

Chapter Four



Finding the Enemy Within



Finding the Enemy Within: Towards a Framework for Domestic Intelligence

DAVID HEYMAN

Director, Homeland Security Program
Center for Strategic and International Studies

*Military Expands Intelligence Role in US*¹

*Pentagon, CIA Get Financial Data*²

*Bush Warned About Mail-Opening Authority*³

*FBI Finds It Frequently Overstepped in Collecting Data*⁴

These headlines are some of a steady stream of stories cropping up about government collection of information on Americans in the fight against terrorism. In each case, the story sparks controversy and the Administration defends the actions as legal, necessary, and not unduly intrusive. But these assurances do not relieve public unease about a growing domestic role for national security agencies that traditionally have focused their attentions outward.

Of all the issues that we have wrestled with since 9/11, perhaps none has received more consideration or attention in discussions on homeland security than the acknowledged shortcomings of intelligence—in collection, analysis, and sharing—prior to the September 2001 attacks. In the United States, intelligence collection is split between agencies that look outside of our borders (e.g., the military, the Central Intelligence Agency [CIA]) and those that look inward (the Federal Bureau of Investigation [FBI]). And while there has been significant attention paid to the reorganization, revitalization and resourcing of

1. *The New York Times*, Sunday, January 14, 2007, Eric Lichtblau and Mark Mazzetti, p. A1.
2. *The New York Times*, Sunday, January, 14, 2007, Eric Lichtblau and Mark Mazzetti, p. A17.
3. *The Washington Post*, Friday, January 5, 2007, Dan Eggen, p. A3.
4. *The Washington Post*, Thursday, June 14, 2007, John Solomon, p. A1.

our foreign intelligence services, far less attention has been paid to the domestic side of the equation.

There is, however, a clear new need and many new activities emerging to bolster intelligence capabilities to support post-9/11 homeland security/defense missions. And yet the increase in domestic intelligence (DI)⁵ collection has moved forward with little public discussion, no apparent framework, and little oversight. This raises the prospect of an emerging domestic intelligence ‘system’ where all the pieces don’t fit together, pieces are missing or redundant, and there is no framework for protecting individual liberties. To address DI responsibly requires answering fundamental questions about what agencies should be responsible for collecting intelligence within the United States; what types of domestic information the government should collect, and how it should be used; and how the government needs to coordinate and oversee the process to assure effectiveness and protection of civil liberties.

The Need for Domestic Intelligence

Increased focus on DI is a necessary response to the threat posed by international terrorism. Terrorists live, work, plan, and act all over the world, including within our borders. They move and communicate with relative ease between foreign capitals and U.S. cities. The 9/11 attacks represent a failure of intelligence agencies—foreign and domestic—to communicate and coordinate as the planners and perpetrators lived within and traveled in and out of the United States for months prior to the attack, with little notice.

Despite our success in Afghanistan, eliminating a regime that had provided safe haven for terrorists to train and launch operations to attack us, terrorism has neither been quelled nor conquered. To the contrary, terrorist recruitment and terrorist attacks continue to expand. Homegrown terrorism is on the rise in Europe, Australia, and North America, and the spread of radical Islamist ideology has

5. The term “domestic intelligence” used in this article is shorthand for intelligence – relating to threats of grievous harm to U.S. national security, including from foreign powers, persons, or from international or ‘home grown’ terrorism – collected on individuals located within the United States.

hastened, gaining traction in fragile democratic states from Lebanon to Indonesia.

Countering threats abroad cannot substitute for strengthening protection at home. We must be able to anticipate, prepare for, and interdict attacks at home. Because the threat at home is greater now than during the Cold War, when we worried more about attacks from nation-states abroad than from non-state attackers on American soil, confronting this threat requires greater understanding of domestic information and more flexibility in sharing analysis, and the use of that information.

Emerging Elements of Domestic Intelligence

To address the much-recognized need for intelligence reform following the 9/11 attacks, the U.S. government instituted a series of some of the most sweeping reforms of the nation's intelligence apparatus since the end of World War II. Among the changes following the 2001 attacks are the creation of new organizations, new missions, and new positions. They include:

- Establishment of the Homeland Security Council (HSC) at the White House to coordinate all homeland security-related activities among executive departments (including related-intelligence); and specifically, setting-up a Homeland Security Policy Coordination Committee (HSC/PCC) for the expressed purpose of coordinating interagency policy on detection, surveillance, and intelligence.⁶
- Establishment of a new homeland defense mission for the U.S. military, a new Northern Command (USNORTHCOM) responsible for providing command and control of Department of Defense (DoD) homeland defense and civil support efforts, and a new Assistant Secretary of Defense for Homeland Defense (ASD/HLD) to provide homeland defense related guidance for USNORTHCOM.⁷ Both ASD/HLD and USNORTHCOM will

6. The White House, *Homeland Security Presidential Directive-1 (HSPD-1)*, October 29, 2001. <http://www.fas.org/irp/offdocs/nsdp/hspd-1.htm>.

7. Department of Defense. *Special Briefing on the Unified Command Plan*. Washington: Wednesday, April 17, 2002. <http://www.fas.org/irp/news/2002/04/dod041702b.html>.

require intelligence to perform their duties to protect America at home.

