

## CHAPTER 7

### LEADING THE NEXT PHASE OF HOMELAND SECURITY INTELLIGENCE: PROVIDING BETTER DEFINITIONS, ROLES, AND PROTECTIONS

**Geoffrey S. French<sup>1</sup>**

The terrorist attacks of September 11, 2001 (9/11), exposed major gaps in the collection, exchange, and synthesis of intelligence that may otherwise have prevented them. In its assessment of that intelligence failure, the National Commission on Terrorist Attacks upon the United States (the 9/11 Commission) referred not to a breakdown in foreign intelligence or domestic intelligence, but to a void that existed between the two spheres.<sup>2</sup> This sense of a void rather than a simple malfunction of an existing apparatus partially explains the sheer number of security information-sharing initiatives that have been launched since 2001. Indeed, reform of government intelligence and security activities, authorities, and organizations has been constant from 2001 to the present, typically driven by a sense of urgency derived from the initial shock of the attacks. Major legislation has included:

- The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001,
- Homeland Security Act of 2002,
- Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), and
- Implementing Recommendations of the 9/11 Act.

Other reforms included the establishment of the U.S. Department of Homeland Security (DHS) and the Terrorism Threat Integration Center (TTIC), later renamed the National Counterterrorism Center (NCTC), and the addition of resources to existing counterterrorism missions in the U.S. Department of Defense (DoD) and civilian agencies. The state and local levels of government, as well as institutions, shifted resources to the counterterrorism efforts as well.

The first phase of reform, in other words, sought to fill the void in the generation and exchange of intelligence pertinent to homeland security by a number of means; in retrospect, filling it seems to have been a higher priority than creating a coherent approach to address the issue of homeland security intelligence (HSINT). Kate Martin, director of the Center for National Security Studies, summarized the situation succinctly in her testimony before Congress in 2009: “There has also been a proliferation of agencies and entities with domestic intelligence responsibilities, although it is not clear that such arrangement was a deliberate effort to create redundancy or just an accident resulting from so many different initiatives by different actors.”<sup>3</sup>

A change in administration is an artificial marker of the passing of time, but it does often provide a useful occasion to pause and reexamine governmental approaches and the need for reform. The issue of HSINT is certainly in need of such a review. Even a basic review, in this case, reveals an inability to define HSINT, leading to obvious problematic implications for the information-sharing activities surrounding it. More importantly, collecting intelligence without protecting it from the very adversaries it is meant to address creates a critical vulnerability that threatens

to destabilize the partnerships established to date. A thorough review exposes an emerging need for a new discipline: counterintelligence for homeland security.

## **DEFINING HOMELAND SECURITY INTELLIGENCE**

Given the importance imputed to homeland security since 2001 and the crucial role of information exchange in the success of the many organizations involved in the spectrum of homeland security-related activities, one would think that finding the definition of HSINT is easy. Indeed, there have been multiple attempts to find a definition for HSINT over the past few months. In 2009, the Congressional Research Service published a thorough review of perspectives on HSINT, highlighting the areas of agreement and difference, and Congress has held hearings on its roles and limitations. Yet, no single authoritative definition or consensus has been found.<sup>4</sup>

The first potential source for such a definition is from DHS itself. DHS does not have a formal definition, however. The most recent Chief Intelligence Officer for DHS, Charles Allen, testified on the topic of HSINT on several occasions, describing it succinctly (if informally): the “essence of what constitutes homeland security intelligence is a simple concept – threats to the U.S. Homeland.” HSINT, in this view, is the “unique mission” of DHS in support of the “Secretary and the Department; [its] partners at the state, local, and tribal levels, and in the private sector; and in the Intelligence Community.”<sup>5</sup> Although one can argue whether HSINT belongs uniquely to DHS, the department and its mission are a focal point for HSINT activities and therefore a useful starting point for framing the definition.

Unfortunately, the legal foundation for DHS also lacks a formal definition. The Homeland Security Act of 2002, (Public Law 107-296, November 23, 2002) defines homeland security *information* as:

Any information that relates to the threat of terrorist activity and the ability to prevent it, as well as information that would improve the response to terrorist activity or the identification or investigation of a suspected terrorist or terrorist organization.

