and as Principal Legal Advisor to the National Counterintelligence Executive. The research and writing of this article (exclusive of some final editing) occurred while he was in private practice. William King is a former Air Force intelligence officer and an attorney now in private practice. The views expressed in this article are those of the authors and do not reflect the official policy or position of the Department of Defense, the Department of Justice, the U.S. Government, or any former employer or client of either author.

1. Although both authors have had direct experience with DoD counterintelligence activities, this article is based entirely on publicly available materials. No reference to any classified or otherwise restricted information is intended.

intelligence collection all drive the policy and culture that shape DoD counterintelligence. Our plan is to explore this thicket of regulation, policy, and law with an eye toward evaluating its adequacy in the present environment.

Such a project is certainly appropriate in light of the larger topic of the role of the military in civil society and the specific role of military counterintelligence organizations in activities considered problematic. Since September 11, 2001, the country has experienced yet another iteration of the familiar "pendulum" pattern in the regulation of intelligence activities. In the immediate aftermath of the attacks, there was broad consensus that the national security components of our government had been unduly restricted in the exercise of their appropriate functions by legal and regulatory constraints that responded not to present conditions but to the specter of past abuses. The abuses by the FBI, the CIA, and DoD intelligence components that came to light in the mid-1970s led to an extensive framework of law and regulation intended to prevent misuse of national security powers.[2] That framework, with remarkably few alterations, governed the work of the U.S. intelligence community for a quarter century. The influence of this great spasm of regulation was felt particularly within the DoD, components of which had been responsible for some of the more spectacular of the identified abuses.[3] Some argue that portions of this regulatory matrix had ossified by 2001. Conservative interpretation of the rules governed behavior, with caution reinforced by constant references to the Congressional investigations of intelligence activities in the 1970s. The rules suffered further from the accretion of questionable theories that, at least in retrospect, did not reflect the original intent of the drafters of the regulatory framework.[4] On the eve of 9/11, the components charged with protecting the country against terrorist attack

2. That framework includes both statutes, such as the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§1801-1871 (2000 & Supp. 2004), the Privacy Act of 1974, 5 U.S.C. §552a (2000), and Executive Branch regulations, specifically Executive Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 8, 1981), and its progeny.

3. *See* Final Report of the Select Committee on Governmental Operations with Respect to Intelligence Activities, 94th Cong. (1976) (Book III: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans: Improper Surveillance of Private Citizens by the Military), *available at* http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIIk.htm.

4. One of the best examined instances of this is the matter of the "wall" erected between intelligence and criminal investigative activities following certain interpretations of the FISA and pre-FISA case law. *See* In Re Sealed Case, 310 F.3d. 717 (FISA Ct. Rev. 2002), and Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007) (declining to follow In Re Sealed Case); *see also* David S. Kris, *The Rise and Fall of the FISA Wall,* 17 STAN. L. & POL'Y. REV. 487 (2006), and NATIONAL COMMISSION ON THE TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 78-80 (2004); *see also* Richard B. Schiff, *A Counterintelligence Perspective, Or How I Learned to Stop Worrying and Love the Wall,* 52 Feb. FEDERAL LAWYER 32 (2005).

were, in many respects, hamstrung by the restrictive interpretation of rules designed to protect the civil liberties of Americans.[5]

Following the attacks, the rules were loosened, with varying degrees of care and foresight. Recently, there have been fresh examples of situations in which national security authorities are alleged to have stepped beyond the protective bounds. The "warrantless surveillance" program executed by the National Security Agency (NSA), the seeming overuse of revised national security letter authority by the FBI, and several DoD projects (including the Total Information Awareness program – subsequently renamed the "*Terrorism* Information Awareness" program in response to press criticism – and the Threat and Local Observation Notice (TALON) database) have raised the question of whether our nation's intelligence-gathering components are once again less than adequately regulated.

It is in the context of this "pendulum" that we focus on the role of DoD counterintelligence. Our purpose is to give specific attention to the way in which the DoD's implementation of larger regulatory actions has shaped the counterintelligence environment inside the DoD (and has created implications for civil society beyond DoD). There are a number of reasons for choosing to look specifically at DoD counterintelligence, the most obvious being that DoD counterintelligence components are the common denominator in most of the DoD-related incidents that have garnered national attention as suspected intrusions into civil society. The TALON database, for example, was housed at the DoD Counterintelligence Field Activity (CIFA), which itself was associated with the DoD's post-9/11 data-mining efforts.[6] Military service counterintelligence agents have been involved in an increasing number of activities not in support of military operations, but rather in the domestic civilian environment.[7] The widespread participation of DoD agents on the FBI's Joint Terrorism Task

5. *See id.* There are more specific examples of the effect that the interpretation of DoD intelligence oversight rules had on pre-9/11 activity. One example, though controversial, is the ABLE DANGER matter discussed *infra* at note 162.

6. *See* discussion *infra* at the text accompanying notes 119-125 and 164-167.

7. Perhaps the best known example of the use of DoD counterintelligence components to investigate potential terrorist threats that appear to have no more than a minimal nexus to DoD operations occurred in a widely publicized incident at the University of Texas in 2004. In that incident, Army counterintelligence agents questioned the organizers of an Islamic legal conference at the University of Texas, in response to concerns reported by military attendees at the conference. *See* A.J. Bauer, *Army Agent Questions Law Students*, THE DAILY TEXAN, Feb. 12, 2004, *available at* http://media.www.dailytexanonline.com/media/storage/paper410/news/2004/02/12/University/Army-Agent.Questions.Law.Students-60534 5.shtml. The Army investigated this incident and concluded that the agents had exceeded their authority by questioning individuals not within the Army's investigative jurisdiction. *See* U.S. Army Intelligence and Security Command Press Release No. 03-03-04, *INSCOM Concludes Review of Events at University of Texas Law School* (Mar. 12, 2004), *available at* http://www.fas.org/irp/news/2004/03/inscom 031204.pdf.

Forces and the increased emphasis on counterintelligence support to DoD technology protection efforts are examples of this phenomenon.[8]

Another important reason to examine DoD activities in particular is that the virtual removal of the legal boundary between counterintelligence and law enforcement by the USA PATRIOT Act had significant structural and operational implications for DoD counterintelligence. Similarly, the recent rise in the DoD of the artificially discrete "disciplines" of force protection, research and technology protection, and homeland defense – all of which are more properly understood as hybrids of the older intelligence, law enforcement, and security disciplines – leave DoD counterintelligence components with the potential to choose among alternate rule sets by characterizing their activities either as support to or as a subset of these established disciplines.

Finally, DoD counterintelligence is worth looking at because we now face international terrorist groups not as traditional intelligence adversaries but as direct military adversaries that evade easy geographical classification. This raises the question of how well DoD counterintelligence efforts are integrated into the overall military effort and how well the regulatory framework addresses purely military components that embark on counterintelligence-like missions. We will focus on this final question first.

The first section of this article will examine the basic definition and placement of the counterintelligence function with the DoD. This section will aim to unravel the interlocking sets of DoD directives and regulations that define what components conduct counterintelligence activities, what the limits of their authorities are, and how they are integrated into the larger military function of the Department. Our goal is to reveal how the legal underpinnings of DoD counterintelligence and, in particular, certain persistent fissures in those foundations, may have contributed to the current difficulties in operational oversight.

The second section of the article will look at the post-9/11 evolution of DoD counterintelligence, including both the structural and the ad hoc operational changes that have occurred in the DoD counterintelligence function. An example of the former is the creation of the Counterintelligence Field Activity; the latter is represented by the experience of the TALON program. The examination will include some assessment of oversight mechanisms and evaluations of present trends in DoD counterintelligence within the larger context of re-regulating national security authorities.

---

8. The participation of DoD counterintelligence, law enforcement, and intelligence components in the Joint Terrorism Task Forces has been publicly acknowledged, though the numbers and specific functions of the DoD participants are not generally available. *See* Office of the Inspector General, U.S. Department of Justice, Evaluation and Inspections Report No. I-2005-007, The Department of Justice's Terrorism Task Forces (2005), *available at* http://www.usdoj.gov/oig/reports/plus/e0507/background.htm#jttf.

I. THE DEFINITION AND PLACEMENT OF DOD COUNTERINTELLIGENCE

The beginning of our inquiry, of course, is to understand the boundaries of what constitutes "counterintelligence" in the DoD environment (or elsewhere in the government) and the identity of the various DoD components assigned a counterintelligence function. The project is not as simple as it first appears, however, because the legal definitions and functional assignments do not always correspond. Within the DoD, the proliferation of new disciplines and terms that embody part of the counterintelligence function (like "force protection" and "homeland defense") and the more aggressive application of those disciplines in the domestic environment tend to blur the clear lines implied by the formal definition. Similarly, the conscious integration of counterintelligence methodologies into other DoD functions (e.g., "counterintelligence support to . . .") create hybrid functions that are difficult to properly categorize. It is essential, therefore, to go back to the beginning in approaching this tangled skein of definition and function.

In classical terms, counterintelligence is the function of detecting and opposing the covert activities of a foreign adversary, specifically those aimed at acquiring sensitive information.[9] Simply put, counterintelligence is the business of catching spies and saboteurs. As such, it has always been a part of military operations. It was a concern of America's first Commander in Chief, and was present, to a greater or lesser extent, throughout almost the entire history of the U.S. military.[10] There is little in the way of a formal definition for the military counterintelligence function prior to the end of World War II. Counterintelligence efforts were carried out by military services in response to particular tactical needs. Military counterintelligence expanded in wartime and tended to wither away as hostilities ended.[11] Counterintelligence was also treated as a subset of the

---

9. The precise origin of the term "counterintelligence" is unclear, but it was certainly used as an established term during World War II. *See* Oxford English Dictionary (2nd Ed. 1989) (noting first uses of "counter-intelligence" in the 1940s). In U.S. usage, the word is not hyphenated. *See* Merriam-Webster's Online Dictionary, http://www.m-w.com/dictionary/counterintelligence.

10. Counterintelligence historians often cite a letter that George Washington wrote while commanding the Continental Army: "There is one evil I dread, that is their spies . . . ." *See, e.g.,* "One Evil" poster, Office of the National Counterintelligence Executive, *circa* 2001, *available at* http://www.ncix.gov/publications/posters/poster_one evil.html. An overview of U.S. counterintelligence history, particularly the history of military counterintelligence, can be found the NCIX's four-volume "Counterintelligence Reader," which was released under the Freedom of Information Act. *See* A Counterintelligence Reader (Frank J. Rafalko, ed.), *available at* http://www.fas.org/irp/ops/ci/docs/index.html.

11. *See* JOHN PATRICK FINNEGAN, MILITARY INTELLIGENCE (1998), *available at* http://www.history.army.mil/books/Lineage/MI/mi-fm.htm. This book provides a concise overview of the organizational history of military intelligence in the Army.

larger (and more permanent) discipline of military intelligence. During World War II, both the Army and the Navy created de facto counterintelligence groups within the Military Intelligence Service (MIS) and the Office of Naval Intelligence (ONI), respectively.[12] These entities had broad responsibilities that shifted as the war progressed. At various times, they were responsible not just for the detection of espionage and sabotage, but also for personnel security matters, counter-propaganda and subversion issues, censorship of military correspondence, and the like.[13] It is difficult to find a consistent definition of "counterintelligence" in the military context during this period; most attempts to define particular counterintelligence roles and missions centered on delineating and distinguishing between the responsibilities of Army MIS, ONI, and the FBI in geographic areas where they tended to collide.[14]

Military counterintelligence retained this general flavor in the postwar environment. In addition to its counter-espionage and counter-sabotage missions, military counterintelligence elements were also charged with the personnel security mission as well as with responsibility for investigating matters arising under the loyalty provisions of the new Internal Security Act.[15] In the Navy, and later in the Air Force, counterintelligence elements were also tasked with the investigation of major crimes involving military personnel.[16]

---

12. A Counterintelligence Reader, *supra* note 10.

13. *Id.* Counterintelligence operations occurred primarily in the Army, though the Office of Naval Intelligence developed counterintelligence functions as well during the pre-World War II period. *Id.*

14. During the war, the FBI and military authorities struggled to delineate responsibilities in civilian areas, such as the Panama Canal Zone and Hawaii, that were under some form of military control. *See id.* at http://www.fas.org/irp/ops/ci/docs/ci2/2ch1_b.htm#ciops.

15. The "loyalty" program for federal employees began in 1943. *See* Exec. Order No. 9300, 8 Fed. Reg. 1,701 (Feb. 5, 1943), and was expanded substantially in 1947. *See* Exec. Order No. 9835, 12 Fed. Reg. 1,935 (Mar. 21, 1947). The Internal Security Act of 1950, ch. 1024, 64 Stat. 987 (1950), and the Communist Control Act, ch. 886, 68 Stat. 775 (1954), further expanded demands on counterintelligence components to investigate "loyalty" matters.

16. What is now the Naval Criminal Investigative Service (NCIS) can trace its origins to the establishment in 1882 of the ONI. Then, as now, ONI was principally a maritime foreign-intelligence organization, although its responsibilities expanded during the World Wars to include responsibility for investigating espionage, sabotage, and subversion. In 1966, these latter functions became part of the Naval Investigative Service, which remained a subordinate organization of ONI. In 1982, NIS gained independent budget control, began reporting directly to the Chief of Naval Operations, and assumed responsibility for Navy law enforcement. The ultimate formal restructuring of NCIS into a federal law enforcement agency took place in 1992. NCIS History, Naval Criminal Investigative Service Homepage, http://www.ncis. navy.mil/about/ history.asp (last visited Jan. 31, 2008). On Aug. 1, 1948, less than a year after the establishment of an independent Air Force, and at the urging of Congress, Secretary of the Air Force Symington established the Air Force Office of Special Investigations (AFOSI). Secretary Symington intended to pattern AFOSI after the FBI and appointed FBI Special Agent Joseph Carroll as its first commander. AFOSI's stated primary

It is not our purpose here to rehearse the history of military domestic counterintelligence operations during the period preceding the Church/Pike investigations. However, we believe that several key characteristics can be attributed to this period and that these remain important to understanding the current state of affairs. First, military counterintelligence (and counterintelligence generally) operated under an expansive and imprecise definition. The National Security Act of 1947[17] did effect some basic organization of the intelligence (and presumably counterintelligence) function, but its emphasis was on structural organization. The original Act did not even define the key terms "intelligence" or "counterintelligence."[18] Executive orders and DoD regulations delineated functions for the counterintelligence components, but there was no coherent taxonomy of the intelligence/counter-intelligence function the national or the military level. The situation probably reflected the persistent influence of a still older view of counterintelligence as "spy-catching." The spies that military counterintelligence units were most concerned with catching would have been foreigners attempting to steal U.S. military secrets. These typically would be members of a foreign military organization or agents trained by such an organization. These spies would be either stealing military secrets themselves or would be recruiting U.S. military personnel (or those closely involved in supporting the military). The implication of this classic model was that the military counterintelligence mission did not typically involve much interaction with ordinary U.S. citizens. Unlike their FBI counterparts, military counterintelligence agents were not hunting spies in the general population; they were operating within the military environment, predominantly overseas (where the members of the U.S. military were most accessible to foreign agents). It is not too surprising then, in the absence of a demonstrated need, that the U.S. military entered the Vietnam era without robust internal regulation of intelligence and counterintelligence activities that might affect U.S. citizens. Military intelligence units conducted operations variously characterized as "counterintelligence," "domestic intelligence," "internal security," or "subversion" – all concepts understood in an historical context but not subject to rigorous definition or regulation. Indeed, uncertainty over the

---

responsibilities are criminal investigations and counterintelligence services. U.S. Air Force Fact Sheet, Air Force Office of Special Investigations, *available at* http://www.osi.Andrews.af.mil/library/factsheeets/factsheet.asp? id=4848.

17. National Security Act of 1947, Pub. L. No. 235-80, 61 Stat. 495 (codified as amended at 50 U.S.C. §§401 *et seq.* (2000 and Supp. IV 2004)).

18. *See id.* The definitions of "intelligence," "foreign intelligence," and "counterintelligence" were inserted in 1993. *See* Intelligence Authorization for Fiscal Year 1993, Pub. L. No. 102-496,§702, 106 Stat. 3180, 3188 (1992) (codified as amended at 50 U.S.C. §401a (2000 and Supp. IV 2004)).

precise limits of counterintelligence was one of the factors contributing to the abuses noted by the Church Committee.[19]

The second characteristic of this period was that counterintelligence was, whether by design or simply for lack of an alternative model, fully integrated into the military mission of the DoD. Counterintelligence operations were closely tied to actual military operations and were part of the standard military chain of command. For the most part, counterintelligence was treated as one of the basic military intelligence functions, and counterintelligence units were part of the military service (Army, Navy, and Air Force) chains of command. Oversight of counterintelligence activities, like the oversight of other military functions, was exercised first by military commanders and ultimately by the civilian Secretaries of the Army, Navy, and Air Force. The only significant exceptions to this rule were the Defense Intelligence Agency[20] and the National Security Agency,[21] which, though staffed and led by military personnel, fell outside the purview of any individual military service.