- Formation of a new National Security Branch (NSB) at the FBI to protect the United States against weapons of mass destruction, terrorist attacks, foreign intelligence operations, and espionage.⁸
- Creation of an Undersecretary for Intelligence at DoD charged with integrating defense intelligence, surveillance, and reconnaissance capabilities to better provide warnings, actionable intelligence and counter-intelligence support necessary for national and homeland.⁹
- Establishment of a new assistant secretary for Information Assurance and Infrastructure Protection at the Department of Homeland Security (DHS) (transformed today to Assistant Secretary for Intelligence and Analysis) to identify and assess current and future threats to the homeland, map those threats against our current vulnerabilities, inform the President, issue timely warnings, and immediately take or effect appropriate preventive and protective action.¹⁰
- Induction of the U.S. Coast Guard—responsible for protecting U.S. economic and security interests in any maritime region including America’s coasts, ports, and inland waterways—into the U.S. intelligence community and establishment of the Coast Guard Intelligence Coordination Center as it’s primary interface with the collection, production, and dissemination elements of the national intelligence and law enforcement communities.¹¹
- Creation of the National Terrorist Threat Integration Center (now the National Counterterrorism Center or NCTC), an interagency

8. Federal Bureau of Investigation. *National Security Branch Overview*. ONLINE. Washington: Department of Justice, September 2006. <http://www.fbi.gov/filelink.html?file=/hq/nsb/whitepaper12-06/whitepaper.pdf>.

9. Department of Defense. *Directive Number 5143.01*, November, 2005. http://www.fas.org/irp/doddir/dod/d5143_01.pdf.

10. United States Congress. *Homeland Security Act of 2002*. <http://news.findlaw.com/hdocs/docs/terrorism/hsa2002.pdf>.

11. United States Congress. *Intelligence Authorization Act for Fiscal Year 2002*. <http://thomas.loc.gov/cgi-bin/query/D?c107:6:./temp/~c107wuVNfa>.

body intended “to provide a comprehensive, all-source-based picture of potential terrorist threats to U.S. interests.”¹²

- Consolidation of all U.S. intelligence functions and activities to be coordinated under a newly created Director for National Intelligence (DNI).¹³

The approach to initiating and implementing DI reforms, however, has been ad hoc, fragmented and has emerged without a strategic vision to follow. In October 2005, the new Office of the Director of National Intelligence (ODNI) issued its blueprint for building “an integrated intelligence capability to address threats to the homeland, consistent with U.S. laws and the protection of privacy and civil liberties.”¹⁴ Despite this effort, the document failed to develop specific roles and missions, clear rules for collection, or how information should be shared among intelligence partners and other associated homeland security stakeholders.

In a world where non-state actors can gain asymmetric advantage by operating within the gaps of a dysfunctional or inefficient bureaucracy, one of our goal’s must be to deny terrorists safe harbors in the seams of society—seams between foreign and domestic, civil and military, federal and state, public and private, and even agency to agency—but to do so while also ensuring that we uphold the pillars that are at the heart of America’s constitutional identity—federalism, liberty, and justice. This requirement raises complex legal and policy issues because by its nature, DI collection affects the privacy and civil liberties of U.S. citizens and residents.

Problems in the Absence of a Domestic Intelligence Framework

If there is no framework for DI, no clarity about roles and responsibilities in its collection, each agency will set out on its own to get what it needs. Such activities can have negative consequences not only for

12. United States Congress. *Intelligence Reform and Terrorism Prevention Act of 2004*. http://www.nctc.gov/docs/pl108_458.pdf.

13. *Ibid.*

14. Office of the Director of National Intelligence, *The National Intelligence Strategy of the United States of America: Transformation Through Integration and Innovation*, October 2005: 11. <http://www.odni.gov/publications/NISOctober2005.pdf>.

civil liberties, but also for effectiveness. On the civil liberties side, an undefined, potentially unlimited program of covert surveillance of the American public raises huge privacy concerns, both in perception and in practice. In terms of effectiveness, when collection roles overlap or are not clearly defined, there is great risk that players will trip over each other by pursuing the same leads or sources, or will miss something because they believe others will pursue it. These or other mishaps could compromise important and sensitive activities.

The world of intelligence is largely closed. As a consequence, public debate is often limited between those who are un-informed or poorly informed. Those who have the facts are constrained by secrecy requirements from discussing the details, or, in some cases, even the broad outlines of the activities. Those who ‘know’ can stymie public discourse with arguments that any discussion would telegraph the nature or details of government collection to our enemies. Those that ‘don’t know’ can inspire public fear and diminish public confidence by imagining the worst.

The Bush Administration and its national security officials have generally shied away from any broad discussion of how they will address the increased need for domestic intelligence. In his confirmation hearings, the new DNI, Michael McConnell, stated that the Intelligence Community has been “trained for years to think external, foreign,” but stressed that with the terrorist threat it is important to “think domestically.”¹⁵ The ODNI, however, has so far been reluctant to take responsibility for setting a policy framework for collection and use of domestic intelligence. This leaves each agency to make its own judgments about what information it needs and how to get it.