If DHS can be considered a microcosm of the homeland security effort, however, this definition does not capture the other major threats that the department faces, such as organized criminal groups, drug-trafficking organizations, transnational gangs, and alien-smuggling rings. Terrorism—although the primary impetus for the creation of DHS and the basis of HSINT—does not suffice to define the boundaries of HSINT.

Similarly, the term “domestic intelligence” does not adequately bound the issues of homeland security. Although DHS’s focus is on the application of intelligence to domestic issues, the intelligence itself focuses more often than not on transnational entities. There are certainly domestic terrorist groups that warrant observation by the law enforcement community, but international terrorist groups, criminal organizations, and transnational gangs require the fusion of domestic intelligence with foreign intelligence.

This complexity highlights the inherent difference between the traditional role of the intelligence community and the new role required of DHS and the HSINT community. For military intelligence, the military is both a collector and the primary consumer.

Foreign intelligence has many more applications and consumers, but there is still a relatively limited group needing to receive intelligence reports or analysis, and there are clear rules for how to share and protect such information. In contrast, potential HSINT consumers include: the law enforcement community; federal, state, local, and tribal governments; owners and operators of critical infrastructure; and the public. Similarly, those very same consumers may also be collectors. Citizens or operators of critical infrastructure may be in a position to observe and report suspicious activity or other anomalous behavior that is pertinent to combating a criminal organization, a gang, or a terrorist group. This is not to argue for a police state mentality, with citizens expected to inform on neighbors and friends. It is merely to note that important tips about criminal and terrorist groups often come from ordinary citizens and organizations and not from formal intelligence collection activities. (Some have even argued that the private sector can contribute to the entire intelligence cycle, including the generation of intelligence requirements.<sup>6</sup>) HSINT, in other words, is unique in that its success depends not on retaining the information within a small, closed community, but rather sharing it with very broad segments of society.

The challenge, therefore, is to draw proper boundaries, if any, for the concept of HSINT. The HSINT community has not overcome this obstacle yet. For lack of a formal definition, the term “homeland security intelligence” as used in this chapter is understood to mean intelligence applied to protect against domestic and transnational threats to critical infrastructure and urban security.

## NEW FRAMEWORKS FOR INFORMATION SHARING

The erstwhile lack of a definition for HSINT has led directly to other ambiguities that prevent the HSINT community from effectively collecting, sharing, and analyzing information. First, it confines the definition of the HSINT community so as to exclude the assemblage of federal agencies, state and local law enforcement, and private partners that participate on a consistent or ad hoc basis. It thereby prevents true scope and clarity, for example, on the role of DHS in comparison with the Federal Bureau of Investigation, which has outreach programs to the private sector, including critical infrastructure, and a lead role in law enforcement and counterintelligence—or with NCTC, which is intended to centralize analysis of international terrorism and has some outreach to state and local law enforcement. In some ways, the sheer number of federal entities, information-sharing partnerships, systems, and databases testifies not to the effectiveness of the current combined effort, but to its incoherence.

Second, the lack of definition prevents a true evaluation of the effectiveness of HSINT. When the goal of information sharing itself cannot be identified, the only possible metrics are the availability of information-sharing mechanisms or technologies, or meaningless counts of the number of reports or megabytes of data exchanged. In the DHS 5-year report on progress in implementing recommendations from the 9/11 Commission, for example, it discusses information-sharing explicitly only in terms of the easily quantifiable numbers of state and local fusion centers, the dollar amount of grant allocations to

support information-sharing, and the increasing availability of certain information-sharing networks.<sup>7</sup> A survey published in 2009, reveals the effects of such a statistics-based approach, concluding that the measurement of information sharing through the examination of the availability of systems leads to a neglect of focus on the true goals of information sharing, whether in mission effectiveness or community preparedness.<sup>8</sup> Similarly, the March 2009 hearings before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security revealed problems not with the means of sharing information, but rather with the HSINT activities themselves: confusion over the DHS advisory system, questions over priority of security issues, and dissatisfaction with the ability to analyze suspicious activity reports.<sup>9</sup> The emphasis on sharing information without clear definitions of what that information is, with whom it should be shared, and common goals inevitably leads to poor decisions, investments, and outcomes.