Our examination begins with the modern definitions of "counterintelligence," which were established just after the Church/Pike investigations. The key terms are finally defined in Executive Order 12,333, which President Reagan signed in 1981.[22]

---

19. *See* Final Report of the Select Committee on Governmental Operations with Respect to Intelligence Activities, 94th Cong. (1976) (Book II: Deficiencies in Control and Accountability), *available at* http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIcg.htm.

20. The Defense Intelligence Agency (DIA) is the DoD's primary producer and manager of foreign military intelligence. Secretary of Defense McNamara established DIA upon the recommendation of the Eisenhower-appointed Joint Study Group, in order to more effectively organize the Department's military intelligence activities. Secretary McNamara established DIA by directive, and the agency commenced operations on Oct. 1, 1961. Prior to the establishment of DIA, the three military departments acted independently to collect, produce, and disseminate intelligence for the use of the individual Services. *See* Introduction, History, Defense Intelligence Agency Homepage, http://www.dia.mil/history/40years/intro.html.

21. President Truman issued National Security Council Intelligence Directive No. 9, which resulted in the formation of the National Security Agency (NSA), effective Nov. 4, 1952. The NSA is the successor to the Armed Forces Security Agency, which was formed in 1949 as the organization responsible for coordination of communications intelligence and communications security within the National Military Establishment. The NSA formally established the Central Security Service (CSS) in 1972 to consolidate the efforts of the NSA and the cryptologic elements of the Military Services. The Director of the NSA also serves as the Chief of the CSS. The NSA/CSS missions are the exploitation of foreign signals intelligence and the protection of U.S. information systems. *See* Frequently Asked Questions – About NSA, National Security Agency Homepage, http://www.nsa.gov/about/about00018.cfm; Introduction to History, National Security Agency Homepage, http://www.nsa.gov/history/index.cfm.

22. Exec. Order No. 12,333, *supra* note 2, of course, was not the immediate result of the "investigative era." It was preceded by Exec. Order No.11,905, 41 Fed. Reg. 7,703 (Feb. 18, 1976) and Exec. Order No. 12036, 43 Fed. Reg. 3,674 (Jan. 24, 1978), which represented responses to the investigations by the Ford and Carter administrations, respectively. Exec.

Section 3.4 of the Order contained the following relevant definitions:

> (a) Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs. . . .
>
> (d) Foreign intelligence means information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities.
>
> (e) Intelligence activities means all activities that agencies within the Intelligence Community are authorized to conduct pursuant to this Order. . . .
>
> (i) United States person means a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the Unted States, except for a corporation directed and controlled by a foreign government or governments.

The Executive Order also broadly defines the functional roles for DoD counterintelligence activities. The military services are authorized to collect, produce, and disseminate military and military-related counterintelligence, which must be coordinated with the FBI inside the United States and with the CIA outside the United States.[23] The NSA is authorized to collect signals intelligence (commonly known as SIGINT),

---

Order 12,333, however, represents the post-Church stasis. The Order was amended only twice between 1981 and 2008, and neither amendment substantially affected the counterintelligence provisions. *See* Exec. Order No. 13,284, 68 Fed. Reg. 4,075 (Jan. 23, 2003) (inserting references to the newly created Department of Homeland Security) and Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004) (altering some aspects of Intelligence Community organization). In 2008, the Order was substantially amended by Executive Order 13,470, 73 Fed. Reg. 45,325 (July 30, 2008). While most of the 2008 revisions were organizational in nature and centered on the new roles and responsibilities of the Director of National Intelligence, some affected the definitions discussed in this section. *See id.* and *infra* note 23.

23. Exec. Order 12,333, *supra* note 2, at §1.12(d). The 2008 amendment relocates these provisions to §1.7(f). *See* Exec. Order 13,470 at §2. The requirements for Attorney General-approved procedures are now found in §1.3(b)(20)(C). *See id.* The coordination of domestic counterintelligence activities with the FBI occurs under the terms of a Delimitation Agreement signed in 1979. *See* Army Regulation 381-10, *U.S. Army Intelligence Activities* (July 1, 1984) at App. B, *available at* http://www.fas.org/irp/doddir/army/r381_10.pdf. This regulation was replaced by a newer version in 2007, but the 1984 version contains a brief excerpt of the 1979 Delimitation Agreement.

and may do so for counterintelligence purposes.[24] DIA is responsible for providing military intelligence to the Secretary of Defense and the Joint Chiefs of Staff and is specifically authorized to provide counterintelligence staff support as directed by the Joint Chiefs.[25]

Finally, the Executive Order, in Part 2, sets out the basic ground rules to be followed by all intelligence components. These rules give particular emphasis to the manner in which information concerning U.S. persons is collected, retained, and disseminated by intelligence components, and also regulate the use of specific intelligence techniques. The provisions of Part 2 of the Order are intended to be implemented through agency-specific guidelines that are issued by the agency head and countersigned by the Attorney General (to ensure that they adequately protect the rights of U.S. persons).[26] The DoD implemented Part 2 in 1982 by issuing Regulation 5240.1-R, titled "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons."[27] DoD 5240.1-R became, and still is, the foundational document for all DoD counterintelligence activities.[28]

The original Executive Order 12,333 definition of "counterintelligence" significantly affected the subsequent development of DoD counterintelligence components. The Order created a taxonomy for the intelligence world, one that was vigorously adopted within the DoD. For example, the version of the Order in effect from 1981 until 2008 set up foreign intelligence and counterintelligence as mutually exclusive subsets within the realm of regulated intelligence activities: the definition of "foreign intelligence" specifically excluded counterintelligence (except in the case of information relating to international terrorism).[29] This division

---

24. Exec. Order 12,333, *supra* note 2, at §1.12(b)(6), the same language is found at §1.7(c) after the 2008 amendments.

25. *Id.* at §1.12(a)(5) (1981), now found at §1.7(b).

26. *Id.* at §3.2, now found in §1.3(b)(20)(C).

27. U.S. Department of Defense Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons* (Dec. 1, 1982) [hereinafter DoD 5240.1-R], *available at* http://www.dtic.mil/whs/directives/corres/pdf/524001r.pdf.

28. Each of the military Services issues a regulation further implementing the provisions of DoD 5240.1-R for the components of that service. *See, e.g.*, Army Regulation 381-10, "U.S. Army Intelligence Activities," (May 3, 2007), *available at* http://www.fas.org/irp/doddir/army/ar381-10.pdf; Secretary of the Navy Instruction (SECNAVINST) 3820.3E, "Oversight of Intelligence Activities within the Department of the Navy" (Sept. 21, 2005), *available at* www.fas.org/irp/doddir/navy/secnavinst/index.html; and Air Force Instruction 14-104, "Oversight of Intelligence Activities" (Apr, 16, 2007), *available at* www.fas.org/irp/doddir/usaf/index.html.

29. As noted above, the 2008 amendment to the Order removed this mutual exclusivity. Curiously, when definitions of foreign intelligence and counterintelligence were finally inserted into the National Security Act in 1993, they took a slightly different form. In the current version of the National Security Act, foreign intelligence and counterintelligence are subsets of "intelligence" that clearly overlap. *See* 50 U.S.C. §401(a)(1), (2) (2004); *see also* Kristan J. Wheaton & Michael T. Beerbower, *Towards a New Definition of Intelligence,* 17

was particularly significant in the DoD context because the primary target of DoD intelligence operations was foreign militaries. The largest free-standing DoD intelligence organs (NSA and DIA) were overwhelmingly devoted either to collecting information on the military capabilities of our adversaries (i.e., military intelligence) or to intercepting foreign military communications (SIGINT).[30] Similarly, the primary focus of intelligence activities for the military services was the collection of tactical military intelligence (i.e., the disposition and capabilities of the enemy forces arrayed against U.S. Army, Navy, Air Force, and Marine forces). Military intelligence and SIGINT are both easily categorized as foreign intelligence functions. The taxonomy[31] of the Order separated the counterintelligence function from the predominant DoD intelligence activities.

Part 2 of Executive Order 12,333, and the implementing Procedures for Part 2 found in DoD 5240.1-R, actually create an incentive to deepen and institutionalize the foreign intelligence/counterintelligence divide. The protective oversight rules laid out in DoD 5240.1-R have two basic thrusts: first, they seek to limit the collection, retention, and dissemination of

---

STAN. L. & POL'Y. REV. 319 (2006). The disparity between the two definitions was the source of extensive (though not terribly consequential) debate, and is sometimes referenced in debates over the existence of parallel Title 10 and Title 50 intelligence authorities. While the 2008 amendment to Executive Order 12,333 substantially removes this anomaly, the question of non-Title 50 activities remains current. *See* Exec. Order 12,333 (as amended) at §1.3(b)(21) (referencing coordination of clandestine activities conducted outside of the Intelligence Community).

30. While the cryptologic organizations of the military Services remain part of their individual Services for administrative purposes, they are each subordinate activities of the Central Security Service for all SIGINT matters. As such, their efforts to "conduct collection, processing and other SIGINT operations" are performed as part of the National Security Agency as the unified organization for the national SIGINT mission. DoD Directive 5100.20, The National Security Agency and the Central Security Service §§2.2, 2.3, 5.3, 5.4, and 5.8 (Dec. 23, 1971, Incorporating Through Change 4, June 24, 1991), *available at* http://west.dtic.mil/whs/directives/corres/pdf/510020p.pdf.

31. A "taxonomy" is more than a definitional scheme; it is a hierarchical classification of things that typically reflects a set of underlying principles. The best known taxonomies are, or course, the classifications of organisms used by zoologist, biologists, and other natural scientists. Taxonomies have also been applied in the social sciences, in epistemology, and even in the field of intelligence analysis. *See*, *e.g.,* Rob Johnston, *Developing a Taxonomy of Intelligence Analysis Variables*, 47 STUDIES IN INTELLIGENCE, No. 3, 2003. We believe the term to be appropriate here because the definitional scheme created in the original Executive Order 12,333 and implemented throughout DoD by DoD 5240.1-R embodies certain principles or, more properly, assumptions about the nature of intelligence and counterintelligence. The taxonomy of intelligence is manifest in structures, organizational politics, and culture within the DoD intelligence community. In the case of DoD counterintelligence, the tension between the assumptions underlying the current taxonomy and the realities of the post-9/11 legal environment calls into question the adequacy of existing oversight mechanisms. The effects of the revised taxonomy in the 2008 version of Executive Order 12,333 may emerge over time, but are not discernable as of this writing. The new provisions of the Order still require extensive implementation, and likely will take some time to be reflected in organizational structure and operational policy.

information that specifically identifies U.S. persons;[32] and second, they regulate the application of certain intelligence techniques employed within the United States and outside the United States when targeting U.S. persons.[33] Most of these rules have very little application to a purely foreign intelligence operation. For example, the collection of foreign intelligence information within the United States by anything other than overt means[34] is limited to a narrow exception that specifically excludes collection for the purpose of acquiring information on the domestic activities of any U.S. person.[35] To the extent that foreign intelligence components acquire U.S. person information abroad, they are authorized to do so, provided that the information falls within defined categories that cover most of the foreseeable instances in which "U.S. person" information collected abroad would constitute foreign intelligence.[36] The collection techniques regulated by Procedures 5 through 10 occur primarily within the United States, and the extraterritorial application of them to U.S. persons would occur only in rare (and primarily counterintelligence-related) circumstances.[37] The upshot of this is that a DoD intelligence component that collects only foreign intelligence will have minimal interaction with intelligence oversight rules of DoD 5240.1-R, not because the component is ignoring the rules but because the activity of the component simply does not often fall within the scope of the regulation. It is therefore simpler to concentrate on the collection of foreign intelligence and avoid the complications posed by integrating counterintelligence, in which the most

32. DoD 5240.1-R is organized into 15 Procedures that roughly correspond to the sections of Part 2 of Exec. Order 12,333. There are procedures covering the collection (Procedure 2), retention (Procedure 3), and dissemination (Procedure 4) of U.S. person information.

33. The techniques are electronic surveillance (Procedure 5), concealed monitoring (Procedure 6), physical searches (Procedure 7), examination of mail (Procedure 8), physical surveillance (Procedure 9), and undisclosed participation in organizations (Procedure 10).

34. Overt means are defined in the Procedure as methods of collection whereby the source of the information being collected is advised, or is otherwise aware, that he is providing such information to the Department of Defense or a component thereof. DoD 5240.1-R Proc. 2 §C2.2.4.

35. *Id.* at §C2.5.

36. *Id.* at §C2.3.3. The categories are actually fairly broad, encompassing not just people "reasonably believed" to be agents of foreign powers, international terrorists or drug traffickers, U.S. person organizations controlled by a foreign power, and U.S. persons who are prisoners or targets of foreign activity, but also "corporations or other commercial organizations believed to have some relationship with foreign powers, organizations, or persons." *Id.* at §C2.3.3.5.

37. For example, Procedure 5 would govern the surveillance of a U.S. person espionage suspect abroad, such as an active duty military service member posted overseas. DoD's use of any of these procedures assumes that the target is someone within the jurisdiction of DoD – that is to say, is a target authorized for DoD counterintelligence pursuant to Executive Order 12,333. Overseas intelligence surveillance of an espionage suspect who was a civilian, or even a DoD contractor, would be a matter for the FBI. *See* Army Regulation 381-10, *supra* note 23, at App. B (excerpt from 1979 Delineation agreement explaining FBI jurisdiction over these counterintelligence matters).

problematic U.S. person issues are more commonly encountered. Furthermore, the taxonomy more clearly identifies counterintelligence with the most problematic behaviors identified by the Church/Pike investigations (surveillance of U.S. persons within the United States, domestic intelligence collection, mail opening etc.).[38] The DoD foreign intelligence establishment was thus motivated to have as little to do with counterintelligence as possible.

If foreign intelligence shares one common border with counterintelligence, law enforcement shares another. Obviously, the criminal justice system and counterintelligence stand in some sort of close relationship. Spies (and terrorists), when caught, may be prosecuted if they fall within the military or civilian jurisdiction of the United States.[39] In order to be successful, counterintelligence needs an effective mechanism to exercise the criminal law option of handing over an identified agent of a foreign power to the prosecutors. DoD 5240.1-R was drafted at a time when this meant handing the matter "over the wall." The then recent passage of the Foreign Intelligence Surveillance Act and the Fourth Circuit decision in the *Truong* case were feeding a culture of stricter separation between counterintelligence and law enforcement operations.[40] While this separation had not yet matured into the largely impermeable wall of the late 1990s, its influence was certainly beginning to be felt.[41] DoD 5240.1-R

---

38. An interesting exception to this is the NSA. One of the most extensive domestic surveillance programs identified by the Church Committee was the NSA's SHAMROCK program. *See* Final Report of the Select Committee on Governmental Operations with Respect to Intelligence Activities, 94th Cong. (1976) (Book II(B): The Overbreadth of Domestic Intelligence Activity), *available at* http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIcb.htm. Nonetheless, in the post-E.O. 12,333 years, the NSA managed to reconstruct itself as a purely foreign intelligence operation. Although this history is now obscured by the NSA's post-September 11 involvement in the Terrorist Surveillance Program, the agency in the 1980s and 1990s had been known for its extraordinarily conservative interpretations of the U.S. person restrictions in E.O. 12,333. *See* THE 9/11 COMMISSION REPORT, *supra* note 4, at 87-88.

39. Members of the military subject to the UCMJ can be prosecuted for espionage under 10 U.S.C. §906, and perhaps others provisions of the Code. *See* 10 U.S.C. §§877-934 (the Punitive Articles of the UCMJ). The reach of military jurisdiction in the form of trials by military commission, has, of course, been the subject of considerable discussion in the terrorism context. *See, e.g*., Hamdan v. Rumsfeld, 548 U.S. 557 (2006).

40. *See* United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980) (upholding a warrantless surveillance only so long as it was conducted primarily for foreign intelligence purposes), and David S. Kris, *The Rise and Fall of the FISA Wall, supra* note 4 (detailed description of the FISA "wall" and its effects). The idea of the "wall" was fully acknowledged in DoD legal circles. *See, e.g*., Louis A. Chiarella & Michael A. Newton, *So Judge, How Do I Get That FISA Warrant?: The Policy and Procedure for Conducting Electronic Surveillance*, ARMY LAW. (Oct. 1997), at 25 (overview by Army attorneys of the FISA process and "wall" requirements).