When it comes to discussing this issue, outside of the government, experts have tended to focus primarily on an organizational question: should the FBI remain the country’s DI agency or should we separate the intelligence and law enforcement functions and create the U.S. equivalent of MI-5, the United Kingdom’s domestic intelligence service.

15. Senate Select Committee on Intelligence. *The Nomination of Mike McConnell to Be Director of National Intelligence*. Hearing, February 1, 2007. Washington: Office of the Director of National Intelligence, 2007. <http://intelligence.senate.gov/hearings.cfm?hearingId=2482>.

This is an important question, but it is not the only question, and it should not be the first. What is most important is for the government to create a consistent and clear framework for its collection and use of DI. To do that it must answer three questions:

- Who can collect domestic intelligence, and why?
- What domestic intelligence can the government collect, and how?
- How must the government coordinate and oversee the process?

Who Can Collect Domestic Intelligence and Why?

To be clear, there are three primary roles that intelligence agencies perform: they collect intelligence, carry out clandestine operations, and engage in analysis. Collection might involve clandestine electronic or physical surveillance, use of human sources (including by means of interviews or interrogations), imagery or photo-surveillance, or seizure of records or other physical materials. Operations or actions—which to date has been less common in the DI context—might include undercover operations or disruption activities.¹⁶ Analysis necessarily involves access to all these sources of information, including in some cases private information, for the purposes of providing policy advice or threat information.

The source of information—of ‘domestic intelligence’—whether related to operations or analysis, is collection. Collection and operations are the functions that involve the greatest potential intrusions on individual privacy or liberty. Many concerns of the public regarding collection stem from a fear that a government unchecked and without proper limitations of law or oversight, as has been experienced at times in America and throughout history, will lead to unconstitutional abuses of government authority. In particular, some point to the danger inherent in the government collecting vast amounts of personal data on any and all persons, and that such information would be made available to any government agency for any future use, particularly in ways that the affected individuals may have no knowledge or ability to seek redress. Unlimited collection would not only be an invasion of privacy, it would be counter to the common expectation of Americans

16. Overt actions such as screening or denial of a benefit might also be based on intelligence, although they are not typically regarded as intelligence functions.

to be free to be left alone. Even the perception of unchecked intelligence diminishes greatly the public's trust in government. Further, when the public learns through news leaks of unwarranted, potentially unlawful collection, it leaves many asking what else is going on?

In the late 1970s the Senate Committee known as the "Church Committee" uncovered government abuse in the collection and use of DI.¹⁷ One of the reforms implemented after those revelations was to limit significantly the roles of national security agencies for collecting intelligence within the United States. By Executive Order and internal regulation, the policy since that time generally gave the FBI responsibility for domestic collection—both law enforcement and intelligence. Other national security agencies were to refrain from domestic intelligence collection or operations.

Since September 11, 2001, with the recognition of a greater need for Domestic Intelligence, the policy of FBI's lead and other agencies' restraint has become less clear. As noted above, no fewer than four agencies now play some role in DI today. For reasons of efficiency and of privacy, it is vitally important to define clearly the roles and missions of the various national security agencies in the collection of DI, and take care to avoid duplication of those roles or overstepping and abuse. Having too many agencies responsible for the collection of domestic information is a recipe for harmful errors, controversy, and diminished oversight. To enhance clarity and efficiency, as a general rule, one agency (the FBI, under the existing structure) should be responsible for intelligence collection and operations within the United States. Other national security agencies should be limited to collecting intelligence

17. The Church Committee – the 1976 Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, chaired by Senator Frank Church – recommended numerous reforms after uncovering serious abuses when it examined the history of domestic intelligence activities in the United States. The Church Committee found that from the late 1930's through the early 1970's, "intelligence agencies collected vast amounts of information about the intimate details of citizens' lives and about their participation in legal and peaceful activities" and used that information to abuse the privacy and liberties of U.S. citizens and residents. Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate, *Intelligence Activities and the Rights of Americans* ("Church Committee Report"), bk.2 (Washington D.C.; 1976) p.7. <http://www.aarclibrary.org/publib/church/reports/contents.htm>

within the United States when it is uniquely within their mission or capability, and when they can demonstrate why the FBI cannot serve their needs. And all agencies must have clear and direct paths for information sharing.

Some considerations for developing clear agency DI roles and responsibilities include the following.

The Federal Bureau of Investigation

The FBI is the primary domestic intelligence agency responsible for collecting intelligence within the territory of the United States. Many commentators have discussed the challenges for the FBI in its intelligence role. The FBI's background as a law enforcement agency means that it has primarily emphasized reaction—capturing and prosecuting criminals after the fact—more than prevention. In cases where the FBI has, for example, infiltrated groups to prevent a crime, the focus again is on law enforcement and prosecution. A law enforcement agency is not accustomed to the jobs of providing warning, assessing vulnerabilities, or informing policy-makers. Rewards and incentives in the FBI have tended to be for law enforcement successes, and movement to an emphasis on intelligence successes has been halting. On the other hand, there are important synergies between the law enforcement and intelligence roles. The basic mechanisms of collection—surveillance, use of human sources, undercover operations, and review of records—are similar between the two disciplines, so many skills transfer from one to the other. But there are also differences, primarily that law enforcement conducts cases on activities one is generally already aware of; intelligence, by contrast, attempts to uncover things one was not aware of.