There is a general need, therefore, for one or more frameworks that would help focus the goals of information sharing. Two such frameworks are immediately available. The first is an emphasis on threat information that supports risk-based decisionmaking. When tactical threat analysis—such as the identification of a specific terrorist cell or an active plot—is available, its application is relatively straightforward. Most HSINT, however, is more strategic in nature, providing indications of an adversary's capability or intent to pursue a course of action. Additionally, it tends to have some degree of uncertainty, often due to unreliability of the source, staleness of the information, or credibility problems. The challenge, therefore, is not typically how to share the information; fusion

centers, for example, allow a city or region to integrate information from federal agencies with its own law enforcement information and reports of suspicious activity from local operators of critical infrastructure. Instead, the challenge is how to use strategic HSINT. A single report of adversary capability may indeed be valid in a vacuum, but it is not a compelling case for action without the context provided by risk analysis which aligns the threat with the vulnerability to and consequence of the adversary's actions. By using a risk framework as the basis for collecting, sharing, and reporting threat information, fusion centers will have a way to integrate the various reports into consistent and comparative threat levels for region-specific scenarios. A report from George Mason University describes one such approach used for an assessment of the National Capital Region,<sup>10</sup> which may be useful as a model for other regions in that it delivered the type of information reported to be useful in community preparedness: geographically-specific intelligence about specific adversaries.<sup>11</sup>

The direct threat to a city or region, however, is only one aspect of the counterterrorism and broader homeland security mission. A terrorist group or gang may use one region to raise money or acquire weapons, another to recruit members, and another for communication. In this sense, an adversary can be seen as being in competition with the homeland security community as a whole; obtaining the resources it needs to continue to operate puts it in confrontation with immigration, customs, or other law enforcement. To adopt a military term, the various regions of the country constitute the domestic battlespace in which the adversary operates. Capitalizing on this perspective, the second analytic framework that could

help focus the goals of HSINT is the U.S. military's methodology for Intelligence Preparation of the Battlespace (IPB).<sup>12</sup> IPB requires analysts to understand the political, social, and economic factors affecting an adversary's operations, thus allowing the analysts to view the adversary as a dynamic actor with needs and dependencies as well as goals and objectives. It builds to an assessment of the adversary's potential courses of action and facilitates effects-based outcomes to gain a high-level perspective of how an adversary may react. If fusion centers had a better understanding of how an adversary operates in their regions, the participating agencies could more effectively counter the adversary's actions. If DHS had insight into every fusion center's activities, it would be in a position to coordinate across regions and minimize unintended consequences. In this way, the IPB methodology could help support decisionmaking at all levels and help prioritize and coordinate action by focusing it on specific desired effects on the adversary.

## **INTELLIGENCE AND COUNTERINTELLIGENCE**

Despite the absence of formal definitions, common frameworks, clear roles, and delineated responsibilities for HSINT, many government agencies are investing heavily in time and resources to share information from investigations, interviews, informants, other human intelligence, signals intelligence, and other intelligence disciplines. This activity may have limited value due to the hindrances discussed above, but the continued engagement of state, local, and tribal governments—as well as the private sector—indicates that there is some value. A second indicator of the value of the HSINT community's information and in-

formation-sharing systems is that various adversaries have begun to exploit them.

In October 2008, for example, press reports revealed that the Sinaloa drug cartel had an informant in the U.S. embassy in Mexico City with access to information on DEA operations.<sup>13</sup> One such insider was able to gain information shared between the U.S. and Mexican governments on operations against organized criminal groups and drug-trafficking organizations and passed it on to the cartel. Similarly, in 2005, the target of a U.S. terrorism investigation duped Weiss Rasool, a sergeant with the Fairfax County Police, into using Rasool's access to FBI information to identify the surveillance vehicles. The target provided Rasool with the license plate numbers from cars that the target suspected were following him, which Rasool ran through an FBI database. Rasool saw that the vehicles were not registered to individuals but to a leasing company and thus likely were used for federal law enforcement. He relayed this information to the target of the investigation, tipping him to the federal surveillance and undermining the investigation.<sup>14</sup> This new, ill-defined, and nontraditional type of intelligence has value, in other words, not only to the HSINT community, but also to the very adversaries it is meant to combat.

