Order Code RL33616

Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches

August 18, 2006

Todd Masse
Specialist in Domestic Intelligence and Counterterrorism
Domestic Social Policy

Homeland Security Intelligence: Perceptions, Statutory Definitions and Approaches

Summary

Although the activities involved in homeland security intelligence (HSINT) itself are not new, the relative importance of state, local, and private sector stakeholders; the awareness of how law enforcement information might protect national security; and the importance attached to homeland security intelligence have all increased substantially since the events of September 11, 2001.

There are numerous intelligence collection disciplines through which the U.S. Intelligence Community (IC) collects intelligence to support informed national security decision-making at the national level and the allocation of tactical military and law enforcement resources at the local level. The collection disciplines are generally referred to as those which fall within national technical means or non-technical means. Technical means include signals intelligence (SIGINT), measurement and signatures intelligence (MASINT), and imagery intelligence (IMINT). Non-technical means include human intelligence (HUMINT) and open source intelligence (OSINT). Each of these collection disciplines is source-specific — that is, a technical platform or human source, generally managed by an agency or mission manager, collects intelligence that is used for national intelligence purposes. HSINT, however, is generally not source specific, as it includes both national technical and non-technical means of collection. For example, HSINT includes human intelligence collected by federal border security personnel or state and local law enforcement officials, as well as SIGINT collected by the National Security Agency. Reasonable individuals can differ, therefore, with respect to the question of whether HSINT is another collection discipline, or whether homeland security is simply another purpose for which the current set of collection disciplines is being harnessed. Homeland security *information*, as statutorily defined, pertains directly to (1) terrorist intentions and capabilities to attack people and infrastructure within the United States, and (2) U.S. abilities to deter, prevent, and respond to potential terrorist attacks.

This report provides a potential conceptual model of how to frame HSINT, including geographic, structural/statutory, and holistic approaches. Given that state, local, tribal, and private sector officials play such an important role in HSINT, the holistic model, one not constrained by geography or levels of government, strikes many as the most compelling. The report argues that there is, in effect, a Homeland Security Intelligence Community (HSIC). While this community may not necessarily be a useful construct from a management perspective, it is nevertheless a community as traditionally defined. Although the HSIC's members are diffused across the nation, they share a common counterterrorism interest. The proliferation of intelligence and information fusion centers across the country indicate that state and local leaders believe there is value to centralizing intelligence gathering and analysis in a manner that assists them in preventing and responding to local manifestations of terrorist threats to their people, infrastructure, and other assets. At the policy and operational levels, the communication and integration of federal HSINT efforts with these state and local fusion centers will likely remain an important priority and future challenge. This report will not be updated.

Contents

List of Figures

List of Tables

Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches

Introduction[1]

The term "homeland security intelligence" is heard fairly frequently in the post-9/11 era. The National Commission on Terrorist Attacks Upon the United States (hereafter the 9/11 Commission) stated one of the challenges in preventing such attacks is bridging the "foreign-domestic divide."[2] The 9/11 Commission used this term for the divide that it found not only within the Intelligence Community (IC), but also between the agencies of the IC dedicated to the traditional foreign intelligence mission, and those agencies responsible for the homeland security intelligence (HSINT) and law enforcement missions. Some might categorize security intelligence and law enforcement (criminal) intelligence as "non-traditional" intelligence.[3] Yet, the scope and composition of this non-traditional or homeland security intelligence remains somewhat nebulous.

---

[1] This is the first in a series of reports examining the homeland security intelligence function. Follow-on reports may discuss the role of the various elements of the DHS intelligence enterprise in homeland security intelligence and the implementation of DHS Secretary Michael Chertoff's intelligence initiatives outlined in DHS's "Second Stage Review." The question of how the U.S. government should organize to implement an effective homeland security intelligence function, e.g., the appropriate roles and responsibilities, and attendant de-confliction of overlapping jurisdictions, of the FBI and DHS intelligence elements, are beyond the scope of this report.

[2] See *The Final Report of the National Commission on Terrorist Attacks Upon the United States*, pp. 399-428. Available at [http://www.gpoaccess.gov/911/pdf/fullreport.pdf].