It is a monumental task to take on a new mission and change the culture of an organization. The FBI has a long way to go to build up an experienced, capable cadre of domestic intelligence officers and a functional process for collecting and sharing DI at the headquarters and field levels. Some argue that the answer is to create a separate agency to focus exclusively on domestic intelligence. The challenges of building this capacity from scratch, however, would be extraordinary, including

establishing a new agency culture and a place in the notoriously turf-conscious national security community.

Whatever the ultimate answer to this question, what is clear is that we need one agency to have primary responsibility for intelligence collection and operations within the United States. Right now, that is the FBI and it must reinvigorate its move toward becoming effective in this area. Responsibilities of other agencies should be limited to situations in which, because of a unique capability or mission, they are better suited than the FBI to engage in the collection.

The Department of Defense

The role of the DoD in DI collection has been the greatest recent source of confusion and controversy. With its new domestic military mission—the homeland defense mission of USNORTHCOM—there has been a legitimate need for intelligence to support that mission, but also real concerns that DoD is seeking a much larger role in collection of intelligence within the United States and against U.S. persons.¹⁸

In 2002, for example, Deputy Secretary of Defense Paul Wolfowitz launched the Counterintelligence Field Activity (CIFA) program. The mission of the program is:

*to develop and manage DoD Counterintelligence (CI) programs and functions that support the protection of the Department, including CI support to protect DoD personnel, resources, critical information, research and development programs, technology, critical infrastructure, economic security, and U.S. interests, against foreign influence and manipulation, as well as to detect and neutralize espionage against the Department.*¹⁹

18. US Code Title 50 § 1801 (i) states that a “United States person” means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101 (a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power. http://www.law.cornell.edu/uscode/uscode50/usc_sec_50_00001801----000-.html.

19. United States Department of Defense, Directive Number 5105.67. Department of Defense Counterintelligence Field Activity (DoD CIFA), February 19, 2002.

What is noteworthy is the extraordinary broad scope of this mission that could extend beyond bases, and military facilities and into communities. In fact, under CIFA, the DoD established TALON (Threat and Local Observation Notice), a controversial program to gather raw, non-validated information about threats to the community surrounding DoD facilities to assist in early detection of threats to prevent attacks.²⁰ TALON is similar to and grew out of a program called Eagle Eyes, an Air Force anti-terrorist community watch program that “enlists the eyes and ears of Air Force members and citizens in the war on terror.”²¹

Following a 2006 Defense Department Freedom of Information Act release to the ACLU, the ACLU discovered that the TALON database included data on peaceful, law-abiding protesters as potential threats to the U.S. military, as well as 2,821 reports containing information on U.S. persons.²² Further, the ACLU found that other government agencies had been granted authority to access and use data from TALON, leaving the possibility that even if data were deleted from one source, it might still be maintained indefinitely in files of other government agencies, thus raising serious privacy concerns.²³ The DoD recently announced its decision to end the TALON program.²⁴ In doing so, James Clapper, the new Undersecretary of Defense for Intelligence, said it is “important that the proper balance be struck between the counterintelligence mission, on one hand, and the protection of civil liberties, on the other.”

In general, the DoD’s mission and supporting policies currently do not clearly delimit its role in DI; rather, in some cases they expand

20. See also CQ Homeland, January 31, 2006.

21. See: <http://www.osi.andrews.af.mil/eagleeyes/index.asp>. The Air Force inspector general newsletter in 2003 said program informants include ‘Air Force family members, contractors, off-base merchants, community organizations and neighborhoods.’” (see, “Defense Facilities Pass Along Reports of Suspicious Activity,” Walter Pincus, December 11, 2005, Washington Post. http://www.washingtonpost.com/wp-dyn/content/article/2005/12/10/AR2005121000893.html?nav=rss_nation/nationalsecurity)

22. ACLU. *No Real Threat: The Pentagon’s Secret Database on Peaceful Protest*. January, 2007: 31.

23. *Ibid.*, 5.

24. “Pentagon to End Talon Data-Gathering Program,” Walter Pincus, April 25, 2007, Washington Post. <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/24/AR2007042402540.html>

it. This is perhaps an expected consequence of promulgating a new homeland defense mission to the agency in the absence of a framework for intelligence gathering and use. The Department's current responsibility is to conduct counterintelligence activities in support of DoD components worldwide, including within the United States, and to protect the security of DoD personnel and facilities. The 2003 National Military Strategy defines the overall role of intelligence as follows:

*Intelligence systems must allow commanders to understand enemy intent, predict threat actions, and detect adversary movements, providing them the time necessary to take preventive measures. Long before conflict occurs these intelligence systems must help provide a more thorough understanding of adversaries' motivations, goals and organizations to determine effective deterrent courses of action.*²⁵

More specifically, however, intelligence required for the homeland defense mission may extend beyond military facilities and deeper into civil society:

*The Armed Forces will protect critical infrastructure that supports our ability to project military power.*²⁶

The challenge for policy-makers is to determine the lanes of responsibility and lines of permissibility: what is the appropriate domestic intelligence domain of the DoD and what are the limits of collection? The Department currently has, and should have, authority to collect information on its personnel and its facilities within the United States to support these missions, and more recently in particular, homeland defense, but that authority must be defined clearly and limited so that it does not morph into a general collection authority that duplicates or supplants that of the FBI. Even when collecting information consistent with an appropriate mission, DoD entities should coordinate closely with the FBI, leaving to the FBI the task of carrying out any civilian aspects of the collection.