41. *See, e.g.,* Victoria Toensing, *Terrorists on Tap,* WALL ST. J., Jan. 19, 2006 (describing the effect of the FISA "wall" in a 1985 terrorism matter).

actually excludes from its regulation all DoD law enforcement operations.[42] When intelligence components establish reasonable belief that a crime has been committed, they are to refer the matter to a law enforcement entity, or, if they possess their own law enforcement authority, continue the investigation using law enforcement rules.[43] The distinction drawn here between counterintelligence and law enforcement is already problematic. Reasonable belief that a crime (typically espionage) has been committed is the standard for handing the matter over to law enforcement; reasonable belief that a person is conducting intelligence activities on behalf of a foreign power is the prerequisite set for the collection of U.S. data in a counterintelligence investigation.[44] Thus, it would appear that if one has already met the standard to start collecting information on a U.S. person in a counterintelligence investigation, one would have also met most (perhaps all) of the standard that requires the transfer of the matter to criminal investigators.

The first two assumptions are those referenced above – namely, that DoD foreign intelligence and counterintelligence activities can be separated into exclusive sets, as can DoD counterintelligence and law enforcement activities. These were not entirely unreasonable assumptions in 1982. At that point in history, our principal adversaries were traditionally organized states (the Soviet Union and its Warsaw Pact allies; the People's Republic of China; and rogue states such as North Korea, Iran, and Libya). The primary thrust of DoD foreign intelligence collection was to acquire information on the capabilities, structure, and communications of the militaries associated with each of these states. None of these military forces operated on U.S. soil, and any involvement of U.S. persons in their operations abroad would have been quite extraordinary. By targeting foreign military operations, DoD intelligence components could reasonably collect pure foreign intelligence, with very little risk of acquiring any U.S. person data at all. DoD counterintelligence, on the other hand, also had a clear target. The attempts by our adversaries covertly to acquire information about U.S. military capabilities were similarly focused. Defending against those covert activities involved specialized knowledge of the operational intelligence capabilities of an adversary (such as the identities and targets of foreign intelligence officers operating within the United States or with access to U.S. military facilities abroad) but did not otherwise require acquisition of the foreign intelligence information that was the principal concern of the greater part of the DoD intelligence apparatus. Counterintelligence was a niche specialty that, for good reason,

---

42. *See* DoD 5240.1-R, Proc. 1 §C1.1.3.

43. By this time (1982), the Navy and the Air Force counterintelligence functions were embedded in components that also had law enforcement responsibilities. In the Army, the counterintelligence and the law enforcement functions were assigned to separate components. *See supra* note 16.

44. *See* DoD 5240.1-R, Proc. 2 §C2.3.4.

was largely walled off from the larger DoD intelligence world. DoD counterintelligence agents had training separate from that of other intelligence officers, and, in the Air Force and Navy, were treated generally as not part of the service intelligence apparatus at all.[45]

The DoD counterintelligence and foreign intelligence functions had little to do with each other's business during this period, and the two disciplines developed distinct cultures. Counterintelligence became increasingly dominated by a law enforcement culture (although in the Army, Military Intelligence professionals commonly moved from job to job, back and forth between the two worlds). In the Navy and the Air Force, this was certainly because the counterintelligence function was lodged in larger law enforcement entities (NCIS and AFOSI). However, even in the Army, in those units where the counterintelligence function had its own separate organization, counterintelligence agents acquired the trappings of law enforcement: they carried badges and credentials, dressed in civilian clothing, and even had limited arrest powers.[46] Despite this cultural affinity, it remained the case that law enforcement and counterintelligence were distinguishable.[47] DoD 5240.1-R and the regulations that implemented it in each of the services clearly required that counterintelligence matters be referred to law enforcement once a certain quantum of information was reached.[48] Furthermore, the DoD role in the law enforcement/criminal prosecution phase of any counterintelligence matter was actually fairly limited. Executive Order 12,333 gave the FBI primary jurisdiction over counterintelligence within the United States by requiring the DoD to conduct its counterintelligence operations within the United States in coordination with the FBI.[49] This coordination was

45. *See supra* note 16 (describing the origins of the counterintelligence function in NCIS and AFOSI, as distinct from the foreign intelligence function of each service). By contrast, Army counterintelligence is incorporated into its foreign intelligence components – at the strategic level, under the United States Army Intelligence and Security Command (INSCOM). Among the previously existing Army intelligence organizations consolidated to form INSCOM on Jan. 1, 1977, was the U.S. Army Intelligence Agency, which performed both HUMINT and counterintelligence missions. The 902nd Military Intelligence Group is the principal INSCOM subordinate command conducting counterintelligence activities. *See* The INSCOM Story, INSCOM Homepage, http://www.inscom.army.mil/Organization/History.aspx; Major Subordinate Commands, INSCOM Homepage, http://www.inscom.army.mil/MSC/Default902nd.aspx.

46. *See* Army Regulation 381-20, *The Army Counterintelligence Program* (Nov. 15, 1993) §§8-5 (civilian clothing), 8-12 (apprehension authority), 8-13 (search and seizure authority), and 9-1 through 9-9 (badge and credential program).

47. In the pre-USA PATRIOT Act world, this distinction was driven primarily by the legal notion of the "wall" between intelligence and law enforcement activities. *See supra* notes 4 and 40.

48. *See* DoD 5240.1-R, Proc. 4 §C4.2.2.2, and DoDI 5240.4, "Reporting of Counterintelligence and Criminal Violations" (Sept. 22, 1992). *See, e.g.*, Army Regulation 381-10 (May 3, 2007), at §§16-1 to 16-4.

49. Exec. Order 12,333 §1.11(d) (1981 version).

formalized in a 1979 agreement between the FBI and the DoD on the conduct of counterintelligence. The full text of the agreement has never been released publicly, but external references imply that it gives the FBI primary jurisdiction over many DoD counterintelligence matters and right of first refusal over much of the remainder.[50] The circumstances under which an espionage matter can be investigated, tried, and prosecuted entirely within the confines of DoD are fairly rare.[51] Thus, in many DoD counterintelligence matters, the point at which the case is referred to the FBI was also the effective point of transition from counterintelligence to law enforcement.[52]

DoD 5240.1-R also institutionalized far more basic assumptions that shaped DoD counterintelligence. The ability to identify what is and what is not "U.S. person" information is a prerequisite to the legal analysis of any counterintelligence question under this regulation. The definition of "U.S. person" and, more important, the presumptions to be employed in cases of doubt, presuppose physical encounters that can be accurately pinned to a map. The "U.S. person" definition provided in Procedure 1, for example, states that a person or organization outside the United States shall be "presumed not to be a United States person unless specific information to the contrary is obtained."[53] The corollary that a person or organization encountered within the United States was presumed to be a U.S. person (unless known to be an alien) was also established.[54] Neither DoD 5240.1-R nor any of the implementing regulations, however, give any guidance on how to determine the legal location of the person when the encounter is non-physical. DoD 5240.1-R embodies an "analog" understanding of the world; it assumes that communications proceed from origin to destination along a logical path that can be determined and reflects geography. At the

---

50. *See supra* note 23.

51. Essentially, this situation occurs only when the subject of the investigation is an active duty military service member who is eventually charged under the Uniform Code of Military Justice. Even when these circumstances apply, the cases are sometimes still handed to the FBI to enable prosecution in the civilian courts. This is particularly true in cases involving electronic surveillance subsequent to the passage of FISA. The use of FISA information is well established in the federal courts. *See, e.g.,* United States v. Squillacote, 221 F.3d 542 (4th Cir. 2000), *cert. denied,* 532 U.S. 971 (2001); United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987), *cert. denied,* 486 U.S. 1010 (1988); United States v. Badia, 827 F.2d 1458 (11th Cir. 1987), *cert. denied*, 485 U.S. 937 (1988). But the use of FISA information presents some procedural challenges when used in the military courts. *See* United States v. Ott, 637 F. Supp. 62 (E.D. Cal. 1986) (noting that federal courts have exclusive jurisdiction to rule on the legality of a FISA surveillance, so that such a question arising in a court martial would be properly transferred to the U.S. district court with jurisdiction over the site of the court martial) .

52. Despite the fact that the FBI is both a law enforcement organization and a component of the Intelligence Community, DoD references tend to focus predominantly on its law enforcement identity.

53. DoD 5240.1-R, Definitions at §DL1.1.25.2.

54. *Id.*

time the regulation was written, a telephone call that originated from a 202 area code must have been made in the United States, particularly within the Washington D.C. area. The advent first of cellular phones and then of fully digital telephony collapsed that assumption. Email, which existed only in limited form in 1982, renders geographical assumptions about electronic communications almost entirely irrelevant.[55]

DoD 5240.1-R also assumes that the overall paradigm for DoD counterintelligence is investigative. In other words, counterintelligence is viewed as the business of gathering information to identify and prosecute known (or semi-known) individuals who are acting as the agents of foreign powers. Procedure 2 authorizes the following under the heading of counterintelligence:

> C2.3.4. Information may be collected about a United States person if the information constitutes counterintelligence, provided the intentional collection of counterintelligence about United States persons must be limited to:
>
> C2.3.4.1. Persons who are reasonably believed to be engaged in, or about to engage in, intelligence activities on behalf of a foreign power, or international terrorist activities.
>
> C2.3.4.2. Persons in contact with persons described in subparagraph C2.3.4.1., above, for the purpose of identifying such person and assessing their relationship with persons described in subparagraph C2.3.4.1., above.

Here again, the assumption is appropriate to the era in which it was written. In 1982, spy hunting was the quintessential counterintelligence activity. An espionage case typically started with a reasonably specific lead or anomaly that indicated a successful recruitment by a foreign agent of some person who had access to sensitive information. The work of the DoD counterintelligence agent was to build the case identifying that person and the secrets he or she had compromised. While this exercise sometimes involved isolating the identity of the suspect by analyzing data reflecting who had access to the compromised information, this was typically a

---

55. The language of DoD 5240.1-R still exerts an influence over this question. The military services have all revised their implementing regulations of 5240.1-R in recent years, *see supra* note 28, yet none of the newer regulations resolves the substance of this issue. The Army, for example, adds an "Internet Considerations" section to its regulation, but only addresses the question of when non-content header information (like IP addresses, URLs, and email addresses) may be collected. *See* Army Reg. 381-10, §1-9 (2007). The situation here is certainly not that the military services are unaware of the issue; rather it reflects their lack of authority to alter the language of DoD 5240.1-R. *See* DoD 5240.1-R, Proc. 1 §C1.5 (Amendment requires approval of the Secretary of Defense, and perhaps also the Attorney General). Our point is that the problem is not one of interpretation, but rather one that arises from the taxonomy itself. It cannot be fixed without revisiting the underlying assumptions of the regulation.

limited exercise (since the information at issue was always classified, those with access were, by definition, a substantially restricted subgroup of the general population). What counterintelligence did not generally do was engage in the broad collection and analysis of data in search of potentially relevant leads. That was a foreign intelligence paradigm that, as explained above, did not generally need to accommodate concerns about U.S. person information. During this period (the 1980s and 1990s), DoD counterintelligence did encompass some noninvestigative functions, such as counterintelligence analysis and counterintelligence collections. These, however, were narrowly defined and generally functioned as adjuncts to either the investigative or the foreign intelligence process.[56]

The retention (Procedure 3) and dissemination (Procedure 4) rules for U.S. person data similarly reflect the investigative paradigm in that they assume the quantities of collected U.S. person data will be limited enough to enable individualized assessment of the justification to retain or disseminate U.S. person data.[57] The language of Procedure 3, for example, is meant to apply only to data that has already been organized to allow retrieval by the U.S. person's name or identifying data.[58] The authors of the Procedure no doubt had in mind a physical file on the individual or the retention of the individual's information in a form that was indexed by name. Current technology enables such retrieval from virtually all textual material and thus makes the Procedure broadly applicable. One then has to either come up with a workable scheme for conducting the assessments required by Procedure 3 C3.3.2 on large bodies of otherwise

56. Counterintelligence analysis concentrates on the preparation of finished analytical products on topics related to the investigative process. For example, analysts might prepare products summarizing the tradecraft and capabilities of foreign intelligence officers targeting DoD assets, or might summarize what had been learned from recent espionage cases or offensive counterintelligence operations. These products could then be disseminated through the mechanisms of the military intelligence community in a process largely supervised by the DIA. The DIA also managed the collections process. *See* Commission on the Roles and Capabilities of the United States Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (Mar. 1, 1996) at 112, *available at* http://www.access.gpo.gov/intelligence/int/pdf/int014.pdf. This process involves setting a collection requirement against which operational units could respond with any relevant information they were encountering. Such information was recorded in an Intelligence Information Report (IIR) and was then uploaded into the general foreign intelligence databases. A counterintelligence collection requirement might involve, for example, a request to report on the types of covert communication techniques that a particular country's intelligence officers were using. Conversely, a counterintelligence component might seek a requirement that foreign intelligence components report on technologies that were of special interest (and thus likely espionage targets) of a particular foreign country. Collection, reporting, and analysis form a circular process that is often referred to as the Intelligence Cycle. *See, e.g.*, "The Intelligence Process" as explained on the United States Intelligence Community website at http://www.intelligence.gov/2-business.shtml.

57. *See* DoD 5240.1-R, Proc. 3 (retention) & Proc. 4 (dissemination).

58. DoD 5240.1-R, Proc. 3 §C3.2.

undifferentiated data or decide that such types of data simply cannot be retained if they pose the threat of containing any U.S. person information.[59]

In summary, then, the legal taxonomy and regulatory scheme that followed the Church/Pike period outlined the contours of DoD counterintelligence. Counterintelligence was distinct from the dominant DoD intelligence genre, foreign/military intelligence. Counterintelligence was the discipline most closely identified with potentially troublesome interactions between DoD and U.S. persons. As such, counterintelligence was subject to strict regulation of its information collection and investigative methods by DoD 5240.1-R. That regulation, however, assumed that counterintelligence was largely an investigative discipline that would acquire information in a limited and targeted way to identify agents of foreign powers. The regulations also assumed that the information collected typically would have physical or "analog" qualities that enabled easy categorization and control. As a matter of law and policy, counterintelligence was distinct from law enforcement and, conversely, DoD law enforcement components did not exercise an intelligence function.

II. COUNTERINTELLIGENCE IN THE U.S. MILITARY STRUCTURE

To the extent that DoD counterintelligence is viewed as a unitary set of missions, functions, and resources, it is a relic of the pre-1986 U.S. military establishment. Contrary to a fundamental organizing principle of the DoD – unity of command and unity of effort[60] – the activities of DoD counterintelligence remain largely under the control of the individual military departments. Lacking common direction and with no binding mechanism for interservice coordination, DoD counterintelligence has resisted the post-World War II trend toward unified command and control.

This trend has been marked by a series of significant – if incremental – statutory, executive, and administrative measures designed to streamline and strengthen the application of U.S. military force. Legislative measures began with the National Security Act of 1947, which was "to provide for the effective strategic direction of the armed forces and for their operation under unified control for their integration into an efficient team of land, naval, and air forces."[61] The 1947 Act made many changes to the national

59. The implementing regulations follow the model of individualized assessment. *See* SECNAVINST 3820.3E at para. 5 (implementing DoD 5240.1-R and Exec. Order 12,333 requirements without modification); Air Force Instr. 14-104 §11.3; and Army Reg. 381-10 §§3-1 to 3-3. The Army regulations, for example, impose an annual review of all intelligence files and databases for identifiable U.S. person information, which must then be assessed to determine whether retention is still necessary to an assigned function. *Id*. at §3.3(c).

60. Joint Staff Director for Operational Plans and Joint Force Development, Joint Publication 1, Doctrine for the Armed Forces of the United States, at xv (May 2, 2007).

61. Pub. L. No. 80-235, 61 Stat. 495 §2 (1947) (codified at 50 U.S.C. §401). For a

security apparatus, including combining the Department of War and the Department of the Navy into a single National Military Establishment under a Secretary of Defense.[62]

The Act has been amended numerous times in order to further refine the structure of the DoD and enable unified command-and-control of operating forces. In the early 1980s, the congressional Armed Services committees determined the existing statutory structure (which included significant amendments to the National Security Act made in 1949, 1953, and 1958) to be inadequate. The Department of Defense Reform Act of 1958, in particular, and at President Eisenhower's urging, strengthened the status of the combatant commands (then and now, the principal organizational construct for joint military planning and operations) and put in place the structure that continues to characterize the U.S. military's operational configuration. However, those examining the issue a quarter century later noted continuing command-and-control problems.

Although the 1947 National Security Act, as amended, was intended to emphasize and bolster the ability of the Department to act jointly, the continued institutional power of the individual military Services, along with weak joint structures, tended to frustrate that intent. A 1985 Senate Armed Services Committee Staff Report (known generally as the Locher Report) stated, "The operational deficiencies evident during the Vietnam War, the seizure of the *Pueblo*, the Iranian hostage rescue mission, and the incursion into Grenada were the result of the failure to adequately implement the concept of unified command."[63] Among the problems leading to that failure was "the imbalance between Service and joint interests."[64]

The ensuing legislative response, the 1986 Goldwater-Nichols Department of Defense Reorganization Act,[65] did not impose a new or radical vision of a joint military structure to replace the Service-dominated structure. Fundamentally, though, it did impose a firm statutory mandate to fulfill President Eisenhower's 1958 vision of unified command. The Goldwater-Nichols Act put in place an enduring arrangement in which joint institutions were strengthened and Service power was specifically limited.