[3] See testimony of Charles Allen, Chief Intelligence Officer of the Department of Homeland Security, before the House Committee on Homeland Security, Subcommittee on Intelligence, Information, and Terrorism Risk Assessment, and the House Permanent Select Committee on Intelligence, Subcommittee on Terrorism/HUMINT, Analysis and Counterintelligence, Oct. 19, 2005. Mr. Allen stated, "My role — and my goal — as Chief Intelligence Officer is to see that homeland security intelligence, a blend of traditional and non-traditional intelligence that produces unique and actionable insights, takes its place alongside the other kinds of intelligence as an indispensable tool for securing the nation."

At the broadest level, there is a plethora of definitions for intelligence;[4] most explain the various types of clandestine intelligence, the methods of intelligence collection (the "Ints"), intelligence consumers, the purposes for which intelligence is collected, and the intelligence cycle.[5] Traditional intelligence collection done clandestinely[6] and overtly,[7] largely at the federal level, to inform national-level policymakers is often differentiated from criminal intelligence gathered by a broader set of federal, state, and local actors generally for law enforcement purposes. Some argue that given that the end result in a criminal case is successful prosecution, that criminal intelligence gathering is largely reactive — a crime takes place, and "intelligence" or evidence is collected to support a prosecution. However, intelligence gathering can also be used to advance the causes of national security, as state and local law enforcement agencies can be viewed as the nation's

---

[4] The terms data, information and intelligence are generally (mis) interpreted to have the same meaning. One manner of differentiating among these terms is the extent to which value has been added to the raw data collected — through overt or clandestine means. The terms exist along a continuum, with data at the far left and intelligence at the far right; as one moves from left to right additional value and context is added to discrete or posited facts to provide enhanced meaning to an ultimate consumer. Information collected clandestinely may or may not be of any inherently greater value than information collected through open source. Information collected is "raw" until its sources have been evaluated, the information is combined or corroborated by other sources, and analytical and due diligence methodologies are applied to ascertain the information's value. Lack of such critical evaluations can lead to flawed "intelligence" being provided to consumers who may take action based on the intelligence.

[5] The intelligence cycle is an iterative process in which collection requirements based on national security threats are developed, and intelligence is collected, analyzed, and disseminated to a broad range of consumers. Consumers sometimes provide feedback on the finished intelligence products, which can be used to refine any part of the intelligence cycle to ensure that consumers are getting the intelligence they need to make informed decisions and/or take appropriate actions.

[6] Intelligence is collected clandestinely by the U.S. Intelligence Community and includes a wide variety of human and national technical means, as outlined below.

[7] Open-source intelligence, or that which is collected through sources available to the general public globally, while long a tool of foreign intelligence-oriented agencies, has become relatively more important in the post-Cold War era. One indication of this relative increase in prominence is the Director of National Intelligence's establishment, pursuant to a recommendation of the WMD Commission, of an Open Source Center in November 2005. The Center will "advance the Intelligence Community's exploitation of openly available information to include the Internet, databases, press, radio, television, video geospatial data, photos, and commercial imagery. The Center's functions will include collection, analysis and research, training, and information technology management to facilitate government-wide access and use. The Center will build on the established expertise of the CIA's Foreign Broadcast Information Service (FBIS), which has provided the U.S. Government a broad range of highly valued products and service since 1941." See Office of the Director of National Intelligence Press Release No. 6-05, Nov. 8, 2005. H.R. 5003, the Homeland Security Open Source Intelligence Enhancement Act of 2006, would require the proposed Under Secretary for Intelligence and Analysis to "make full and efficient use of open source intelligence by acquiring, gathering, processing, and analyzing open source information to produce open source intelligence products."

counterterrorism "eyes and ears."[8] Arguably, not all criminal intelligence gathering is reactive, as some law enforcement organizations and intelligence fusion centers use pro-active intelligence gathering techniques, such as the recruitment of human assets, to prevent terrorist attacks.