25. U.S. Defense Department. *National Military Strategy*, 2004: 10.

26. *Ibid.*

The National Security Agency

The National Security Agency (NSA) has the authority to collect signals and communications intelligence on foreign intelligence targets. Since the Church Committee reforms and before 9/11, general NSA policy has been to refrain from intentionally collecting communications to, from, or about persons or entities within the United States.²⁷ The NSA, however, has powerful and unique collection capabilities that could be critical in fighting terrorism. There will be circumstances under which NSA capabilities should be used to intercept communications from or to someone within the United States, but extraordinary care and clarity are necessary for any such role. The NSA's capabilities have great potential for intruding on individual privacy and constitutional rights. In addition, any use of the NSA to collect DI must be coordinated with the FBI and subject to the procedures and requirements of the Foreign Intelligence Surveillance Act (FISA).

The limitations adopted in the 1970s on agencies permitted to collect DI continue to be wise and the foreign intelligence agencies should not share the mission with the FBI. However, the NSA has collection capabilities that the FBI does not have that could be critical in the fight against terrorism. Therefore, the two agencies must cooperate in their efforts.

The Central Intelligence Agency

The CIA, like the NSA, is a foreign intelligence agency that should have no general domestic mission. Unlike the NSA, the CIA does not

27. See, United States Signals Intelligence Directive (USSID) 18, Section 3, July 27, 1993. Exceptions to this policy for interceptions involving individuals located within the U.S. were made only with approval of the Foreign Intelligence Surveillance Court (FISC) and subject to FISA. The reforms of the late 1970s were, in part, a reaction to NSA activities that targeted anti-war and other political activists within the United States. Since September 11, 2001, the NSA has departed from this policy for targeting related to terrorism, at least with respect to some communications between people located within the United States and others overseas (see Hayden testimony). We discuss here only the policy issues, not the legality of this surveillance involving persons located within the United States. There are significant legal issues related to the failure to comply with FISA in conducting this domestic surveillance, which are not discussed here.

have significant unique technical capabilities that are required for DI. To have the CIA running clandestine operations or collecting human intelligence within the United States outside the legal framework governing the FBI's ability to do so, vitiates any guidance, protection, or oversight attached to such sensitive activities, besides being unnecessarily duplicative, inefficient, and dangerous both to privacy and security. The CIA does have two missions that could require it to operate domestically to a limited extent. First, like the DoD, it has missions to conduct counterintelligence activities related to the protection and security of its facilities and personnel, including within the United States.²⁸ Second, its mission to collect human intelligence overseas can have some domestic aspects, such as debriefing people returning from overseas or recruiting non-U.S. persons who are visiting the United States. As with DoD, exactly when and how these domestic responsibilities will be carried out should be spelled out clearly, and they must not be permitted to expand beyond what is necessary to carry out the specific mission.

The Department of Homeland Security

The Department of Homeland Security is the new kid on the block. On December 2003, DHS became the 15th and newest cabinet agency. According to its mission statement, a primary function of the DHS is to “identify and understand threats, assess vulnerabilities, determine potential impacts and disseminate timely information to our homeland security partners and the American public.” To do this, a principle activity of the department is to “gather and fuse all terrorism related intelligence; analyze, and coordinate access to information related to potential terrorist or other threats.”²⁹

With the integration of the U.S. Coast Guard's new intelligence section into the Intelligence Community, and with the establishment of the Directorate for Information Analysis and Infrastructure Protection (now, “Intelligence and Analysis”), the DHS not only has a significant resource element responsible for collection, but also a functional arm that is responsible for fusion, analysis and dissemination as well.

28. Executive Order 12333, sections 1.8 (c) and (h).

29. U.S. Department of Homeland Security, *Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan*, (2004): 10-12.

What remains to be clearly defined is what intelligence DHS is expected to obtain for itself and what it should receive from others. The U.S. Coast Guard, for example, and the borders, customs, and immigration arms of the department all collect information within the U.S. that is relevant to national security.³⁰ The DHS private sector coordinating councils and newly established links to state and local government fusion centers also provide links to a wide network of key industries responsible for protecting critical infrastructure and other governments where potentially relevant threat information may be found. What is important is that collection, fusion, analysis and dissemination responsibilities be defined clearly and limited to the areas of unique DHS responsibility. For collection beyond these responsibilities, DHS should look to the FBI.

Non-Federal Partners—Local Law Enforcement and the Private Sector

One of the dramatic changes since 9/11 is the expansion of the “national security community.” The front lines of war no longer coincide with political boundaries; they are instead in the streets and buildings of our cities and states, at curbside check-ins at airports, turn-styles at stadiums, and in hospital emergency rooms. As a consequence, the battles we must fight are no longer solely the purview of airmen, soldiers, sailors and marines; they now must also be fought by epidemiologists, cryptologists, firefighters, citizens, businesses and local police. As we expand the domain of national security, we expand the domain of those who may require intelligence. Similarly, as we look to these non-traditional, non-federal national security partners for bolstering security, we need to recognize that they too can help provide information from their activities that may contribute to a better understanding of the threat.