---

comprehensive overview of defense reform in the latter half of the twentieth century, *see generally* Peter M. Murphy & William M. Koenig, *Whither Goldwater-Nichols?,* 43 NAVAL L. REV. 183 (1996).

62. As originally enacted, the National Security Act of 1947 also created the National Security Council, the Central Intelligence Agency, a separate Department of the Air Force, and statutory charters for the functions of each of the military Services. *See* J. Moore & R. Turner, The Legal Structure of Defense Organization, Memorandum Prepared for the President's Blue Ribbon Commission on Defense Management, Jan. 15, 1986, at 15-16 [hereinafter the Packard Commission Memorandum].

63. Staff of Senate Comm. on the Armed Services, Defense Organization: The Need for Change, S. Prt. No. 86, 99th Cong., 1st Sess. (Oct. 16, 1985) [hereinafter Locher Report] at 7.

64. *Id*. at 3.

65. Pub. L. No. 99-433, 100 Stat. 994.

The statutory changes established clearly that operational matters are the province of joint organizations (principally, the combatant commands), while administrative matters are the proper role of the individual Services.

Until Goldwater-Nichols, "the principal ongoing ambiguity in the operational chain of command seemed to be the precise differentiation of operational and administrative functions . . . ."[66] With the passage of Goldwater-Nichols, that ambiguity was largely eliminated, with detailed clarification as to what constituted those "administrative" functions reserved to the Services.[67]

Some ambiguity remains, however. The functions of the DoD counterintelligence organizations, for example, include both administrative and operational aspects,[68] and the present statutory underpinnings of the Department, as embodied in Title 10 of the United States Code, offer little clarity as to whether the resources and activities, in whole or in part, of the Service counterintelligence organizations should properly be controlled by the Services or by a joint or Departmental entity (or entities). Under Goldwater-Nichols, the definitive shift of control of military operations from the individual Services to joint commanders did not, in effect, include the operational activities of the DoD counterintelligence organizations. Neither did it clearly exclude those activities.

While it is generally accepted that counterintelligence remains a common function and an independent Title 10 responsibility of the individual military departments,[69] the text of Title 10 is far from clear on the matter. 10 U.S.C. §162 states that, with particular exceptions, "the Secretaries of the military departments shall assign *all forces* under their jurisdiction to unified and specified combatant commands . . . to perform missions assigned to those commands."[70] But personnel conducting counterintelligence activities for the military departments typically are not

66. Packard Commission Memorandum, *supra* note 62, at 34.

67. *See* 10 U.S.C. §§162, 3013, 5013, and 8013.

68. The "five functions" of DoD counterintelligence are commonly identified as Operations; Collections; Investigations; Analysis & Production; and Functional Services. *See* DoD Directive 5240.2, Department of Defense Counterintelligence (CI) §5.2 (May 22, 1997); SECNAV Instruction 3850.2C, Department of the Navy Counterintelligence §4(b) (July 20, 2005); and DoD Instruction 5240.16, DoD Counterintelligence Functional Services §6.2.4 (May 21, 2005). Operations and Collections may be seen to be, of course, operational in nature, with implications likely to transcend the interests of the particular Service conducting the activity. Functional Services (defined as "CI activities that support other intelligence or DoD operational activities, providing specialized defensive CI services to identify and counter terrorism, espionage, sabotage and related activities of foreign intelligence services" *Id.* §E1.1.3.), and Analysis & Production, in any particular instance, may pertain strictly to the accomplishing Service or may have broader joint or Departmental applicability. Only the investigative function tends to be Service-centric in most cases.

69. DoD Directive 5100.1, Functions of the Department of Defense and Its Major Components §6.4.3 (Aug. 1, 2002).

70. 10 U.S.C. §162 (a)(1) (emphasis added).

so assigned. The clearly stated statutory exceptions to this general principle of "all forces" being assigned to the combatant commanders are those "forces assigned to carry out the functions of the Secretary of a military department listed in sections 3013(b), 5013(b), and 8013(b)" of Title 10. These sections delineate the particular responsibilities of the Secretaries of the Army, Navy, and Air Force, respectively, in conducting the affairs of their departments – administrative responsibilities commonly described as "organize, train, and equip."[71]

However, Service counterintelligence Title 10 responsibilities are understood to derive not from these paragraphs – which are intended specifically to exclude certain forces necessary for the maintenance of a Service from assignment to the combatant commands – but in the paragraphs immediately following. 10 U.S.C. §§3013*(c)*, 5013*(c)*, and 8013*(c)* (emphasis added), state that each Service secretary "is also responsible for . . . the effective supervision and control of the intelligence activities" of his or her Department.[72] What these provisions do *not* state specifically (besides whether or not counterintelligence activities are a subset of "intelligence activities"[73]) is that the personnel conducting those activities are to be excluded from the §162 requirement for forces to be assigned to combatant commands.[74]

What we have, then, whether by design, interpretation, assumption, or acquiescence, are military department counterintelligence organizations conducting military activities – including operations – outside of the joint military command-and-control apparatus that has evolved over the past six decades and which was conclusively confirmed in law over twenty years ago.

Although a mechanism for interservice cross-cueing is highly desirable (the intelligence activities of a foreign power are unlikely to confine their focus to a single uniformed Service or particular Defense agency), unified command-and-control are generally not necessary. One might argue, though, that unified command-and-control is critical for the efficient and effective *operational* employment of DoD counterintelligence resources to counter the efforts of foreign intelligence services or terrorist entities.

---

71. A. Barrett, *Empowering Eisenhower's Concept*, JOINT FORCES QTLY., Autumn 1996, at 13.

72. 10 U.S.C. §§3013(c)(7), 5013(c)(7), and 8013(c)(7).

73. Although the language in 10 U.S.C. §§3013(c), 5013(c), and 8013(c) was inserted in 1986, as noted in note 17, a 1993 amendment codified in Title 50 *does* define "counterintelligence" as a subset of intelligence. *See* 50 U.S.C. §401a(1).

74. However, as is common throughout Title 10, §162 provides for considerable organizational flexibility with the provision "Except as otherwise directed by the Secretary of Defense. . . ." 10 U.S.C. §162(2). In the case of counterintelligence, the Secretary, arguably, has so directed in DoD Directive 5100.1, §6.4.3, where the responsibility to "provide adequate, timely, and reliable intelligence and counterintelligence for the Military Department and other Agencies as directed by competent authority" is identified as one of the "Common Functions of the Military Departments."

Since 1986, the United States has applied military power (in the commonly understood sense of bullets fired, bombs dropped, missiles launched, peacekeepers deployed, humanitarian relief delivered, and so forth) under unambiguous joint command. However, unless done specifically pursuant to the execution of a military operation plan wherein the joint force commander is assigned operational control of supporting DoD counterintelligence elements, DoD counterintelligence operations are executed only *in coordination with*, and *not* under the command-and-control of, a joint commander.[75]

In 1985, the Locher Report noted that "mission integration" is "the principal organizational goal of DoD."[76] In the period preceding the terrorist attacks of September 11, 2001, DoD counterintelligence was a "community" lacking in "mission integration." In the groundswell of introspection that followed the attacks, and as the entire national security apparatus experienced fresh scrutiny, the DoD recognized in its counterintelligence activities a general lack of central coordination, control, and deconfliction. In the following years, the Department took steps to provide at least a measure of central management, although those steps represent, in themselves, a departure from orthodox "jointness."[77]

III. EVOLUTION OF DOD COUNTERINTELLIGENCE IN THE POST-9/11 ENVIRONMENT

The legal, political, and operational changes that occurred as a result of the attacks of September 11, 2001, had a profound impact on the nature of DoD intelligence operations. Some have been (unintentionally, from the perspective of the government) high-profile: the September 11 attacks obviously brought substantial changes in the collection rules[78] of the NSA.[79]

---

75. DoD Directive 5240.2 § 4.6.

76. "Mission integration" is defined as "the integration of the distinct military capabilities of the four Services to prepare for and conduct effective unified operations in fulfilling major U.S. military missions." Locher Report, *supra* note 63, at 2.

77. *See*, in particular, our discussion of the DoD Counterintelligence Field Activity, beginning *infra* at the accompanying text to note 151.

78. Although the details of the changes remain unknown, it is a fair assumption that the initial "Terrorist Surveillance Program" (TSP) involved some temporary exceptions or revisions to United States Signals Intelligence Directive 18 (USSID 18), the document that, for the NSA and the signals intelligence world, implements Executive Order 12,333 and DoD 5240.1-R. The basic text of the 1993 version of USSID 18 has been publicly available for some time. USSID 18 and a number of other NSA documents are available on the National Security Archive website. *See* National Security Archive Electronic Briefing Book No. 24, "The National Security Agency Declassified" (Jan. 13, 2000) http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index2.html#doc7. The basic text of USSID 18 simply incorporates the familiar provisions of Exec. Order 12,333 and DoD 5240.1-R. However, the document contains references to multiple annexes, many of which remain classified. *See id.* It is also unclear whether the publicly available 1993 version of USSID

Others, such as those relating to counterintelligence, have been less noticed, though they affect some of the fundamental assumptions behind the oversight of counterintelligence activities. Specifically, significant shifts occurred on both the foreign intelligence and law enforcement borders of counterintelligence.

On the foreign intelligence side, the shift was the result of an international terrorist entity taking center stage as the principal military adversary of the United States. The pursuit of al Qaeda and the global war on terrorism essentially brought about a reversal of the traditional division of labor between the military/foreign intelligence community and the counterintelligence/law enforcement community. As discussed above, the pre-9/11 model was based on the assumption that the principal job of the military (and its foreign/military intelligence components) was to deal with the overt military components of the foreign powers arrayed against us. The pre-9/11 world view, of course, encompassed the reality that foreign powers also had components that operated against us covertly: spies and saboteurs that typically used the civilian population as their operating environment. Dealing with these covert operatives was the province of counterintelligence.[80] International terrorist groups were lumped together with other covert foreign power activities because of the similarity in tactics (operation of covert cells in the civilian population) and identification with sabotage (a traditional concern of counterintelligence).[81] Another way of

---

18 is the version currently in force.

79. Some of the public statements made by NSA officials when explaining the TSP also nicely illustrate isolation of the DoD foreign intelligence establishment from the counterintelligence world, in which collection of U.S. person information is more common. Some of these statements have rather broadly overstated the limits on domestic collection imposed by E.O. 12,333 and the Foreign Intelligence Surveillance Act. *See, e.g.,* Hon. J. Michael McConnell, Remarks and Q&A by the Director of National Intelligence, delivered at the 2007 Excellence in Government Conference (April 4, 2007) ("So if the intelligence community is tracking someone suspected of terrorism and they arrive in this country in a legal status, they're now off limits to the intelligence community. Switch to law enforcement. The rules and regulations on law enforcement are much more stringent with regard to conducting surveillance of either U.S. citizens or U.S. persons. So the terrorists that came here and operated here prior to 9/11, so long as they were here legally and so long as they did not break the law, they were mostly invisible to us.") (transcript available at http://www.dni.gov/speeches/20070404_speech.pdf).

80. Strictly speaking, offensive operations – finding and neutralizing these covert operatives – were the responsibility of counterintelligence. Force protection and personnel security components had defensive roles. Such nomenclature is confusing, however, because inside the DoD the term "offensive counterintelligence" or "OFCO" refers to a specific sub-discipline of counterintelligence, the specific description of which remains classified. *See* http://www.dtic.mil/whs/directives/corres/html/524009.htm (a page on the DoD publications website documenting the existence of a classified instruction, DoDI 5240.9 "Support to the Department of Defense Offensive Counterintelligence Operations (U)" (Nov. 28, 1989)).

81. However, even the 1982 definitions recognized that international terrorism was somehow different. It is the one recognized exception to the otherwise exclusive definitions of counterintelligence and foreign intelligence. *See* Exec. Order 12,333 at §3.4(d) (1981)

expressing the pre-9/11 view would be to say that a vast preponderance of the DoD military and intelligence apparatus was oriented toward the overt, conventional operations of foreign state adversaries, while a small, walled-off corner of the apparatus was oriented toward the purely covert activities of foreign adversaries. The division was not absolute, of course. Since at least the Vietnam era, the military had given serious attention to counterinsurgency operations, and had therefore addressed terrorism in the context of force protection. However, counterinsurgency typically presupposed an irregular adversary operating in a foreign environment, not one that sought targets inside the U.S. homeland.[82]

Following the 9/11 attacks, the division of labor changed substantially.[83] The immediate imperatives for the DoD became the protection of the homeland from additional attacks by covert al Qaeda cells of international terrorists and the prosecution of a global war on terrorism against the widely dispersed al Qaeda elements. The first of these imperatives, which came to be characterized in the DoD as the "homeland defense" mission, meant the conduct of fairly extensive military operations within the United States. These operations, the most visible of which were the combat air patrols maintained over major urban areas and the use of troops to secure airports, would eventually lead to the creation of a new combatant command intended to operate within the United States.[84] Some aspects of these homeland defense operations were noncontroversial. Who else but the military could fly combat air patrols over U.S. cities? Some elements of

---

and DoD 5240.1-R at DL1.1.11 (both defining "foreign intelligence" as "not including counterintelligence except for information on international terrorist activities").

82. The Department of Defense defines "counterinsurgency" as "[t]hose military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat insurgency." Joint Staff Director for Operational Plans and Joint Force Development (J-7), Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms (Apr. 12, 2001, as amended through Oct. 17, 2007) at 128, *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf. "Counterterrorism" carries a much more specific connotation: "Operations that include offensive measures taken to prevent, deter, preempt, and respond to terrorism." *Id.* at 130.

83. There had been some shift in priorities even prior to 9/11, as the military recognized the growing threat of international terrorists. In particular, international terrorism was clearly a significant focus of the U.S. Special Operations Command (USSOCOM) throughout the 1990s. *See* Department of Defense Inspector General, Report of Investigation H05L97905217, "Alleged Misconduct by Senior DOD Officials Concerning the ABLE DANGER Program and Lieutenant Colonel Anthony A. Shaffer, U.S. Army Reserve" (Sept. 18, 2006), at 6-15 (summarizing USSOCOM anti-terrorism analytical project), *available at* http://www.dodig.mil/fo/foia/ERR/r_H05L97905217-PWH.pdf. The successful 9/11 attacks entailed an almost exponential acceleration of this process, particularly among the conventional military forces.

84. Northern Command (NORTHCOM) was established on October 1, 2002, with the mission of anticipating and conducting Homeland Defense and Civil Support operations to defend, protect, and secure the United States and its interests. About U.S. Northern Command, USNORTHCOM Homepage, http://www.northcom.mil/About/index.html.

the DoD's U.S. operations fit within the traditional model of military assistance to civilian authorities.[85] Other aspects of the DoD role raised significant issues about the domestic operations of DoD components. If defense against terrorism was now militarized, what role did civilian law enforcement and the civilian counterintelligence parts of the FBI play in this defense, and where were the demarcation lines? Did the fact that our military adversary (al Qaeda) sought as one of its principal aims to develop the capability to attack targets within the United States mean that DoD intelligence components should begin collecting information on al Qaeda's activities within the United States? Since DoD counterintelligence components were authorized to conduct counterintelligence in support of military activities, would they now have a greater domestic role? Did the traditional oversight and coordination mechanisms for DoD counterintelligence allow it to support the military's homeland defense function?

DoD counterintelligence components encountered these questions in an increasingly chaotic environment that was characterized by, among other things, weakened connections to the underlying (but still unaltered) taxonomy of intelligence functions. A good example of this was the reality, outside the DoD, of a growing separation between counterintelligence and counterterrorism operations. Although the legal definition of "counterintelligence" remained unchanged and continued to encompass both traditional foreign powers and international terrorist groups, the FBI and CIA began to use the term "counterintelligence" to refer exclusively to the operations aimed at foreign state actors (i.e., traditional espionage) and the term "counterterrorism" to refer to operations aimed at international terrorists. The FBI structurally bifurcated its counterintelligence and counterterrorism functions by creating a separate Counterterrorism Division. The FBI and other government agencies later coordinated their counterterrorism efforts in the National Counterterrorism Center (NCTC).[86] As a result, the rump counterintelligence components in each organization focused more exclusively on traditional counterintelligence targets like espionage and foreign intelligence services. A similar movement was occurring at the national level. The National Counterintelligence Executive (NCIX) was created by presidential directive on December 28, 2000[87] and

85. The military has always been able to provide limited assistance to civilian authorities in times of crisis. These circumstances are codified at 10 U.S.C. §§331-335 (The Insurrection Act) and are statutory exceptions to the Posse Comitatus Act (18 U.S.C §1385), which generally prohibits the military from taking on domestic law enforcement functions. Under its charter, NORTHCOM is responsible for coordinating military assistance to civilian authorities. *See supra* note 84.