The terms domestic intelligence and homeland security intelligence are often used colloquially and interchangeably by some observers. Depending on how one defines "homeland security," this may be understandable. If, however, one bounds the activities associated with intelligence geographically, a systemic malady which was at least a proximate cause of the intelligence failure resulting in the terrorist attacks of September 11, 2001, the two terms are inherently distinct. That is, domestic intelligence could be defined as that which is collected, analyzed, and disseminated within the United States; yet, homeland security intelligence may be much more broadly defined without regard to the geographic origin of the intelligence collected. The rationale for the integration of what is traditionally defined as foreign intelligence with that which is thought of as domestic intelligence is concisely stated by Director of National Intelligence (DNI) Ambassador John Negroponte: "What happens abroad can kill us at home."[9]

One of the broadest definitions of intelligence is that "intelligence is knowledge, organization, and activity."[10] Arguably, one of the most meaningful purposes of intelligence is "to establish where the danger lies."[11] Some would argue based on this definition that "intelligence is intelligence" — that is, differentiating traditional from non-traditional intelligence is a theoretical matter which may have little relation to the end result — protecting national security. This argument might continue that threats to U.S. national security by and large originate overseas and, since its formal and statutory inception in 1947, the U.S. Intelligence Community has always been the first line of defense in identifying and understanding these threats. Although compelling, this argument could lead some observers to conclude that the state, local, and private sector intelligence players are simply "bolt on" modules to the existing

---

[8] See Marilyn Peterson, *Intelligence-Led Policing: The New Intelligence Architecture*, U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, Sept. 2005.

[9] See speech of John D. Negroponte, Director of National Intelligence, before the U.S. Chamber of Commerce, July 10, 2006.

[10] Sherman Kent, *Strategic Intelligence* (Archon Books, 1965). Dr. Kent was, however, quick to point out that the knowledge, organization and activity to which he referred was "high-level, foreign, positive intelligence." According to Dr. Kent, it was important to note that what was excluded from this definition of intelligence was (1) "the domestic scene ... it is not concerned with what goes on in the United States," and (2) the "police function." The "positive comes into the phrase to denote that the intelligence in question is not so-called counterintelligence and counter-espionage nor any other sort of intelligence designed to uncover domestically produced traitors or imported foreign agents." Not that Dr. Kent discounted the importance of this other type of intelligence; indeed he referred to it as "security intelligence," a definition which will be explored further below. Dr. Kent is the namesake for the Central Intelligence Agency's Sherman Kent School of Intelligence Analysis.

[11] See Thomas Powers, *Intelligence Wars: American Secret History From Hitler to Al-Qaeda* (New York Review Books, 2002), p. 381.

federal community. Such a status quo plus model could be interpreted by some to mean that state, local, and private sector entities are new and passive consumers of federally gathered and analyzed intelligence products, yet not necessarily full intelligence cycle partners. This may not necessarily be the case, as state, local, and private sector organizations have taken on a more activist and proactive role in protecting their populations and infrastructure, a role that includes collecting their own intelligence while working with federal law enforcement and IC partners stationed in Washington, DC, and within their respective districts.[12]

The "intelligence is intelligence" position might beg the question of what is the most appropriate strategy for homeland security intelligence — a "top-down" federally driven model where the traditional "Ints" are dominant, a "bottom-up" state, local, and private sector model where the thousands of state and local law enforcement intelligence collectors are dominant, or some unique partnership that strikes a balance between these two extreme models? To some extent, HSINT may be perceived by some as a federally led "top-down" model through which the federal government's intelligence entities provide raw intelligence and/or finished terrorism threat assessments to state, local, and tribal law enforcement entities which may make independent determinations of whether the intelligence is actionable. Another alternative is a "bottom up" model through which criminal intelligence,[13] of the type collected long before the events of September 11, 2001, provides an assessment of the local environments in which a national security and/or a criminal threat might become a reality. A third model, among others, might envision a less hierarchical or a more decentralized structure in which roles and responsibilities of federal, state, and local players are more clearly delineated, information shared more widely, and coordination between law enforcement and traditional intelligence actors closer. These models will be highlighted below.