To elaborate this concept, DHS defined in its *Intelligence Enterprise Strategic Plan*, a newly identified “homeland security intelligence community” (HSIC). According to the plan, the HSIC “includes the

30. See for example discussion on role of intelligence in achieving maximum maritime domain awareness in U.S. Coast Guard, *National Plan to Achieve Maritime Domain Awareness* and U.S. Coast Guard *Strategy for Maritime Safety, Security, and Stewardship*, January 2007, as well as in U.S. Department of Homeland Security, *National Strategy for Maritime Security*, (2005): 16.

organizations of the [homeland security] stakeholder community that have intelligence elements.” It goes on further to define the stakeholder community as “all levels of government, the Intelligence, Defense, and Law Enforcement Communities, private sector critical infrastructure operators, and those responsible for securing the borders, protecting transportation, and maritime systems, and guarding the security of the homeland.”³¹

An example of one of the more significant stakeholders and newer member of the national security community is the over 13,000 state, local, and tribal law enforcement agencies. As eyes and ears of their local communities, and so-called boots-on-the-ground, these resources represent a potentially substantial force multiplier to federal agents. Local police generally have better relationships within their communities—communities where terrorist plans are often developed. They are more likely to come in contact with those running operations. And they are more likely to assess what constitutes ‘normal’ activities or not. Two of the 9/11 terrorists, for instance, came in contact with local law enforcement. Muhammad Atta, on April 26, 2001, presented his driver’s license during a traffic stop.³² And on September 9, 2001 Ziad Jarrah received speeding ticket in Maryland while driving on I-95.³³

Similarly, terrorist encounters with the private sector could help provide clues to potential threats. Zacharias Moussaoui’s flight instructor became suspicious of him due to the fact that he was so eager to learn how to fly large planes and yet had no desire to obtain a pilots license.³⁴ More recently, a Circuit City employee reported to New Jersey authorities that two men had recently brought him a tape of themselves and eight other men firing automatic weapons while chanting “Allah Akbar” (god is great). The two men had requested that he transfer the tape from VHS to DVD format. This incident sparked a 15 month long investigation ending in the arrest on May 7, 2007, of six men who

31. See U.S. Department of Homeland Security, *DHS Intelligence Enterprise Strategic Plan*, January 2006.

32. *Final Report of the National Commission on Terrorist Attacks Upon the United States*, July 22, 2004: 231.

33. *Ibid.*, 253.

34. *Ibid.*, 247.

were plotting attacks on soldiers training at Fort Dix who were bound for Iraq.³⁵

The changes in the national security environment have increased the need to develop and share information and intelligence across all levels of government and the private sector. As a result, new partnerships between non-federal actors and the historic national security community must be and have been established. These new relationships, in turn, however, raise important questions regarding what information is needed in order for each party to perform its respective security functions, and then ultimately what information can and should be collected, by whom, and shared with whom.

What Domestic Intelligence Can the Government Collect, and How?

The Fourth Amendment of the United States Constitution protects all U.S. persons from unreasonable search and seizure by the government. When it comes to collection, particularly within the United States, ensuring requirements of security and civil liberty is a difficult balancing act, posing the legitimate need for government to seek out and interdict potential terrorist threats within the United States on the one hand, while, on the other hand, preserving the rights and protections afforded to Americans under the Fourth Amendment.

The questions for policy-makers today are, given new and emerging DI requirements, as well as new and emerging roles of government and non-governmental agencies, and a dramatically different environment where threat information may reside, then:

- What may government collect, and how?
- Is all information valid, necessary, and useful?
- Should all means of collection be available and utilized?
- How, if at all, should the government be limited in what it may or may not collect?

35. Geoff Mulvihill, "Tipster in Fort Dix Plot Comes Forward," in the *Associated Press*, May 30, 2007. <http://www.washingtonpost.com/wp-dyn/content/article/2007/05/30/AR2007053000168.html>.

To answer these questions, we need to first consider two aspects of collection: the target of collection and the source of information. The *target* of collection is the person or persons involved in a possible plot or who may know of a possible plot (e.g., a plot to commit a terrorist act or espionage). The *source* of information is where relevant information related to a possible plot resides (e.g., on a computer, on a pad of paper, in someone's mind). The *source* of information is a predicate to the *how*; it also plays an important role in shaping what the government may or may not collect.

Collection is source-specific. It can be acquired by technical means (e.g., signals intelligence or SIGINT, measurement and signatures intelligence or MASINT, and imagery intelligence or IMINT), or non-technical means (e.g., human intelligence or HUMINT, or open source intelligence or OSINT). In a world that is now dependent on information technology for communications and for operations, targets use computer networks to convey, store, or share their secrets. In other words the source of information is increasingly found electronically. That is not to say that person-to-person communications are not still relevant; they are. And direct surveillance, remote observation, and interrogation remain critical elements of collection. But, as a result of the revolution in information technology, there is now a vast store of digital information found in communications over the Internet, through wireless or satellite transmissions, and on computers or personal data assistants (PDAs).