86. This bifurcation is reflected in the current organization of the FBI's National Security Branch. *See* Federal Bureau of Investigation, National Security Branch Overview (2006), *available at* http://www.fbi.gov/hq/nsb/whitepaper12-06/white paper.htm.

87. *See* Fact Sheet, "The PDD on CI-21: Counterintelligence for the 21st Century" (Jan. 5, 2001), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-75.htm.

was later established by statute[88] to coordinate all U.S. counterintelligence activities.[89] After a decidedly rocky start,[90] the Office of the NCIX (ONCIX) began to develop national counterintelligence policy and even promoted a revised definition of "counterintelligence."[91] The ONCIX does not appear to have asserted any role in the coordination of counterterrorism policy; it chose instead to take the view that counterintelligence was to be concerned only with the intelligence gathering activities of international terrorist groups.[92] NCIX policy documents are clearly oriented toward

---

88. The Counterintelligence Enhancement Act of 2002, Pub. L. No. 107-306 §§902-904, 116 Stat. 2383, 2434-2437 (2002) codified at 50 U.S.C. §§402(b)-(c) (as amended).

89. The NCIX was the latest in a series of efforts to better coordinate U.S. counterintelligence activities. It arose out of a study effort known as CI-21, which examined the need for better organization of counterintelligence activities in the post-Cold War era. An almost identical exercise occurred in the mid-1990s following the Aldrich Ames espionage case and resulted in the creation of the National Counterintelligence Center (NACIC), which was the entity that the NCIX replaced. The National Counterintelligence Center replaced another coordinating body that the FBI, CIA, and DoD had established following the "Year of the Spy" (1985, a year in which a series of significant espionage cases emerged). *See generally* David M. Crane, *Divided We Stand: Counterintelligence Coordination Within the Intelligence Community of the United States,* 1995-DEC ARMY LAW. 26 (1995) (historical overview of coordination issues). Neither the NCIX nor the NACIC, nor any of their predecessor entities held any significant operational authority over the agencies that actually conduct counterintelligence operations (FBI, CIA and DoD). The role of the NCIX is limited to community functions like education and outreach, budget development, policy writing, and coordination. In 2004 the NCIX was integrated into the Office of the Director of National Intelligence. *See generally* COMMISSION ON THE INTELLIGENCE CAPABILITIES OF THE UNITED STATES REGARDING WEAPONS OF MASS DESTRUCTION, REPORT TO THE PRESIDENT OF THE UNITED STATES 485-492 (2005) [hereinafter WMD COMMISSION REPORT].

90. *See id.* One difficulty was filling the position of National Counterintelligence Executive, especially during the critical first years of its operation. The position was vacant for nearly eighteen months between the first Executive (David Szady, an FBI official) and the second (Michelle Van Cleave, a DoD official). When Van Cleave left in March of 2006, the position remained open until the appointment of Joel Brenner in August 2006. The NCIX also struggled to meet some basic statutory obligations. Though the Counterintelligence Enhancement Act of 2002 required the NCIX to produce an annual strategy, *see* The Counterintelligence Enhancement Act of 2002 *supra* note 88, the first such strategy document was not issued until 2005, *see* Office of the National Counterintelligence Executive, "The National Counterintelligence Strategy of the United States" (2005), *available at* http://www.ncix.gov/publications/policy/FinalCIStrategyforWebMarch21.pdf, and the second was issued in 2007, *see* Office of the National Counterintelligence Executive, "The National Counterintelligence Strategy of the United States of America" (2007), *available at* http://www.ncix.gov/publications/policy/FinalCIStrategyforWebMarch21.pdf.

91. *See* Definition of "counterintelligence" posted at http://www.ncix.gov/issues/index.html. *See also* National Counterintelligence Strategy of the United States (2005) Preface (describing counterintelligence as "defensive and offensive activities conducted at home and abroad to protect against the traditional and emerging *foreign intelligence* threats of the 21st Century" (emphasis added)).

92. International terrorist groups are unlikely to have formal intelligence services. The examples cited by the NCIX of terrorist intelligence gathering are far more tactical in nature (i.e., are more in the form of pre-operational surveillance in preparation for an actual attack).

counterespionage, information security, and critical infrastructure protection.[93]

Faced with the need to redefine its role in the context of the war on terrorism, DoD counterintelligence could not rely on much guidance from the ONCIX or from its counterparts in the FBI and CIA counterintelligence operations. Unlike the CIA and the FBI, the DoD tended not to separate counterintelligence and counterterrorism. Counterintelligence components remained responsible for operations against terrorist groups. The complication for DoD counterintelligence was not that counterterrorism was breaking off as a separate discipline, but rather that, under the rubric of counterterrorism, other entities inside DoD were beginning to conduct counterintelligence-like activities, including activities within the United States. As discussed above, the military was beginning to approach counterterrorism as a military issue, a mission that might well play out on U.S. soil. This military approach would drag along the foreign/military intelligence elements of the DoD. On the other end of the spectrum, DoD counterintelligence saw increasing counterterrorist activities by law enforcement and force protection components.

The growing role of DoD law enforcement and force protection components in counterintelligence-like activities can only be understood in the context of the broader relationship between counterintelligence and law enforcement. This relationship, of course, underwent a substantial and rapid transformation following the 9/11 attacks. Prior to 2001, DoD law enforcement as a whole had only minimal connections with the DoD counterintelligence world. There were, of course, two DoD law

---

See National Counterintelligence Strategy of the United States (2005) at 3-4 and National Counterintelligence Strategy of the United States of America (2007) at 5 (counter intelligence to neutralize the "intelligence activities" that precede terrorist attacks). The idea that counterintelligence would focus only on the intelligence gathering activities of terrorists and not on the execution of actual attacks is at odds with the existing taxonomy. Terrorist attacks are essentially some combination of sabotage and assassination – both of which are addressed as counterintelligence in the existing definitions. *See* Exec. Order 12,333 at §3.5(a).

93. Both 2005 and 2007 National Counterintelligence Strategies make initial mention of the Global War on Terrorism but then immediately shift emphasis to traditional espionage activities, economic espionage, and espionage via the information infrastructure. *See supra* note 92. More accessible examples of the same trend are to be found in the recent public speeches of the Executive. In addressing both private sector and military intelligence audiences, the Executive does not even mention terrorist groups as a counterintelligence concern. *See, e.g.,* Joel F. Brenner, Strategic Counterintelligence: Protecting America in the 21st Century (Oct. 24, 2007) (remarks delivered to the NRO-NMIA Military Intelligence Association Counterintelligence Symposium), *available at* http://www.ncix.gov/publications/speeches/NRO-NMIA-CI-Symposium-24-Oct-07.pdf and Joel F. Brenner, Counterintelligence in the 21st Century: Not Just a Government Problem (Dec. 4, 2007) (remarks delivered to the AFCEA Counterintelligence Conference), *available at* http://www.ncix.gov/publications/speeches/AFCEASpeech.pdf. Both speeches (one to a military audience and one to a private sector group) contain virtually no mention of terrorism as a counterintelligence issue. Rather, the focus is on traditional espionage, cyber-security issues, and economic espionage. *Id.*

enforcement organizations (NCIS and AFOSI) that had both law enforcement and counterintelligence authorities, but these belonged to a special class of law enforcement organizations. Within the DoD, the NCIS, the AFOSI, and the Army Criminal Investigative Command are known as the Military Criminal Investigative Organizations or MCIOs. They are responsible for major investigations and employ special agents.[94] They are roughly the analog to the FBI in the civilian law enforcement systems and frequently conduct joint investigations with the FBI. The bulk of DoD law enforcement is composed of the military police,[95] which are responsible for maintaining day-to-day security and order in military facilities. The MCIOs and the military police respond to different chains of command.[96]

The principal focus of both the MCIOs and the military police is the investigation of crimes that fall within the DoD's jurisdiction. Most often, this involves the enforcement of the Uniform Code of Military Justice (UCMJ) with respect to those individuals who are subject to it.[97] Because DoD facilities are populated with many persons not subject to the UCMJ (DoD civilian employees, contractors, visitors), the military police and MCIOs necessarily maintain a close relationship with the civilian law enforcement organizations with primary jurisdiction over those individuals.[98] In addition to these traditional law enforcement duties, the

94. "Special agents" are investigators who have arrest authority, are issued badges and credentials, and are authorized to carry firearms. The term is typically associated with criminal investigators (such as FBI agents) and with the Series GS-1811 federal criminal investigators. GS-1811 status is important because it entitles the investigator to receive special availability pay and other benefits. *See* U.S. Office of Personnel Management, "Availability Pay" (Dec. 11, 1998) http://www.opm.gov/oca/pay/HTML/AP.HTM (summarizing definitions and benefits for federal criminal investigators). The potential availability of 1811 status and pay is, perhaps, a factor contributing to some of the counterintelligence/law enforcement fusion that can be observed in DoD.

95. We use the term here generally. In the Army and the Marine Corps, the police force is called "Military Police"; in the Air Force, it is the "Security Forces"; and in the Navy, "Masters at Arms."

96. Army and Marine Military Police report to the Provost Marshal. *See, e.g.,* Office of the Provost Marshal, U.S. Army FORSCOM Homepage, http://www.forscom._army.mil/dcspim/provost_marshal.htm, and Provost Marshal Office, U.S. Marine Corps Base Camp Pendleton Homepage, http://www.pendleton.usmc.mil/base/ses/pmo/pmo.aspb. Air Force Security Forces at the wing level typically report to the Mission Support Group. *See, e.g.,* U.S. Air Force Fact Sheet, 1st Mission Support Group, *available at* http://www.langley.af.mil/library/factsheets/factsheet_print.asp?fsID'3716&page'1. Navy Masters at Arms typically report to the unit executive officer. See job descriptions at Enlisted Rating Insignia, U.S. Navy Homepage, http://www.navy.mil/navydata/navy_legacy_hr.asp?id'262.

97. The UCMJ is codified at 10 U.S.C. §§801-946. Persons subject to UCMJ jurisdiction include active duty members of the armed forces, certain reservists, National Guard members in federal service, cadets and midshipmen, certain military retirees, certain federal civilian employees assigned to and serving with the armed forces, prisoners of war in military custody, and "persons serving with, employed by, or accompanying the armed forces outside the United States." *Id.* §802.

98. The basic jurisdictional principles and implementation procedures are summarized

military police, backed up by the MCIOs, are also responsible for the security of the DoD's installations and equipment. In recent years, the military term "force protection" has become the common descriptor for these activities. When U.S. forces are deployed overseas, especially in combat situations, "force protection" has a fairly specific meaning. The DoD defines "force protection" as

> . . . actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease.[99]

In a deployed environment, then, force protection consists of all those activities that a commander would take to ensure that the enemy has not degraded the military force by attacking the vulnerable rear or support components of the force. So security personnel are posted in and around installations where U.S. troops are housed, dependents and contractors are made aware of threat information, and other similar precautions are taken.

In the wake of the 9/11 attacks, force protection became a watchword for DoD installations within the United States as well.[100] DoD law enforcement, under the rubric of force protection, began to step up its base security efforts, which entailed an increased level of cooperation with civilian law enforcement. Inside the United States, DoD law enforcement always relied on civilian law enforcement for information relevant to the

---

in DoDI 5525.07, "Implementation of the Memorandum of Understanding (MOU) Between the Departments of Justice (DoJ) and Defense Relating to the Investigation and Prosecution of Certain Crimes" (June 18, 2007), http://www.dtic.mil/whs/directives/corres/html/552 507.htm. The provisions of the MOU are also written into the U.S. Attorney's Manual. *See* U.S. Department of Justice, U.S. Attorney's Manual, Title 9, "Criminal Resource Manual" §669, http://www.usdoj.gov/usao/eousa/foia_reading_room/ usam/title9/crm00669. htm.

99. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms (as amended though Oct. 17, 2007) at 211-212, *available at* http://www. dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

100. Just as the 1995 bombing of the Federal Building in Oklahoma City spurred a re-evaluation of security for federal buildings generally, the successful terrorist attack on the Pentagon in 2001 initiated a flurry of force protection initiatives aimed at defeating terrorist attacks. The growing use of the military term reflected the overall militarization of the counterterrorism environment post-9/11. For example, in 2002 the DoD civilian police force (the Pentagon Police) morphed into the Pentagon Force Protection Agency and dramatically expanded its mission. *See* "The Pentagon's Police," Pentagon Force Protection Agency website, http://www.dtic.mil/dps/about.html, and DoDD 5105.68, Pentagon Force Protection Agency, http://www.dtic.mil/whs/directives/corres/pdf/510568p.pdf.

protection of DoD facilities. The military police, and other DoD security forces, were responsible for guarding the gates and patrolling within DoD facilities but had little or no jurisdiction "outside the fence." The DoD relied on the FBI to provide information about foreign intelligence or terrorist threats to specific installations and on local police forces to provide information on criminal activities in the vicinity of the installation. As a consequence, DoD law enforcement had fairly regular interaction with civilian law enforcement pre-9/11 and had little difficulty expanding these contacts in the post-9/11 setting. What changed after 9/11 was the sense of reality and urgency attached to the threat. The goal of domestic force protection was, first and foremost, to prevent another catastrophic attack on a DoD facility. Besides strengthening standard physical security measures and raising awareness,[101] the detection of pre-operational surveillance activities by terrorists at DoD facilities was a promising means of prevention.[102]

The difficulty with watching for pre-operational activities by terrorists is that these activities often may, in and of themselves, be innocuous. Consider the example of a car approaching the gate of an Air Force base.[103] The car pulls up to the gate and is approached by the security forces on duty. The driver tells the guard that he has made a wrong turn and did not intend to approach the gate (a fairly common occurrence at military bases). The guard will instruct the driver to turn around and leave the gate area. The errant motorist may simply have made an innocent mistake, and if so pose no threat at all. However, from the force protection perspective (and especially in a heightened threat environment), the motorist may be using a classic pre-operational surveillance technique. Assume that this is the case and that the motorist is actually a terrorist planning to attack the base on some later occasion by using a car bomb. The terrorist, posing as a lost motorist, is getting a close-up view of the base's gate security. He will learn how many guards are posted at the gate, what their response is to the

101. These kinds of activities form the core of DoD anti-terrorism program or ATP, which involves routine training and awareness programs at all DoD component levels. *See* DoDD 2000.12, "DoD Anti-Terrorism Program" (Aug. 18, 2003), *available at* www.dtic.mil/whs/directives/corres/html/200012.htm.

102. The idea here is that terrorists planning an attack are likely to case a potential target, and perhaps even engage in activities designed to test the defensive responses of the target. This behavior has been observed in numerous terrorist incidents, including the 9/11 attacks themselves. *See* THE 9/11 COMMISSION REPORT, *supra* note 4, at 158, 244-245, and The National Counterintelligence Strategy of the United States of America (2007), *supra* note 90, at 5. One strategy of force protection is to detect such pre-operational activities and then act to disrupt the pending attack.

103. This paragraph contains an extended hypothetical suggested by examples included in the document initiating the DoD-wide TALON program. *See* Deputy Secretary of Defense Memorandum on the Collection, Reporting and Analysis of Terrorist Threats to DoD within the United States, (May 2, 2003), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB230/04.pdf .

appearance of an unauthorized vehicle, what weapons are readily accessible to them, and what obstacles would prevent the car from driving past the guards. From a force protection perspective, the motorist is a potential threat. The guards at the gate have little or no means of determining whether a particular instance of a "lost motorist" is innocuous or not.

Under such circumstances, what information should the DoD personnel be collecting? Should a description of each "lost motorist" be collected? Should the driver be asked for his license and the information taken down by the guards? Once collected, how should this information be used? Should it be shared with other security forces on the bases, or more broadly in the DoD? Clearly, if the same "lost motorist" showed up at other gates or other DoD facilities with the same story, the pre-operational nature of the activity would be apparent, and the identity of the driver might be a critical clue to the prevention of an attack. But this outcome is certainly the narrow exception. The vast majority of lost motorists are just that; and the collection of information about them would entail the handling and analysis by DoD law enforcement of personal information about likely U.S. persons who had violated no law and who posed no threat at all to DoD.[104]

The scenario just discussed was the motivation behind the DoD's controversial TALON program, and it illustrates the legal difficulty posed by the rise of domestic force protection activities. The traditional post-Church taxonomy governing the collection of U.S. person information embodied two general paradigms: foreign/military intelligence (broad-spectrum collection of information that, by virtue of targets' nature, was unlikely to involve U.S. persons) and counterintelligence (which involved substantial collection of U.S. person data, though in a highly targeted, narrow-spectrum investigation).[105] Force protection presented the challenge of relatively broad-spectrum domestic collection in which individualized targeting occurred after the fact, if at all. The challenge is compounded by the fact that the primary collectors of force protection information are DoD

104. The "lost motorist" scenario is but one of a number of common potential pre-operational activities. Others include individuals photographing or observing facilities from a greater distance (and without directly interacting with DoD personnel), individuals attempting to elicit information from DoD personnel about access to the facilities in which they work, and individuals who may be using other activities (deliveries, tours of facilities, protests) as means of getting a closer look. *See id.* All such tactics raise the same issue of how genuine (and rare) pre-operational surveillance can be separated from lawful and innocuous activity. Some, such as protest activity, raise special concerns about the chilling effect on protected expression. Others, such as the case of individuals photographing DoD facilities at a distance, may raise jurisdictional and coordination issues with local law enforcement. Some examples of actual force protection reports, and related materials, are collected in the National Security Archive's Electronic Briefing Book on CIFA and the TALON Program. *See* Jeffrey Richelson, "The Pentagon's Counterspies," National Security Archive Briefing Book No. 230 (Sept. 17, 2007), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/ NSAEBB230/index.htm.