Some perceptions of HSINT among leaders in the IC and observers of the intelligence process seem illustrative.

---

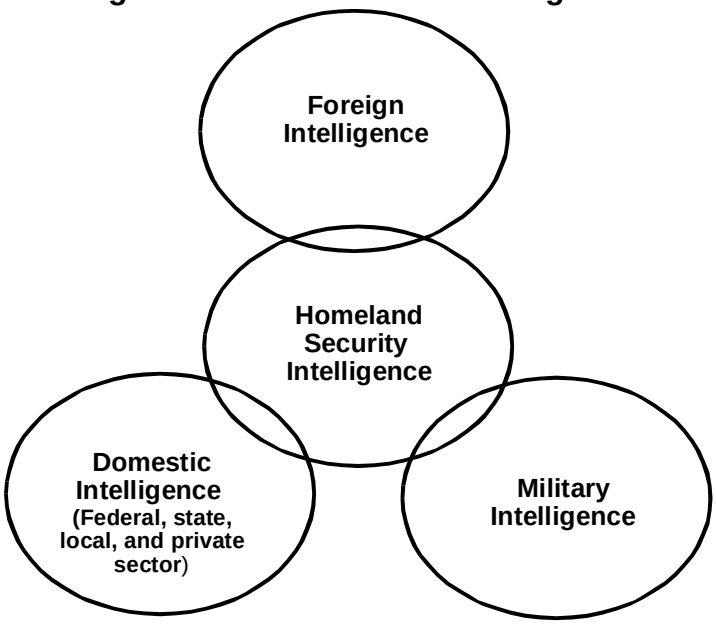
[12] Some of the benefits and challenges associated with using state and local law enforcement in the War on Terrorism are outlined in K. Jack Riley, Gregory F. Treverton, Jeremy M. Wilson, and Lois M. Davis, *State and Local Intelligence in the War on Terrorism*, a RAND, Infrastructure, Safety and Environment Study, 2005.

[13] Part of the complexity of framing HSINT is the relationship between criminal or law enforcement intelligence and traditional foreign intelligence. Generally, the interpretation of traditional foreign intelligence is that it is collected covertly and overseas, and is provided to policymakers to inform national security decisions and actions. By contrast and in general, criminal intelligence is gathered overtly or clandestinely and domestically as evidence to support a prosecution of a criminal act, or to learn more about a criminal enterprise. For further information on criminal intelligence, see RAND, *State and Local Intelligence in the War on Terrorism*, 2005, by K. Jack Riley et al.; U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Intelligence-Led Policing: The New Intelligence Architecture*, Sept. 2005; and David L. Carter *Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies*, Nov. 2004. For information on the relationships between law enforcement intelligence and foreign intelligence, see CRS Report RL30252, *Intelligence and Law Enforcement: Countering Transnational Threats to the United States*, by Richard A. Best, Jr. See also, Richard A. Posner, *Remaking Domestic Intelligence* (Stanford, CA: Hoover Institution Press, 2005).

Some Perceptions of HSINT

Leaders within the Intelligence and Homeland Security communities often speak openly about the responsibilities, priorities, accomplishments, and challenges their agencies face. DNI John Negroponte recently stated that the Intelligence Community has tasked itself with "bolstering intelligence support for homeland security as enterprise objective number one."[14] He spoke of this priority within the context of the DNI's mandate resulting from the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 to "integrate the foreign, military and domestic dimensions of the United States intelligence into a unified enterprise" and "connecting the dots across the foreign-domestic divide."[15] At the aggregate level, even if it is assumed that there is one unified intelligence discipline, according to DNI Negroponte, there are three different *dimensions* of intelligence — foreign, military,[16] and domestic. Under this school of thought, HSINT could become another dimension of intelligence that is distinct in some manners, yet overlaps with the aforementioned dimensions. At a relatively simplistic level, the relationships among the dimensions of intelligence could be depicted according to **Figure 1** below.

Figure 1. Dimensions of Intelligence



---

[14] See speech of DNI John D. Negroponte before the U.S. Chamber of Commerce, July 10, 2006.

[15] Ibid.