Therefore, in addition to classic techniques of physical surveillance, use of human sources, imagery, interviews, examination of records or other physical materials, collection must also rely on electronic or digital surveillance.

The explosion in digital technology, however, poses a number of challenges. First, there is the challenge of volume. What are the limits of collection? The new challenge today is what are the limits of collection for *unknown* targets—that is how do we find the enemy within, when there is no predicate for suspicion of an individual or individuals. Most of the nineteen hijackers who attacked America on 9/11 were unknown to intelligence or law enforcement officials, and

there was little if any remarkable characteristics or information about them that stood out when they came to the United States.

In an increasingly paperless society, however, where nearly every transaction can be captured and stored digitally, individuals leave behind digital fingerprints in nearly every thing they do, every day. Consequently, when we seek to find the proverbial ‘needle in a haystack’—the enemy within—the supply of potentially useful information is almost limitless. There are perhaps as many databases today to search containing so-called ‘dots’ to connect, as there are types of services available to people—financial profiles, spending habits, phone usage, travel patterns, web-surfing interests, video surveillance files, library borrowing or book/magazine past purchases, among others. Through the use of analytic or data-mining tools³⁶ analysts can find links and patterns that may point to suspicious behavior, or even terrorist links or activities.

But too much information may be almost as bad as not enough. We don’t want to add more hay to the haystack when the needle is already too small to find. For the analyst who must discern critical information from volumes of useless or meaningless information, more data may make the task harder. Further, without clear guidance, the world of data mining can become much like a fishing expedition attempting to catch a guppy with a drift net. In the process other information, perhaps interesting but unrelated, may get caught up in the net. For example, if we are looking for terrorists or terrorist connections, other bad actors (e.g., criminals, tax cheats, or dead-beat dads) or simply embarrassing information (e.g., perversions, obsessions, or illicit affairs) may also materialize. Is that information then useable? For what purpose? Can and should individuals be prosecuted for these other offenses? What becomes of the information? Is it FOIAble (i.e. available to the public)?³⁷ Without clear rules-of-the-road, massive collection may also yield to massive invasion of privacy.

36. Data mining has been defined as “the science of extracting useful information from large data sets or databases.” *Principles of Data Mining* by David J. Hand, Heikki Mannila, and Padhraic Smyth.

37. FOIA – Freedom of Information Act. See 5 U.S.C. § 552. U.S. Government Law (2002). Department of Justice. <http://www.usdoj.gov/oip/foiastat.htm>.

One particular concern with new threats of radical Islamic terrorism is the rise of so-called “homegrown terrorism.” Homegrown terrorism refers to terrorism by individuals born, raised, or based and operating primarily in the United States. In the context of DI, this threat requires some form of collection to help security officials identify, uncover and prevent potential terrorist acts. Current (publicly accessible) limitations on DI, however, restrict government agencies from spying on U.S. citizens unless pre-approved by a Foreign Intelligence Surveillance Court,³⁸ the U.S. Attorney General, or the Director of the National Security Agency, under certain circumstances.³⁹ These restrictions must be carefully reviewed.

What is important is to approach collection of DI in a rigorous and thoughtful way. Data mining is a new and potentially useful tool that can bring non-obvious relationships to analysts’ attention that might otherwise have been overlooked. It is also a tool that may bring unrelated, irrelevant, or even false relations to light. There are clear limitations today against collecting against U.S. persons, yet also rising concerns regarding homegrown terrorism. Clear guidelines must be developed and implemented. Constitutional rights protect American citizens against illegal search and seizure or invasion of privacy. Before collection is to be undertaken, specific questions must be answered, to include:

- What is to be accomplished by collecting the information?
- What type of information should be collected?
- How much information should be collected?
- Where and how long should the information be stored?
- Who should have access to this information and for what purposes?

38. The FISA Court (FISC) is a U.S. federal court authorized under 50 U.S.C. § 1803. Established by the Foreign Intelligence Surveillance Act of 1978 (FISA), the FISC oversees requests for surveillance warrants against suspected foreign intelligence agents inside the United States by federal law enforcement agencies. http://www.law.cornell.edu/uscode/html/uscode50/usc_sec_50_00001803----000-.html.

39. See for example, National Security Agency, *United States Signals Intelligence Directive 18 (USSID 18)* “Legal Compliance and Minimization Procedures,” July 27, 1993. Section 4, “Collection”: 2-6.

- How will unexpected derogatory or potentially damaging information be handled?
- What oversight systems are in place to ensure civil liberties are properly considered and appropriately protected?

Like other types of searches in society that take place without a warrant and that are permissible by law, under some circumstances there may be times when all of these questions cannot be adequately answered, but those times should be few, rare and the exception.

How Must We Oversee the Process?

A significant issue highlighted by the recent revelation that the NSA was carrying on a program of warrantless wire-tapping of Americans is the lack of sufficient oversight over unknown or new programs. It's one thing to have new covert missions, new collection programs, and new intelligence activities to improve situational awareness for homeland security, but without proper oversight poorly designed programs may be left underperforming, agencies that overstep their bounds may go unchecked, and a skeptical public may lose confidence in their government. In each of these circumstances, it does little to improve DI or homeland security.