105 These are general characterizations. Counterintelligence operations were already straining somewhat against the purely investigative paradigm. *See supra* note 56.

law enforcement personnel, whose activities are not even governed by the intelligence oversight rules.[106] The collection of U.S. person information by DoD law enforcement components is governed by the general rules established in DoD Directive ("DoDD") 5200.27.[107] Those rules allow for the collection of U.S. person information for the protection of DoD functions and property but specify the types of activity that merit such protective collection.[108] A number of the specified activities appear to afford some latitude for the collection of force protection information, such as activities endangering facilities.[109] After listing the specified permitted collection targets, as well as some general prohibitions, the rules create an exception under the heading "Operational Guidance":

> Nothing in this Directive shall be construed to prohibit the prompt reporting to law enforcement agencies of any information indicating the existence of a threat to life or property, or the violation of law, nor to prohibit keeping a record of such a report.[110]

The "exception" language could well be read to allow the broad collection of force protection information discussed above, depending on the interpretation given to the language "indicating the existence of a threat." Information collected pursuant to DoDD 5200.27 is subject to a general limitation on retention: such information has to be destroyed within 90 days "unless its retention is required by law or unless its retention is specifically authorized under criteria established by the Secretary of Defense, or his designee."[111] The regulation thus acknowledges that DoD components will have legitimate reasons to collect U.S. person information in the course of their ordinary operations, but there will be a presumption against the retention of any such information. Applying this principle to a particularly thorny example, if an antiwar group were to plan a protest at the gate of an Army base, the security forces protecting that base would be able to collect information about the planned protest (i.e., the potential size of the protest, the activities planned, the identity of the organizing group etc.) because such information would be relevant to the protection and operation of the base.[112] However, once the protest has actually occurred,

---

106. *See* DoD 5240.1-R, Proc. 1 §C1.1. The oversight rules of 5240.1-R do not apply to DoD law enforcement activities, even when those activities are conducted by DoD counterintelligence components (such as the NCIS or AFOSI).

107. DoDD 5200.27, "Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense" (Jan. 7, 1980), *available at* http://www.dtic.mil/whs/directives/corres/html/520027.htm.

108. *Id.* at §4.1.

109. *See id.* at §4.1.6.

110. *Id.* at § 6.1.

111. *Id.* at §6.4.

112. The fact that a protest is non-violent and lawful does not necessarily remove these

these justifications for collecting the information would cease to exist and, absent specific direction from the Secretary of Defense, there would be no reason to retain the information. The provisions of DoDD 5200.27 would therefore mandate its destruction within 90 days of collection.[113]

From the perspective of a component charged with detecting pre-operational activity, however, the ninety-day limitation presents a problem. Patterns indicating pre-operational activity may only become apparent over time or may only emerge when data is analyzed in the context of newer intelligence. An intelligence or counterintelligence analyst might require an extended period of time to determine whether or not the collected information holds any intelligence value. For this reason, rules governing intelligence activities generally allow for longer periods of retention. DoD 5240.1-R, Procedure 3, for example, allows for the general retention of any information that was properly collected pursuant to its collection provisions[114] and allows the retention of other incidentally acquired information if it is "necessary to understand or assess foreign intelligence or counterintelligence."[115] The rules also allow the retention of incidentally collected U.S. person information that may indicate involvement of activities that may violate federal, state, local or foreign law.[116] The only time restriction imposed by the intelligence/counterintelligence rules is that a permanent retention decision be made within ninety days for any U.S. person material collected.[117]

The ill-fated TALON program illustrates one approach to the force protection conundrum.[118] The TALON program was authorized by Deputy Secretary of Defense Wolfowitz in 2003 to "identify, report, share, and analyze nonvalidated threat information in the United States."[119] Essentially, the TALON system was created to provide for the nationwide collection of information that potentially indicated pre-operational terrorist activity (e.g.,

---

concerns. Protests outside DoD facilities could affect authorized access to the facilities, or otherwise trigger legitimate concerns for DoD law enforcement personnel.

113. DoDD 5200.27 at §6.4. Unlike the intelligence oversight rules, *see* DoD 5240.1-R, Proc. 2, §C2.3.2, DoDD 5200.27 does not create a general exception for publicly available information. Thus, even if the information about the protest was drawn entirely from articles published in newspapers, this Directive would still require its destruction.

114. These collection provisions are found in Procedure 2, and allow, *inter alia*, the collection of U.S. person information when "the information is needed to protect the safety of any person or organization, including those who are targets, victims, or hostages of international terrorist organizations." *See* DoD 5240.1-R, Proc. 2, §C2.3.11.

115. DOD 5240.1-R, PROC. 3, §C.3.3.

116. *Id.* at §C3.3.2.4.

117. *Id.* at §C3.3.4. The requirement is hardly onerous, since the evaluator must only determine that the U.S. person information arguably falls within one of the rather generously categories defined in Procedure 3.

118. A full examination of the TALON program is beyond the scope of this article. The National Security Archive's Electronic Briefing Book contains a valuable collection of the primary sources on TALON that are now publicly available. *See supra* note 104.

119. Deputy Secretary of Defense Memorandum, *supra* note 103.

the "lost motorist" and similar scenarios, as discussed above).[120] The 2003 document described the categories of nonvalidated threat information to be collected by "all DoD intelligence, counterintelligence, law enforcement, and security organizations that have a mission to collect force protection and threat information" and directed that such information be forwarded to the Counterintelligence Field Activity (CIFA).[121] CIFA was to maintain a database repository of these reports and share them with the Joint Intelligence Task Force – Combating Terrorism (JITF-CT).[122] The apparent goal of this program was that CIFA and/or JITF-CT would analyze the collected information to detect any patterns that would indicate pre-operational terrorist activities and then disseminate such conclusions to the appropriate components. The TALON program was a subject of understandable concern to civil libertarians, as it clearly involved the collection by DoD of a great deal of U.S. person data within the United States. In 2005, news reports began to surface that the TALON database included information on antiwar protest groups. The resultant controversy, fueled by the perceived similarity between this activity and some of the abuses identified by the Church Committee in 1975, ultimately led to the termination of the TALON program in 2007.[123] A careful examination of the TALON documents reveals that the most troubling collections (those involving lawful protest groups) were not actually collected by the DoD; rather, they were generated or collected by civilian law enforcement agencies and transmitted to DoD law enforcement agencies through force protection liaison channels.[124] DoD law enforcement components then reported them to CIFA through the TALON program. In other instances, U.S. person information swept up in the force protection paradigm was

120. *See* Department of Defense, Information Paper: DoD TALON, (undated) (a DoD document summarizing the rationale for the TALON program), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB230/14.pdf. TALON was based on a pre-existing Air Force program of the same name. *See* Department of Defense Inspector General Report No.07-INTEL-09, "The Threat and Local Observation Notice (TALON) Report Program," (June 27, 2007) at 1.

121. Deputy Secretary of Defense Memorandum, *supra* note 103, at 2.

122. *Id.* JITF-CT is a DIA component responsible for the "indications and warnings" of terrorist attacks. Though, as a DIA component, it functions in the foreign/military intelligence paradigm, its functions apparently overlap somewhat with the counter intelligence functions of CIFA. *See* The DoD Role in Homeland Security, Defense Study and Report to Congress (July 2003) at 13, *available at* www.ndu.edu/uchs/NDAA%20FY02%20Report%20(DoD%20in%20HS)%20-%20final.pdf.

123. Department of Defense Press Release, DoD to Implement Interim Threat Reporting Procedures (August 21, 2007) (announcing that CIFA will close the TALON database effective Sept. 17, 2007), *available at* http://www.defenselink.mil/releases/release.aspx?releaseid'11251.

124. See examples of controversial TALON reports collected in Richelson, *supra* note 104. Documents 17a through 17i on this site are copies of TALON reports noting, in most cases, the non-DoD source of the initial report. *Id*.

initially brought in to the DoD (or collected, in those instances where a DoD component was the actual collector) primarily by law enforcement components under the relatively permissive collection rules of DoDD 5200.27. The information was then transmitted to CIFA, which retained it, presumably in accordance with the provisions of DoD 5240.1-R. In other words, the force protection challenge led to the creation of a hybrid that mixed DoD law enforcement collection rules with DoD intelligence oversight retention rules. The end result was that nonvalidated "threat" information on U.S. persons found its way into a DoD intelligence and counterintelligence database for analysis.[125]

As the controversy over the TALON database grew, DoD recognized the tension in the two rule sets[126] and would eventually admit to Congress that DoD components involved in TALON were "following multiple rule sets regarding the collection and retention of this information."[127] The Department swiftly clarified that CIFA's retention of TALON data was governed by DoD 5240.1-R[128] and subsequently issued guidance that established specific requirements for retention of information.[129] The DoD Inspector General (IG) reviewed the TALON program in the spring of 2007 but hardly clarified the situation. The IG concluded that because CIFA (at least prior to 2006) was conducting a law enforcement and force protection function and the collection of the TALON information was permissible as a law enforcement activity, CIFA should have applied the ninety-day retention rule, DoDD 5200.27.[130] Shortly thereafter, CIFA closed the TALON database.[131]

---

125. *See* Deputy Secretary of Defense Memorandum, *supra* note 103.

126. An internal DoD document obtained by the ACLU reflected this confusion, among many other issues relating to the program. *See* Department of Defense, "Review of the TALON Reporting System" (n.d.), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB230/15.pdf.

127. Letter from the Deputy Undersecretary of Defense (Counterintelligence and Security) to the Hon. John W. Warner (Jan. 27, 2006), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB230/10.pdf.

128. *See* Undersecretary of Defense for Intelligence Memorandum to the Director, CIFA, The TALON/CORNERSTONE Database (Feb. 2, 2006), *available at* www.defenselink.mil/pubs/foi/talon_policy.pdf.

129. *See* Deputy Secretary of Defense Memorandum, "Threats to the Department of Defense" (Mar. 30, 2006), *available at* www.defenselink.mil/pubs/foi/talon_policy.pdf. The Procedures attached to this memorandum allow indefinite retention of U.S. person data in TALON reports only if there is a "reasonable belief" that the U.S. person is engaged in, or is about to engage in, international terrorist activities. The Procedures thus narrow the permanent retention categories in DoD 5240.1-R to the single category of international terrorism. However, CIFA may retain information for up to ninety days while making this determination of "reasonable belief." *Id.*

130. DoD Inspector General Report No. 07-INTEL-09, *supra* note 120, at 6, 8-9. The legal reasoning in the TALON IG Report is somewhat garbled. The report analyzes CIFA's retention of data under law enforcement rules, but cites definitions from the Foreign Intelligence Surviellance Act, and concludes that CIFA did not violate the provisions of FISA. The report discusses DoD 5240.1-R, Procedure 2, in passing, but omits any mention

The TALON database provides a good illustration of the manner in which the rapid growth of a domestic force protection mandate can outstrip the existing rule sets. Faced with a novel challenge, operational components gravitated toward the rules that allowed them to accomplish the stated mission: the "collectors" turned to the law enforcement rules (5200.27), which established a lower threshold for domestic collection, while eventual custodians and analysts turned to the more generous retention provisions of the intelligence rules. The end result was the inclusion of U.S. person data in DoD intelligence databases under circumstances that did not appear to meet the standards established in the post-Church era regulations. The TALON example also illustrates that the key issue here is not always the adequacy of particular regulations but rather the clarity of the definitions that govern which set of regulations applies to a given activity. In particular, force protection information (and activities) seem to occupy an ambiguous space between law enforcement and intelligence operations and create the possibility that, whether through confusion or by intent, operators will cobble together rule sets to create a hybrid that falls short of the standards that we had thought were already enacted in the regulatory milieu.

In many respects, the development of the "force protection" concept mirrors that of the "homeland defense" concept examined above.[132] Just as the presence of an international terrorist group as a military adversary pushed the foreign/military intelligence operations into the domestic arena, it also pushed the law enforcement and security components of DoD into the domestic intelligence business via the force protection imperative. In both instances, the operations of other components began to encroach on the traditional environment of DoD counterintelligence but without uniformly adopting the associated oversight mechanisms. This process is, of course, not inherently unwelcome. One would expect and hope that national security components of the government would adapt operationally to a changing threat environment. The question, however, is whether the law sufficiently informs that adaptation. While the law relevant to national security has certainly changed in response to the 9/11 attacks, the translation of those changes into the DoD regulatory milieu has been slow.

Nowhere is this more apparent than at the counterintelligence/law enforcement seam exposed in the TALON example. Like the rest of the intelligence community in the years prior to the passage of the USA PATRIOT Act, DoD intelligence activities were governed by rules that presumed a strict separation between intelligence and law enforcement operations. The legal "wall" between intelligence and law enforcement

---

of the most obviously relevant collection categories (e.g., "Physical Security," *see* DoD 5240.1-R, Proc. 2 §C2.37, and "Threats to Safety," *see id.* §C2.3.11.).

131. *See* Department of Defense Press Release, *supra* note 123.

132. *See supra* notes 80-85 and accompanying text.

arose from the familiar, and still controversial, primary purpose issue in the law of national security electronic surveillance. While the legal issue here was tied to FISA, its impact in the operational culture was felt far beyond the circle of counterintelligence investigations that involved FISA surveillance. Both the intelligence (DoD 5240.1-R) and law enforcement (DoDD 5200.27) rules embodied this division. DoD 5240.1-R treated dissemination of information to law enforcement as a process limited to certain defined circumstances.[133] In this structure, the DoD rules mirrored the Attorney General Guidelines then in effect for the FBI.[134]

Following the passage of the USA PATRIOT Act and the subsequent litigation over the primary purpose test,[135] the Attorney General issued a revised set of guidelines for FBI national security operations. The National Security Investigative Guidelines, issued on October 31, 2003, essentially erase the distinction between criminal investigations and counter-intelligence investigations for the FBI.[136] The new guidelines contain specific guidance for the FBI on how to conduct the proactive collection of threat information, which is roughly analogous to the force protection collections undertaken by DoD, and explain the relationship between that activity as conducted under the NSIG and similar activities conducted under other Attorney General Guidelines (such as those for "General Crimes"[137] and extraterritorial operations).[138] The revision of the NSIG was part of a larger review of all Attorney General Guidelines conducted after 9/11, and this project was ultimately brought to completion by the issuance, in 2008, of new Attorney General's Guidelines for Domestic FBI Operations that integrated the NSIG, the General Crimes Guidelines, and other authorities into a single consolidated document.[139]

---

133. *See* DoD 5240.1-R, Proc. 4.

134. *See* Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (May 25, 1995), Sec. VII, *redacted version*, *available at* http://www.fas.org/irp/agency/doj/fbi/terrorismintel2.pdf.

135. *See supra* note 4.

136. *See* The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (Oct. 31, 2003), *redacted version, available at* http://www.usdoj.gov/olp/nsiguidelines.pdf, p. 2 (investigations under these guidelines are usually both criminal and counterintelligence).

137. *See* The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (May 30, 2002), *available at* http://www.usdoj.gov/olp/generalcrimes2.pdf .

138. *See* National Security Investigations Guidelines, *supra* note 136, at 3; The specific NSIG provisions governing the techniques of these "threat assessments" remain classified, but the unclassified portions of the NSIG certainly imply that the topic of proactive collection is covered in detail later in the document.

139. *See* U.S. Department of Justice, The Attorney General's Guidelines for Domestic FBI Operations, (Sept. 29, 2008), *available at* http://www.usdoj.gov/ag/readingroom/guidelines.pdf. These new Domestic Operations Guidelines became effective on December 1, 2008, and are generally unclassified.