As local law enforcement organizations consolidate intelligence from informants, interviews, and observations,<sup>15</sup> they create the possibility that a single point of vulnerability could compromise all of their informants. If they share information across regions, then one city's intelligence could be spoiled by its being compromised by another city's intelligence center. If a regional intelligence center fuses local intelligence with national intelligence, a local vulnerability could

lead to a compromise of the sources or methods from signals intelligence, imagery intelligence, or human intelligence. A recent incident illustrates the vulnerability introduced by efforts to fuse information among different levels of government. In California, two intelligence analysts have pleaded guilty to mishandling classified material by providing it to a local law enforcement organization. Larry Richards, a detective with the Los Angeles County Sheriff's Department and a reserve colonel in the Marine Corps, allegedly recruited Gary Maziarz and Eric L. Froboese to provide terrorism-related intelligence that they had access to in their official positions at Camp Pendleton. Richards requested information about terrorist or suspected terrorist cases in Southern California—some classified Top Secret—which Maziarz and Froboese retrieved and transmitted. Maziarz testified that he felt he was helping overcome the obstacles that prevent information-sharing among military and civilian government agencies.<sup>16</sup>

If this incident is indicative of prevailing pressures to share information, it sets up the participants to be vulnerable to multiple types of technical or operational exploitation. Often, the urgency to share information—especially when coupled with incompatible or inconvenient communications systems—causes parties to share information outside secure channels or to fall prey to ruses, deception, or other stratagems leading to inadvertent revelation of information to adversaries.

To address the risk of loss of shared intelligence to gangs, criminal groups, terrorist groups, or foreign intelligence, the HSINT community needs to take several actions, beginning with defining the protective measures that ensure the confidentiality of the

information and information-sharing systems. Security alone will not suffice, however. Well-financed or sophisticated adversaries have the means to recruit or infiltrate organizations with access to information, or engage in espionage by technological exploitation. Counterintelligence—the discipline of identifying, penetrating, and neutralizing adversaries’ attempts to collect and analyze friendly intelligence—is a necessary component. If gangs, organized criminal groups, and terrorist groups are collecting information on homeland security and law enforcement operations, there are established steps that can be taken to detect and manipulate that collection. If criminal or terrorist groups (or their affiliates) have operational assets—recruited, coerced, or infiltrated insiders—there are standard proven methods to detect and turn them. Just as HSINT is an inchoate art that differs from the work the intelligence community has traditionally done, counterintelligence for homeland security will require novel approaches to counter the intelligence collection efforts of transnational groups as opposed to foreign intelligence services.

Unfortunately, the HSINT community has not explored these concepts to any depth,<sup>17</sup> and the difficulties of implementing counterintelligence are daunting, given that information-sharing systems have already been established and are operational. Since the HSINT community is highly diffuse, a centralized approach would leave major vulnerabilities at every fringe node of the network. A strong counterintelligence program at one fusion center may simply redirect the adversary to another region. Although the challenges in creating an effective counterintelligence program to protect HSINT are formidable, the high stakes demand that we succeed. If an adversary has

insight into homeland security or law enforcement operations, he can undermine, negate, or manipulate them. If trust begins to break down within the HSINT community, the entire information-sharing apparatus may collapse. There is an urgent need for counterintelligence analysis and operations to support the HSINT community. This support may begin with awareness training, risk assessments, and implementation of strict Operations Security (OPSEC), but it must ultimately be a nationwide effort coordinated by DHS as the primary steward of HSINT. Without such a high-level effort, all HSINT collection and analysis are at risk.

## CONCLUSION

After 9/11, the need for reform became clear. The counterterrorism effort had several gaps, including poor connections among federal agencies; minimal information exchange between federal government agencies and state, local, and tribal governments; and negligible information exchange between the public and private sectors. The first phase of HSINT reform was to institute a number of processes to help fill the void between domestic and foreign intelligence. The HSINT community and its infrastructure are far from complete, however. The second phase of HSINT reform must provide (1) clearer mechanisms for collection and processing, (2) better communication for risk-based decisions, and (3) stronger counterintelligence support of homeland security operations.