Oversight for DI currently exists in each of the three branches of government. At the Executive branch level, agencies have independent inspector generals with the power to review intelligence programs (among others) either in part or in whole.⁴⁰ In addition, the Justice Department, which serves as the country's law enforcement agency, may have additional oversight responsibilities in certain circumstances.⁴¹

40. Dan Eggen, "Concord Monitor," in *The Washington Post*, January 11, 2006. <http://www.concordmonitor.com/apps/pbcs.dll/article?AID=/20060111/RE-POSITORY/601110368/1001/NEWS01>. And in some instances, more than one inspector general may have jurisdiction over the given issue.

41. DOJ oversight programs. See, for example, Department of Defense, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*, DoD 4240.1-R, December 1982. See also, Department of Justice, *Attorney General Guidelines on General Crimes, Racketeering, and Terrorism ("Guidelines")*, May 30, 2002.

The Executive branch has statutory obligations to ensure that Congressional Intelligence Committees are kept “fully and currently informed” on intelligence activities.⁴² These obligations extend to the newly created Director of National Intelligence and intelligence agency heads. It requires them to furnish material concerning any and all intelligence activities in a timely manner. The judiciary branch, too, has an oversight function. A court may strike down unconstitutional statutes or improper actions by the Executive branch.

Both the Judiciary and Legislative branches are limited in their oversight by what the Executive branch reveals to them. On certain sensitive matters, where the Executive branch has chosen to limit congressional notification to the so-called Gang of Eight⁴³ (such as the NSA wire-tapping controversy), members of Congress are only made aware of these activities if the Executive branch chooses to inform them, and even then, members generally are not permitted to consult with their staff or any other members, or anyone for that matter, leaving them at some disadvantage in terms of their normal course of review and oversight. Similarly, the Judiciary branch can only adjudicate matters that have been brought to its attention by the Executive branch, if the information is not publicly available elsewhere.

With new DI roles and emerging missions, congressional oversight must be re-examined, particularly for ensuring that government activities that did not previously exist, nor were envisioned under current authorities or previous jurisdictions, are afforded adequate guidance and outside evaluation. Specifically, three over-arching questions must be addressed:

1. Who is responsible for developing the overall DI framework?

Domestic intelligence collection must begin with a domestic

42. See National Security Act of 1947, Secs. 501-503 [50 U.S.C. 413 - 413(b)]. For further discussion on the statutory obligations of the Executive Branch on intelligence matters, see also: Alfred Cumming, Congressional Research Service, *Statutory Procedures Under Which Congress Is To Be Informed of U.S. Intelligence Activities, Including Covert Actions*, January 18, 2006.

43. The “Gang of Eight” is understood to include the Speaker of the House, the Minority Leader of the House, the Majority and the Minority Leaders of the Senate, and the Chairs and Vice Chairs of the intelligence oversight committees of both houses.

intelligence framework. Should this be developed by Congress? By the White House? By the DNI? Or DHS? All of these parties must be at the table. What is the overall architecture for developing a DI capability that utilizes all elements of information collection and analysis? On the supply of intelligence, who are the key actors? What are their roles? What information/intelligence could each actor supply regarding threat and vulnerability assessments? Are there duplications of effort? Are there existing shortcomings in the overall U.S. effort? Are efforts currently being undertaken by one actor that could be, should be or may be better undertaken by another actor? Similar questions should be asked on the demand side: Who are the primary recipients of intelligence products? What information/intelligence do stakeholders require to perform their security functions? Are there gaps between stakeholder demands and intelligence supply?

2. How does the DI ‘system’ run? Who can task collection requirements? How are multiple streams of information and intelligence to be fused and integrated? Who is responsible for analysis? Given the increased need to “connect dots”, how is information shared from one entity to another? Are there clear policies for how intelligence/information can be used? How long can agencies retain information?

3. What oversight is in place to maximize performance while also minimizing abuse, misuse, and mistrust? Looking across each branch of government, what checks are in place for preventing abuse and ensuring redress for oversteps and/or errors? Are existing authorities sufficient?

Conclusion

The attacks on 9/11 exposed shortcomings within the U.S. intelligence community in the gathering, processing and sharing of intelligence about foreign terrorists on American soil. Unfortunately, despite military, intelligence, financial, and diplomatic actions abroad, radical Islam continues to spread and terrorist plots continue to be discovered. Several plots have targeted U.S. sites on American soil. These plots have been found to be planned both by foreign terrorists as well as by

U.S. persons either on their own or in collaboration with other foreign terrorists. As a result, we must continue to develop the capacity to find the enemy within—to identify threats, uncover plots, track suspects, uncover networks, and interdict them before they can do harm. We must be able to do this against both foreign and U.S. persons, as the threat is no longer distinguishable by simple divisions between foreign and domestic, at home and abroad. This requirement poses direct challenges to American civil liberties. We must therefore ensure that any domestic intelligence system that may emerge be developed deliberately, with consideration for all elements and stakeholders involved. We must put in place a framework that clearly delimits roles and missions, determines what to collect and how, and elaborates a robust oversight capability to ensure that the privacy and constitutional rights of Americans continue to be protected and preserved.