[16] At the most general level, military intelligence is that which is collected, analyzed, disseminated, and possibly acted upon by Department of Defense entities (including the Armed Forces intelligence elements, the Unified Commands, the combat support agencies of the National Reconnaissance Office, National Security Agency and National Geospatial-Intelligence Agency, as well as the Defense Intelligence Agency) and is related to another foreign power's capabilities to attack U.S. national interests militarily. For more information, see [http://www.intelligence.gov/1-members.shtml].

Although each of the dimensions of intelligence (referred to above) could be further subdivided, the domestic intelligence dimension, under a broad understanding of the term, would include the role state, local, tribal, and private sector entities play in collecting, analyzing, and disseminating information and intelligence within their respective areas of jurisdiction or industries. DNI Negroponte has defined the domestic agenda as "institution building and information sharing without damaging the fabric and values of our political culture."[17] With respect to institution building, the approach remains federal-centric, that is, DNI Negroponte referred specifically to the refinement of the FBI's National Security Branch, the further development of the National Counterterrorism Center (NCTC), as well as the development of the DHS Office of Intelligence and Analysis. State governments, local law enforcement, the private sector, and tribal entities are mentioned by DNI Negroponte at a procedural level — that is, in the sense of "facilitating these multidirectional flow of information."[18]

Secretary of Homeland Security Michael Chertoff recently provided his insights into and thoughts about defining the scope of HSINT. Using the metaphor of intelligence as the "radar of the 21st century" to provide early warning of terrorist attacks, Secretary Chertoff stated,

> Intelligence, as you know, is not only about spies and satellites. Intelligence is about the thousands and thousands of routine, everyday observations and activities. Surveillance, interactions — each of which may be taken in isolation as not a particularly meaningful piece of information, but when fused together, gives us a sense of the patterns and the flow that really is at the core of what intelligence analysis is all about.... We (DHS) actually generate a lot of intelligence...we have many interactions every day, every hour at the border, on airplanes, and with the Coast Guard.[19]

Some observers have characterized domestic intelligence in the following manner:

> Domestic intelligence entails the range of activities focused on protecting the United States from threats mostly of foreign origin. Focused narrowly, it includes the FBI's counterterrorism work with local law enforcement. On a much broader scale, however, it also involves a broader set of intelligence activities overseen by the Director of National Intelligence, the secretary of defense, the attorney general, and the secretary of homeland security. The goal is to integrate federal, state and local governments, and, when appropriate, the private sector on a secure collaborative network to stop our enemies before they act. Those enemies include individuals and groups attempting to transport weapons of mass

---

[17] Ibid.

[18] Ibid.

[19] See Remarks by Secretary of Homeland Security Michael Chertoff 2006 Bureau of Justice Assistance, U.S. Department of Justice and SEARCH Symposium on Justice and Public Safety Information Sharing, Mar. 14, 2006.

> destruction, international terrorists, organized criminals, narcotics traffickers, and countries that are working alone or in combination against U.S. interests.[20]

Another observer has defined "domestic national security intelligence" as

> intelligence concerning the threat of major, politically motivated violence, or equal grievous harm to national security or the economy, inflicted within the nation's territorial limits by international terrorists, homegrown terrorists, or spies of saboteurs employed or financed by foreign nations.[21]

According to Dr. Sherman Kent, known as the father of intelligence analysis, security intelligence is defined as

> the intelligence behind the police function. Its job is to protect the nation and its members from malefactors who are working to our national and individual hurt. In one of its most dramatic forms it is the intelligence which continuously is trying to put the finger on clandestine agents sent here by foreign powers. In another, it is the activity which protects our frontiers against other undesirable gatecrashers: illegal entrants, smugglers, dope runners, and so on... By and large, security intelligence is the knowledge and the activity which our defensive police forces must have before they take specific action against the individual ill-wisher or ill-doer.[22]

Some of the similarities between these perceptions include (1) a fundamental belief that intelligence is the first line of defense for the nation,[23] (2) threats to U.S. national security are largely, although not solely, of foreign origin, and (3) there is a national intelligence role for non-traditional players (largely state, local, tribal law enforcement, as well as the private sector), a role in which they make contributions to preventing terrorist attacks or other inimical acts directed against U.S. citizens within the United States. Where some may view a difference in these perceptions is the explicit role and responsibilities that these non-traditional entities play. Are these entities solely recipients of federally collected raw and finished intelligence products? At a policy and, importantly, local level, are non-traditional players viewed by federal

---

[20] See Rand Beers et al., *The Forgotten Homeland; A Century Foundation Task Force Report*, 2006, p. 149.