Although the DoD 5240.1-R is the DoD analog to the NSIG and the subsequent Domestic Operations Guidelines in that all are mandated by provisions of Executive Order 12,333,[140] there has been no analogous post-9/11 revision of the DoD 5240.1-R. Indeed, the currently posted version of DoD 5240.1-R does not even reflect the addition of physical search authority to the FISA statute in 1994.[141] The process of revising DoD 5240.1-R is, of course, a substantial one and would require the involvement of the Attorney General.[142] Nonetheless, nearly eight years after 9/11 and nearly six years after the issuance of the revised NSIG, DoD intelligence and counterintelligence components are still operating under a rule set that does not acknowledge any post-9/11 developments in the law. The rules applicable to DoD law enforcement collection of U.S. person information (DoDD 5200.27) were last revised in 1980.[143] The neglect of these now critically relevant rule sets is striking, and certainly brings to mind some of the findings of the Church Committee about the need for clear and relevant guidance to properly govern DoD intelligence activities.[144]

The unrevised state of the DoD's foundational oversight documents is particularly troubling in light of the broad exposure of DoD law enforcement, counterintelligence, and even intelligence elements to the FBI's integrated approach under the 2003 NSIG and, now, under the 2008 Domestic Operations Guidelines. Much of this interaction occurs on the Joint Terrorism Task Forces (JTTFs). JTTFs, which currently exist in at least 103 cities, are FBI entities that incorporate other federal, state, and local law enforcement officers as well as representatives from the intelligence community.[145] Under the JTTF construct, JTTF members from other agencies are detailed to the FBI, operate under FBI supervision, and follow the FBI's Attorney General Guidelines.[146] The number and size of

---

140. Exec. Order No. 12,333 at §1.3(b)(20) (corresponding to §1.11(d) in the older version of the Order: DoD to conduct counterintelligence pursuant to guidelines "agreed upon by the Secretary of Defense and the Attorney General").

141. Physical search authority was added to the FISA in 1994. *See* Pub. L. No. 103-359, Title VII (Oct. 14, 1994), 108 Stat. 3443. DoD 5240.1-R makes no reference to FISA in Procedure 7 (Physical Search). *See* DoD 5240.1-R, Proc. 7, *cf. id.* and Proc. 5 (referencing thoughout the electronic surveillance provisions of the FISA).

142. *See* DoD 5240.1-R at §§C1.4 and C1.5.

143. The currently posted version of DoDD 5200.27 was issued on January 7, 1980. *See* http://www.dtic.mil/whs/directives/corres/html/520027.htm.

144 *See supra* notes 4 and 19.

145. In 2005, the DOJ Inspector General reviewed the performance of the JTTFs and other post-9/11 task forces. *See* Office of the Inspector General, U.S. Department of Justice, The Department of Justice's Terrorism Task Forces, Evaluation and Inspections Report I-2005-007 (2005), *available at* http://www.usdoj.gov/oig/reports/plus/e0507/.

146. Non-FBI members of JTTFs are supposed to be integrated under the terms of an individual Memorandum of Understanding, though the IG report noted that no MOUs existed for many task force members, and that the terms of the template MOU needed updating. *Id.* at http://www.usdoj.gov/oig/reports/plus/e0507/results.htm#dept10.

the JTTFs grew dramatically following 9/11, and DoD involvement appeared to keep pace with that growth. The AFOSI, the NCIS, and the Defense Criminal Investigative Service[147] are all represented on individual JTTFs. In addition, the Defense Intelligence Agency and, separately, its Directorate for Human Intelligence are represented on the umbrella National Joint Terrorism Task Force located at FBI headquarters.[148] CIFA also had some role in supporting the DoD presence on the JTTFs.[149] Given the scope of the DoD counterintelligence and law enforcement presence on the JTTFs, it is difficult to believe that some pressure for a more integrated intelligence/law enforcement approach does not exist within the MCIOs and the DoD counterintelligence components, especially those that incorporate both counterintelligence and law enforcement authorities. If this is the case, then the potential, in the absence of current legal guidance, for more ad hoc mixing of rule sets à la TALON certainly exists. The potential negative effects of such activities are magnified in the post-9/11 environment by the greater availability to DoD of investigative tools to obtain information relating to international terrorism.[150]

While the TALON program is an example of an individual operation responding to the changing legal environment, CIFA represented an entire organization shaped by the tensions we have been discussing. CIFA has sometimes been characterized as a secret DoD agency created in the wake of the 9/11 attacks.[151] In fact, the existence of CIFA has never been classified, and its charter, DoDD 5105.67, is publicly available in unredacted form on a variety of DoD websites.[152] Although the directive

147. The Defense Criminal Investigative Service (DCIS) is the criminal investigative arm of the DoD Inspector General's Office. It derives its jurisdiction from the Inspector General Act of 1978 and thus would focus on the investigation of fraud, waste, and abuse in DoD programs. In recent years, however, the DCIS has claimed a much broader law enforcement role and now identifies counterterrorism as one of its major missions. *See* Department of Defense, Office of the Inspector General, "Support to the Global War on Terror" http://www.dodig.mil/gwot_iraq/gwot.htm. DCIS appears to have devoted a substantial portion of its 300 special agents to service on the JTTFs. *See id.* (listing DCIS presence on thirty-nine JTTFs).

148. *See* DOJ IG Report, *supra* note 145.

149. *See* The DoD Role in Homeland Security, *supra* note 122, at 13.

150. The USA PATRIOT Act, for example, created a new "national security letter" authority that can be used to obtain credit card information. *See* Pub. L. No. 107-56, §358(g)(1)(B), 115 Stat. 272, 327-328 (2001), codified at 15 U.S.C. §1681v. Unlike other compulsory national security letters, this authority (which are available only to the FBI) this authority is available to any "government agency authorized to conduct investigations of, intelligence or counterintelligence activities or analysis related to, international terrorism . . ." *Id. See also* Michael J. Woods, *Counterintelligence and Access to Transactional Records: A Practical History of USA PATRIOT Act Section 215,* 1 J. NATL. SEC. L. & POL'Y. 37, 54-55 (2005).

151. *See, e.g.,* Walter Pincus, *Pentagon's Intelligence Authority Widens*, WASH. POST, Dec. 19, 2005, at A10.

152. DoDD 5105.67, "Department of Defense Counterintelligence Field Activity (DoD CIFA)" (Feb. 19, 2002), *available at* http://www.cifa.mil/Library%20and%20 References/

creating CIFA was finally issued in February 2002, the creation of CIFA was not prompted by the 9/11 attacks.[153] Rather, CIFA was born out of two pre-9/11 initiatives, one external to DoD and the other internal. The external initiation was the process that gave rise to the National Counterintelligence Executive (NCIX).[154] Prompted by persistent concerns over the disorganized state of counterintelligence, the Clinton Administration created a study initiative known as "Counterintelligence for the 21st Century" (CI-21). The CI-21 process culminated in the issuance of Presidential Decision Directive 75 in December 2000, which created the NCIX.[155] One of the principal functions of CIFA was to organize DoD counterintelligence along the same lines that the NCIX would organize national counterintelligence. These functions are reflected in many provisions of DoDD 5105.67.[156] The need for DoD to organize internally was driven by the need for DoD counterintelligence to speak with a single voice in the NCIX process. Unlike the other components of the NCIX (the FBI and the CIA), DoD's counterintelligence functions were spread across the three military departments (Army, Navy,[157] and Air Force) and a handful of DoD agencies.[158] In order for the NCIX to operate as envisioned,

---

documents/CIFA%20Charter.pdf and at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB230/02.pdf. DoDD 5105.67 no longer appears in the official online respository of DoD Issuances (http://www.dtic.mil/whs/directives/) since it was formally cancelled when CIFA functions were integrated into the Defense Intelligence Agency in 2008. *See infra* note 185. At the time of this writing, the CIFA public website was still functioning, and documents cited herein to that website are accessible using the URLs provided.

153. DoD Directives and Instructions are subject to an extensive coordination process. *See* DoDI 5025.01, "DoD Directives Program," Encl. 3 (Oct. 28, 2007) http://www.dtic.mil/whs/directives/corres/pdf/502501p.pdf. It is therefore likely that DoDD 5105.67 was actually drafted many months before its original signature date and probably before September 11, 2001.

154. *See supra* note 89.

155. *See* Fact Sheet, *supra* note 87.

156. *See, e.g.,* DoDD 5105.67, §4.1 (DoD policy to support NCIX), §4.3 (DoD policy to provide single point of coordination for NCIX),§6.1.3 (designating official to represent Secretary of Defense to the NCIX), §6.2.4 (Director of CIFA's role in DoD interaction with NCIX), and §6.4.1 (directing military departments to support CIFA in implementing PDD-75).

157. The Marine Corps and all of its counterintelligence functions are part of the Department of the Navy.

158. DoD agencies (which are not components of any military department) handle counterintelligence in a variety of ways. In some cases, a military service is designated the "executive agent" for counterintelligence in a given agency. This means that counterintelligence agents from that military service handle any counterintelligence matters arising in that particular agency. Other agencies, typically those with greater need for counterintelligence support, are authorized to create their own counterintelligence programs (i.e., to hire their own counterintelligence staff). Such agencies are said to have "organic" counterintelligence capability. *See generally* DoDD 5143.01: "Under Secretary of Defense for Intelligence (USD(I))," Encl. 2 (Nov. 23, 2005), *available at* http://www.dtic.mil/whs/directives/corres/html/514301.htm.

particularly with respect to budgetary and program management functions, DoD needed to provide a single authorized point of contact.

The internal DoD initiative that contributed to the creation of CIFA predated the CI-21 process, though it resembled it in some respects. In the mid- to late-1990s there was growing concern in DoD about the protection of technology critical to military operations, as well as the protection of critical infrastructure. Some of this concern mirrored the national concern regarding critical infrastructure protection that was a powerful presence in the defense and intelligence communities in the late 1990s.[159] DoD's particular concern was that its critical technologies might be compromised by espionage, computer intrusion, or "open source" collection by foreign adversaries.[160] During this period, the term "research and technology protection" (RTP) began to be used to describe efforts to protect DoD's critical technology. At the end of the 1990s, there were both studies and a formal "Mission Area Analysis"[161] focusing on these issues and on general sufficiency of DoD counterintelligence and security components to meet these challenges.

The DoD office that was responsible for these efforts, the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (commonly referred to as ASD(C3I)) created the Joint Counterintelligence Assessments Group (JCAG) in 1999.[162] JCAG was an analytical operation that focused on assessing counterintelligence threats generally and threats to technology in particular.[163] One key idea embodied in JCAG was that of "horizontal technology protection." The idea was that a critical technology should be protected equally across the DoD (i.e., not regarded as highly sensitive in one DoD component and left relatively unprotected in others). Another key feature of the JCAG concept was the

159. This work of the President's Commission on Critical Infrastructure Protection was important in raising broad awareness of these issues, as was concern over the impending Y2K event. *See* Joe D. Whitley, George A. Koenig & Steven E. Roberts, *Homeland Security, Law, and Policy Through the Lens of Critical Infrastructure and Key Asset Protection,* 47 JURIMETRICS J. 259, 260 (2007).

160. All of these concerns are cited in the current version of CIFA's official history, which is available on the CIFA website at http://www.cifa.mil/About%20CIFA/history.asp.

161. *See id.*

162. Information on the creation of JCAG came to light during the investigation of the ABLE DANGER matter. "ABLE DANGER" was an analytical program that was alleged to have identified one or more of the September 11 terrorists prior to the 9/11 attacks. JCAG employed some of the same technologies as ABLE DANGER and thus was noted in the Inspector General investigation of ABLE DANGER. According to these documents, JCAG was created in May 1999. *See* Department of Defense Inspector General, Report of Investigation H05L97905217, "Alleged Misconduct by Senior DOD Officials Concerning the ABLE DANGER Program and Lieutenant Colonel Anthony A. Shaffer, U.S. Army Reserve" (Sept. 18, 2006) at 45-47, *available at* http://www.dodig.mil/fo/foia/ERR/r_H05L97905217-PWH.pdf [hereinafter ABLE DANGER IG Report].

163. While the exact parameters of the JCAG's originally envisioned functions are unclear, the entire operation was subsumed into CIFA, and its surviving functions are described in DoDD 5105.67 at §§6.2.10-6.2.13.

deployment of innovative technology to allow all-source analysts to deal with large amounts of information. From the outset, this involved the potential handling of U.S. person information in the context of broad-spectrum analysis.[164] According to congressional testimony, JCAG "demonstrated how data mining and intelligence analysis could be conducted in a counterintelligence and technology protection capacity."[165] JCAG's data-mining activities, however, did not end with this project. JCAG was associated with the data-mining efforts of the Total Information Awareness (TIA) program[166] and was closely involved in work of DOJ's Foreign Terrorist Tracking Task Force in the immediate aftermath of 9/11.[167] Accomplishing horizontal technology protection entailed a certain ability to coordinate counterintelligence and security activities across the DoD. Though such authority never appears to have been vested in the JCAG, it came to be part of CIFA when, in 2001, the JCAG initiative merged with the external PDD-75 process to form CIFA.

The CIFA Charter, as DoDD 5105.67 is sometimes called, stands as a legal artifact reflecting the tensions in the regulatory environment surrounding DoD counterintelligence. According to the charter, CIFA was established pursuant to the authority vested in the Secretary of Defense by Title 10, U.S. Code.[168] The document contains no specific citation to any provision of Title 10, perhaps because that Title contains no language directly applicable to the organization of DoD counterintelligence activities. The reference to Title 10 is most likely to cite the generic authority of the

---

164. The IG Report noted that this had aroused sufficient concern to lead to a congressional subpoena in 1999 and the subsequent shutting down of a JCAG demonstration project. *See* ABLE DANGER IG Report, *supra* note 162, at 46-47.

165. Erik Kleinsmith, Testimony before the United States Senate Committee on the Judiciary, "Able Danger and Information Sharing," (Sept. 21, 2005), *available at* http://www.au.af.mil/au/awc/awcgate/congress/able_danger_sep05_kleinsmith.htm.Kleinsmith, the former Chief of Intelligence for the US Army INSCOM Land Information Warfare Activity, also testified that the demonstration project "ran throughout the later half of 1999 and our results were ultimately subpoenaed by Congressman Dan Burton's office through the House Reform Committee on November 16th, 1999." *Id.*

166. The participation of JCAG is alluded to in TIA documents obtained through the Freedom of Information Act. JCAG apparently participated in a TIA data-sharing project called Sirocco. *See* DARPA, Total Information Awareness (TIA) System Description Document (SDD), (July 19, 2002), at §4.2, *available at* http://epic.org/privacy/profiling/tia/tiasystemdescription.pdf. This is a lengthy and nearly impenetrable technical document that references JCAG analysts as participants on various charts.

167. *See* Senate Select Committee on Intelligence, "September 11 and the Imperative of Reform in the Intelligence Community" (Dec. 10, 2002) (Additional Views of Senator Richard C. Shelby), at 38. Senator Shelby noted that the purpose of the FTTTF was to develop "deep-access data-mining techniques" and deploy them in the hunt for terrorists operating inside the U.S. *Id.* The FTTTF was co-located in the CIFA facility and "JCAG, a.k.a., the Counterintelligence Field Activity or CIFA" was providing technical support. *Id.*

168. *See* DoDD 5105.67 at §1.

Secretary of Defense to organize the functions of the Department.[169] Somewhat curiously, the document does not cite to paragraph 1.12(e) of the then current version of Executive Order 12,333, which specifically delegates to the Secretary of Defense the ability to assign intelligence functions to DoD components not specifically named in the Order.[170] However, the text of the charter makes it very clear that CIFA was a DoD intelligence component fully subject to the intelligence oversight provisions established by the Executive Order.[171]

After specifying the various counterintelligence functions assigned to CIFA, the charter announces that CIFA shall carry out most of these functions "operating as a law enforcement activity within the Department of Defense pursuant to the authorities vested in the Secretary of Defense in [Title 10]."[172] The language has the effect of "dual-hatting" CIFA with both DoD counterintelligence and DoD law enforcement authorities. One can certainly read in this structure an attempt to enable CIFA to better deal with the pre-9/11 bifurcation of intelligence and law enforcement functions.[173] Prior to the full implementation of the USA PATRIOT Act,[174] the ability to work or handle information on either side of the "wall" would have been critical, especially for an entity that was supposed to coordinate with non-DoD components such as the NCIX and the FBI.

However, in the DoD context, such ability comes at the cost of significant legal ambiguity: How is it decided whether a particular function is being performed as law enforcement or as an intelligence component? Is the information produced or received in each mode handled differently? Which set of rules, DoD 5240.1-R or DoDD 5200.27, is going to apply in any given situation? The CIFA charter contained no guidance, and no public DoD guidance on the coordination of these two rule sets has appeared since the creation of CIFA.[175]

---

169. 10 U.S.C. §113(b).

170. Exec. Order No. 12,333 §1.12(e) (1981) (authorizing the Secretary of Defense to use "other offices within the Department of Defense appropriate for conduct of the intelligence missions and responsibilities assigned to the Secretary of Defense").