Government reform is easiest in the wake of a highly publicized failure of an agency or activity. Publicly visible failures make a strong case for reform because they create general agreement on the nature of the

breakdown and the changes that will address them. In some cases, especially when the cause is a lack of an organization to perform a task rather than a malfunction of an existing organization, the urgency to implement reform can mask and prolong the underlying problem rather than addressing it satisfactorily. In the case of HSINT, the failure was real, and the urgency to address it was valid. The activities put into place as a result, however, have only incrementally addressed the problem due to inattention to clear definitions, roles, and responsibilities. One can argue over the value of HSINT as currently constructed, but argument on either side leads to the same basic need for reform. If current information collection and exchange do not have value, then reform is required to ensure that the nation is not wasting time, resources, and talent. If it does have value, then reform is required to ensure that the collection and exchanges are properly protected from adversaries who can also benefit from their value.

Government reform absent a failure is more difficult, requiring leadership to identify the issues and persuade others of their importance and urgency. Given the investments in HSINT and the serious repercussions of another failure, the Obama administration needs to review the situation and address the foundational issues that threaten to compromise the entire endeavor.

## ENDNOTES - CHAPTER 7

1. The views expressed here belong solely to the author and do not reflect positions of the U.S. Government or CENTRA Technology, Inc.

2. U.S. Congress, "National Commission on Terrorist Attacks upon the United States," *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, Washington, DC: U.S. Government Printing Office, 2004, p. 263.

3. House Committee on Homeland Security, "Homeland Security Intelligence: Its Relevance and Limitations," Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security, Washington, DC: 111th Cong., 1st Sess., March 18, 2009, p. 3.

4. Mark A. Randol, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, RL 33616, Washington, DC: Congressional Research Service, January 2009.

5. Senate Select Committee on Intelligence, Intelligence Reform and Homeland Security Intelligence, Hearing before the Senate Select Committee on Intelligence, Washington, DC: 110th Cong, 1st Sess., January 25, 2007, pp. 4-5.

6. Alex Martin and Peter Wilson, "The Value of Non-Governmental Intelligence: Widening the Field," *Intelligence and National Security* Vol. 23, No. 6, December 2008, pp. 767-776.

7. Progress in Implementing 9/11 Commission Recommendations, Washington, DC: Department of Homeland Security, July 22, 2009, p. 11.

8. Hamilton Bean, "Exploring the Relationship between Homeland Security Information Sharing and Local Emergency Preparedness," *Homeland Security Affairs*, Vol V, No. 2, May 2009.

9. See for example, the testimony of John W. Gaissert, Douglas C. Gillespie, and Joan T. McNamara before the Subcommittee

on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security, March 18, 2009.

10. Elizabeth Jackson, William L. McGill, and Christopher Geldart, "Regional Risk Analysis: A Coordinated Effort," Washington, DC: George Mason University, April 2009.

11. Bean, p. 10.

12. Jin Kim and William M. Allard, "Intelligence Preparation of the Battlespace: A Methodology for Homeland Security Intelligence Analysis," *S AIS Review*, Vol XXVIII, No. 1, Winter-Spring 2008.

13. Associated Press, "U.S. Embassy Agent: I Spied for Mexican Cartel," October 27, 2008.

14. Tom Jackman, "Fairfax Officer Admits Misusing Computers; Plea Entered in Illegal License Checks," *Washington Post*, February 1, 2008, p. B1; Department of Justice, Press Release, "Fairfax County Police Sergeant Pleads Guilty to Unauthorized Computer Access," January 31, 2008.

15. For one discussion of the collection and use of intelligence for law enforcement, see Stephen G. Serrao, "Intelligence-Led Policing," *Law Officer*, Vol. 5, Issue 7, July 1, 2009, p. 10.

16. Rick Rogers, "Marine Took Files as Part of Spy Ring," *San Diego Union-Tribune*, October 6, 2007; Tony Perry, "Marine Reservist Pleads Guilty to Leaking Intelligence Documents," *Los Angeles Times*, June 12, 2009.

17. For one discussion of the need for counterintelligence support of infrastructure protection, see John MacGaffin, "Counterintelligence and Infrastructure Protection," *Security in the Information Age: New Challenges, New Strategies*, Washington, DC: Joint Economic Committee, May 2002.