171. *See* DoDD 5105.67 at §§6.1 and E2.1.1.1. CIFA is also enumerated as a DoD intelligence organization under the authority of the Undersecretary of Defense for Intelligence. *See* DoDD 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," (Nov. 23, 2005).

172. DoDD 5105.67 at §6.2.17.

173. Put another way, the dual authorities assigned in the CIFA charter would make CIFA follow the model of the FBI, the NCIS, and the AFOSI (all of which locate counterintelligence and law enforcement functions in a single organization), rather than the Army model (which divides the functions into separate organizations). *See supra* note 16.

174. Though enacted on October 26, 2001, the full effect of the USA PATRIOT Act in removing the "wall" separating intelligence and law enforcement was delayed by the In re Sealed Case litigation. A fully "wall-less" environment did not really exist prior to the publication of the revised Attorney General guidelines for national security investigations in late 2003. *See supra* note 4.

175. See discussion *supra* notes 135-144. It is theoretically possible that such guidance

CIFA was, in many senses, a forward-looking organization. Its operational integration of counterintelligence and law enforcement nicely prefigured the post-9/11 investigative environment. However, since this operational integration occurred within the DoD, it happened without the concurrent harmonization of legal authorities that eventually occurred in the civilian environment.[176] Getting out ahead of a solid legal framework was certainly a contributing factor in the TALON database incident. In retrospect, the seeds of the TALON problem were there in the CIFA charter. The full extent of the operational integration is difficult to assess from public sources. However, for a substantial part of its history, a central portion of the CIFA structure was the Counterintelligence Law Enforcement Center (CILEC), which appeared to serve as a fusion center for counterintelligence, law enforcement information, and force protection information.[177] While it remains difficult to document the precise function of the CILEC, the Defense Criminal Investigative Service (DCIS), a DoD law enforcement entity that participated in the CILEC, inserted this description into a recent budget document: "The CILEC, consisting of contractors, analysts, and military personnel, is responsible for facilitating, integrating and deconflicting DCIS and other DoD law enforcement information within CIFA and at the DoD, National, and International levels."[178]

In a similar vein, the CILEC mission is described in contract documentation:

> The mission of the CILEC is to identify and assess threats to DoD personnel, operations, research, technology, infrastructure, and information and capabilities, from foreign intelligence services, terrorists, and other clandestine or covert entities, including insiders; plan, manage and direct CI Campaigns and other priority CI and national security-related law enforcement (LE) activities to mitigate, neutralize or exploit threats; integrate CI, security, intelligence, and law enforcement information bearing on those threats; provide actionable intelligence, CI Common Operating

---

could have been issued in a classified or nonpublic forum, though this seems unlikely, because the full text of both existing rule sets have been publicly available since their publication.

176. Arguably, the civilian integration of law enforcement and counterintelligence/ counterterrorism is still far from complete, but substantive guidance certainly exists in the form of the revised Attorney General guidelines.

177. *See* Office of the Inspector General, "Operation and Maintenance, Office of the Inspector General Fiscal Year (FY) 2008/ FY2009 Budget Estimates" at OIG-870, *available at* http://www.defenselink.mil/comptroller/defbudget/fy2008/budget_justification/pdfs/operation/O_M_VOL_1_PARTS/28_OIG.pdf.

178. *Id*.

> Picture (CI COP), and information products to Defense and national decision makers.[179]

The operational blending of counterintelligence, law enforcement, and force protection that was observed in the TALON incident seems to have been institutionalized in the structure of CIFA.[180]

The CIFA charter embodies other tensions in the regulatory milieu. For example, the Title 10 question of the placement of counterintelligence operational functions within the military services (as opposed to with the joint command or DoD structure) is evident in the "savings" language of Paragraph 6.2.17, which indicates that, though CIFA is authorized to operate as a law enforcement activity, it (as a DoD entity) is not in any way to supplant the existing investigative jurisdiction of the military services (and the DCIS).[181] On the surface, this provision would seem to apply only to law enforcement operations, but the section states that "CIFA shall not engage in the investigation, apprehension, or detention of individuals suspected or convicted of criminal offenses against the laws of the United States."[182] Inasmuch as "crimes against the laws of the United States" would include espionage, acts of terrorism, and providing material support to terrorist organizations, the restriction would sweep in most counterintelligence operations as well. CIFA, like many other umbrella organizations, appears to have been the product of a compromise that allowed it to "manage" the programmatic aspects of DoD counterintelligence without actually conducting investigations and operations. This tension between the DoD-centric authorities of CIFA and the Title 10 authorities of the military services was recognized as limiting CIFA's ability to accomplish the objectives of PDD-75 by the WMD Commission, which in 2004 conducted a broad review of Intelligence

---

179. The text is drawn from a summary of a Blanket Purchase Agreement (BPA) awarded to Lockheed Martin to provide analytical support to CIFA. The summary of BPA FA4814-04-A-0011 is posted on the Lockheed website at http://contracts.lmsource.com/index.cfm?regid'%22%2E%40%20%20%0A&fwnavid'%22%2E%40L%20%0A&navMode'%28%3FT%3D%3A%28Y%3EJ%3B1%5C%20%0A. This description resembles that provided in a 2005 CIFA Information Paper obtained through a Freedom of Information Act request. *See* National Security Archive Electronic Briefing Book No. 230, Document 3b, *available at* http://www.gwu.edu/~nsarchiv/ NSAEBB/NSAEBB230/03b.pdf.

180. The present status of the CILEC is unclear. It is mentioned in a budget document that was created in 2007, *see supra* note 177, and it appears on an undated organizational chart obtained through the Freedom of Information Act, *see* National Security Archive Electronic Briefing Book No. 230, Document 3a, *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB230/03a.pdf, but it does not appear on the organizational chart posted at the time of this writing on the CIFA public website. *See* http://www.cifa.mil/About%20 CIFA/org.asp. Interestingly, the CIFA website referenced a major reorganization in 2007, *see id*., and posted a set of "Strategic Goals" that contain no mention at all of law enforcement. *Id.*

181. DoDD 5105.67, §6.2.17.

182. *Id.*

Community functions.[183] The Commission recommended increasing CIFA's operational authority over the military services.[184] The DoD demurred somewhat and in late 2005 gave CIFA "mission tasking authority," which allowed CIFA to "task a Military Department CI organization or a Defense Agency's organic CI element to execute a specific CI mission or conduct a CI function within that organization's charter."[185] This authority, while it allowed CIFA to better orchestrate DoD counterintelligence agencies, stopped short of enabling CIFA to actually engage in those activities. It seemed to indicate that the DoD did not envision CIFA developing into a "full-spectrum" counterintelligence agency that would ultimately absorb DoD counterintelligence – or even any particular counterintelligence function or mission set – into one organization.[186] After announcing plans in the summer of 2007 to shrink and re-focus CIFA on traditional counterintelligence functions, DoD actually disestablished CIFA as an independent organization in the summer of 2008 and integrated its functions into the newly created Counterintelligence and HUMINT Center within the DIA.[187] There is as yet little public indication of how the operations formerly housed in CIFA will actually function within the DIA.

Despite the uncertainty of its current status, the presence of CIFA has already been felt in the regulatory environment. In the first five years of its existence, the Office of the Under Secretary of Defense for Intelligence has overseen the revision and reissuance of a number of DoD Instructions relevant to counterintelligence.[188] The most notable revision in most of these documents was the inclusion of CIFA and its new functions. For example, in the new version of DoD Instruction 5240.10, which deals with

183. *See* WMD COMMISSION REPORT, *supra* note 89, at 483-497.

184. *Id*. at 493-495.

185. Office of the Undersecretary of Defense, "Background Paper: Department of Defense Counterintelligence Field Activity" (Dec. 1, 2005), *available at* http://www.cifa.mil/Library%20and%20References/documents/Mission%20Tasking%20Authority.pdf.

186. *See id.* at 1.

187. *See, e.g.,* Keith Costa, "Clapper Approves Sweeping Reorganization of Pentagon Coutnerintelligence," InsideDefense.com (June 28, 2007), and Keith Costa, "New DoD Strategy for Counterintelligence in the Works," InsideDefense.com (July 12, 2007). These two press reports, which CIFA has posted on its website at http://www.cifa.mil/Library%20and%20References/12Jul07.asp, indicated that CIFA was likely to be downsized and would receive a new charter. *Id.* On August 4, 2008, DoD announced that CIFA was disestablished and that CIFA "resources and responsibilities" were to be combined with DIA's counterintelligence and HUMINT capabilities in the new Defense Counterintelligence (CI) and Human Intelligence (HUMINT) Center within DIA. *See* Department of Defense Press Release No. 651-08, DoD Activates Defense Counterintelligence and Human Intelligence Center, (Aug. 4, 2008), *available at* http://www.defenselink.mil/releases/release.aspx?releaseid'12106. The press release notes that CIFA's law enforcement authority did not transfer to the new center. *Id.*

188. Given CIFA's role in policy development, *see* DoDD 5105.67, §6.2.2, it is likely that CIFA staff had significant input into the development of these new Instructions.

the coordination of counterintelligence operations with the work of the combatant commands, CIFA's first enumerated responsibility is to

> ensure that force protection and critical asset protection horizontal risk assessments are conducted and products provided in a timely manner to principals in the office of the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, the Military Departments, the Combatant Commands, the Defense Agencies, and other DoD Components, as required.[189]

The new Instruction on counterintelligence "functional services" recognizes the role of CIFA and directs all DoD counterintelligence components to conduct "CI activities in support of force protection, to include participation in CI surveys and vulnerability assessments and surveillance detection."[190] There is an intriguing post-CIFA revision to an Instruction entitled "The Force Protection Response Group," but the text of that Instruction is classified.[191] CIFA's role in the TALON process was institutionalized in the new instruction on counterintelligence collections management.[192] Finally, the new instruction on counterintelligence analysis and reporting directs CIFA to establish a "strategic analysis capability" and to "conduct CI analysis for horizontal protection, research and technology protection, and critical infrastructure protection."[193]

The post-CIFA revisions of DoD counterintelligence instructions are significant because they represent the institutionalized expectations of the clients of DoD counterintelligence (i.e., the combatant commands, the defense agencies, the Office of the Secretary of Defense). Whether the mission is ultimately performed by a former CIFA component now absorbed by DIA or some successor component, it is clear that broad-spectrum collection and analysis, as well as TALON-like force protection services, are now viewed as integral to the DoD counterintelligence function. The post-9/11 need for fusion of intelligence and law

---

189. DoDI 5240.10, "Counterintelligence Support to the Combatant Commands and the Defense Agencies," (May 14, 2004) §5.2.2.1. This instruction also offers some perspective on the complexity of the relationship between counterintelligence components and the combatant commands that are a consequence of the Goldwater-Nichols language in Title 10.

190. DoDI 5240.16, "DoD Counterintelligence Functional Services" (May 21, 2005), §6.2.6.

191. *See* DoDI S-5240.15, "The Force Protection Response Group (FPRG)" (Aug. 26, 2005). The unclassified title of this Instruction appears in the online depository of DoD issuances at http://www.dtic.mil/whs/directives/ corres/html/524015.htm. The notation there indicates that the text of the Instruction is classified and that it was last revised on August 26, 2005. *Id.*

192. DoDI 5240.17, "DoD Counterintelligence Collection Reporting" (Oct. 26, 2005), §5.7.8.

193. DoDI 5240.18, "Counterintelligence Analysis and Production," (Dec. 4, 2006), at §§5.3.2 and 5.3.3. *See also* DoDI 5240.19, "Counterintelligence Support to the Defense Critical Infrastructure Program" (Aug. 27, 1007) (noting CIFA's organizational role in this program).

enforcement information, the importation of force protection to the domestic environment, and the application of integrated analysis and data-mining efforts in the counterintelligence environment all prompted immediate operational responses (like TALON, TIA, and similar efforts). The evolution of CIFA and DIA counterintelligence and the attendant changes in the regulatory milieu suggest that these responses have been institutionalized and identified with the mission of DoD counterintelligence.

CONCLUSION

The current state of DoD counterintelligence is one of dystopic evolution. Counterintelligence has acquired new limbs but not the capacity to regulate them in symmetrical motion. The operational culture of DoD counterintelligence has assimilated the imperatives of force protection, homeland defense, and information fusion, but the legal culture that would balance these imperatives with the protection of civil liberties remains a pastiche of unintegrated authorities. In this state, DoD counterintelligence operators have been able to pick and choose between competing rule sets – a risky practice that should not be allowed to become ingrained in the operational culture. Those DoD counterintelligence components now are interacting more directly with domestic civil society. Under the present legal framework surrounding these activities, this is cause for real concern, which should be a catalyst for a comprehensive upgrade of that framework.

Too often, however, reflection and scholarship in areas that touch on counterintelligence activities focus narrowly on a specific program or topic that brings the national security/civil liberties question into sharp focus. Our argument is that the present regulatory difficulties are the result of deep tensions in the foundations of counterintelligence activities, beginning with the taxonomy that establishes the boundaries of the discipline itself. As counterterrorism has been militarized, the relationship between counterintelligence components and the military command structure becomes critical. Now that broad-spectrum all-source analysis in a hybrid information-sharing environment is challenging focused investigation as the dominant paradigm of counterintelligence, the rules governing the use of U.S. person information need to fit this model as well. All of these tensions between existing legal authorities and the operational culture would require a broad approach to revision, one that should be grounded in a deep understanding of both the relevant culture and the law. The process of revision, if it is to succeed with DoD counterintelligence, must not stall at the level of legal theory or national policy – it has to be followed through all the way down through the levels of internal guidance (e.g., DoD Directives and Instructions, as well as the specific implementing regulations of the specific military services and defense agencies). In our research, we noted a real dearth of systematic legal scholarship on the regulatory

environment internal to DoD. Yet this is the level of regulation that most directly shapes the operational culture.

There are three particular areas in which existing legal authorities need serious reexamination. The first, and most obvious, is the revision of DoD's intelligence oversight rules (DoD 5240.1-R) to reflect the post-USA PATRIOT Act information-sharing environment. In essence, the DoD should implement an integrated approach to counterterrorism investigations, something similar to the structure found in the Attorney General's Guidelines for the FBI. If DoD components are going to interact with civilian law enforcement on JTTFs and other counterterrorism initiatives, then the DoD rules should be fully consistent with their civilian counterparts. An integrated approach would eliminate the ambiguities that seem to prompt ad hoc choices between rule sets. The revision should, like the new Attorney General guidelines, contain provisions for threat assessments that would suffice to meet the DoD's force protection requirements, and otherwise unambiguously integrate the idea of force protection.

Second, DoD counterintelligence, like its civilian counterparts, needs the benefit of a legal construct that addresses the application of broad-spectrum collection and analysis techniques such as data-mining, link analysis, and SIGINT collection in environments populated with U.S. person data.[194] This is particularly critical in the DoD because these techniques have already matured in the foreign intelligence environment, and they stand so tantalizingly available to political calls for the deployment of more powerful tools against the terrorist threat. The current rule sets, reflecting the traditional taxonomy of foreign intelligence and counterintelligence, do not adequately address the use of these techniques when encounters with U.S. person data are more than incidental. In U.S. person environments, the existing rules assume an ability to make individual assessments of data that are increasingly unrealistic in a digital world. The result is to create all-or-nothing counterintelligence where the ambiguities of multiple rule sets can be leveraged to enable broad collection.

Third, we need to reexamine, and clarify, the meaning of Title 10 of the U.S. Code in relation to intelligence and counterintelligence activities. The exclusion of the intelligence functions from the dominant chain of military command does not serve us well when we encounter international terrorists

194. There have been previous attempts to initiate this process. In 2003, the Secretary of Defense, responding to concerns about TIA and data mining generally, appointed the Technology and Privacy Advisory Committee (TAPAC) to examine the use of advanced information technologies. The TAPAC report, issued in March 2004, contained a very useful analysis of the issues. *See* Technology and Privacy Advisory Committee, "Safeguarding Privacy in the Fight Against Terrorism" (2004), *available at* http://www.cdt.org/security/usapatriot/20040300tapac.pdf. Unfortunately, the Report did not prompt any significant revision of operational authorities or any new legal guidance within the DoD.

(a traditional counterintelligence target) as a military adversary. The idea that there are separate military (Title 10) and intelligence (Title 50) legal foundations for essentially the same types of activities is dangerous and threatens the same dysfunctional choice of law options that have plagued the counterintelligence environment in other contexts. Giving counterintelligence a truly unified command structure in DoD is a prerequisite to achieving unified oversight and regulation.

These three undertakings are daunting, each in its own way. All three, however, aim to harmonize legal oversight with the observed evolution of the counterintelligence mission. Evolution here, like elsewhere, moves in only one direction, since the post-9/11 features of the DoD counterintelligence mission are not going to recede. As we once again consider adjusting the regulatory environment in response to the specter of abuse, we should ensure that the improvements in legal oversight are as fundamental as have been the changes in the activities they govern.