[21] See Posner, *Remaking Domestic Intelligence*.

[22] See Sherman Kent, *Strategic Intelligence* (Archon, 1965), p. 209-210.

[23] Although the facts and circumstances surrounding the recent British investigation of an alleged plot to blow up several commercial air flights from London to the United States continue to become public, intelligence appears to have played an important role. Deputy Commissioner Peter Clarke, Head of the United Kingdom's (U.K.) Anti-Terrorist Branch, stated "The Investigation has focused on intelligence, which suggested that a plot was in existence to blow up transatlantic passenger aircraft, in flight." See Statement of Peter Clarke, Aug. 10, 2006. It has been reported that U.K. authorities discovered this plot through an anonymous tip in the aftermath of the London train and bus bombings of July 2005. It has also been reported that an undercover British agent infiltrated the terrorist group. If corroborated, such an infiltration would represent a significant intelligence success. See "Agent Infiltrated Terrorist Cell, U.S. Says," CNN, available online at [http://www.cnn.com/2006/US/08/10/us.security/index.html].

personnel as equal partners, and/or "force multipliers?" At the federal level, what policies and mechanisms are in place to provide those non-traditional entities with feedback on the intelligence they collect and provide to the federal government?

Although the breadth of these questions is beyond the scope of this report, it may be illustrative to view HSINT through the eyes of national strategy.

The National Intelligence Strategy and Homeland Security Intelligence

According to the DNI's relatively recent *National Intelligence Strategy of the United States of America: Transformation Through Integration and Innovation*, one of the basic objectives is to "[b]uild an integrated intelligence capability to address threats to the homeland, consistent with U.S. laws and the protection of privacy and civil liberties."[24]

The strategy stipulates that the nature of the transnational threats to the United States "force us to rethink the way we conduct intelligence collection at home and its relationship with traditional intelligence methods abroad." Moreover, the strategy states that

> U.S. intelligence elements must focus their capabilities to ensure that (1) Intelligence elements in the Departments of Justice and Homeland Security are properly resourced and closely integrated within the larger Intelligence Community, (2) all Intelligence Community components assist in facilitating the integration of collection and analysis against terrorists, weapons of mass destruction, and other threats to the homeland, and (3) state, local, and tribal entities and the private sector are connected to our homeland security and intelligence efforts.[25]

Any national strategy, one could argue, by definition only focuses on and provides direction to the entities and agencies that the federal government controls. A broader reach and/or direction to entities beyond this purview might run the risk of presupposing that the affected community(ies) agree with the national strategy and/or have the resources to implement such direction. Therefore, it may be appropriate that the *National Intelligence Strategy*, while recognizing a homeland security intelligence role for state, local, and tribal entities, as well as the private sector, does so only in a general manner that does not stipulate the activities these communities will implement as part of the broader community of entities working to protect U.S. national security. It could also be argued, however, that while including a role for state, local, and tribal entities to be "connected to our homeland security and intelligence efforts," the National Intelligence Strategy categorizes homeland security intelligence traditionally as driven, in large part, by the federal

---

[24] See Office of the Director of National Intelligence, *The National Intelligence Strategy of the United States of America: Transformation Through Integration and Innovation*, Oct. 2005, p. 11.

[25] Ibid.

entities most associated with the domestic intelligence mission — that is, the activities undertaken by the intelligence elements of the Departments of Justice and Homeland Security.[26] How the term "connected" is defined becomes of critical importance, as it implies communication among federal, state, and local intelligence officials, but the quantity and quality of this communication has been a subject of debate among federal, state, and local officials.[27]

---

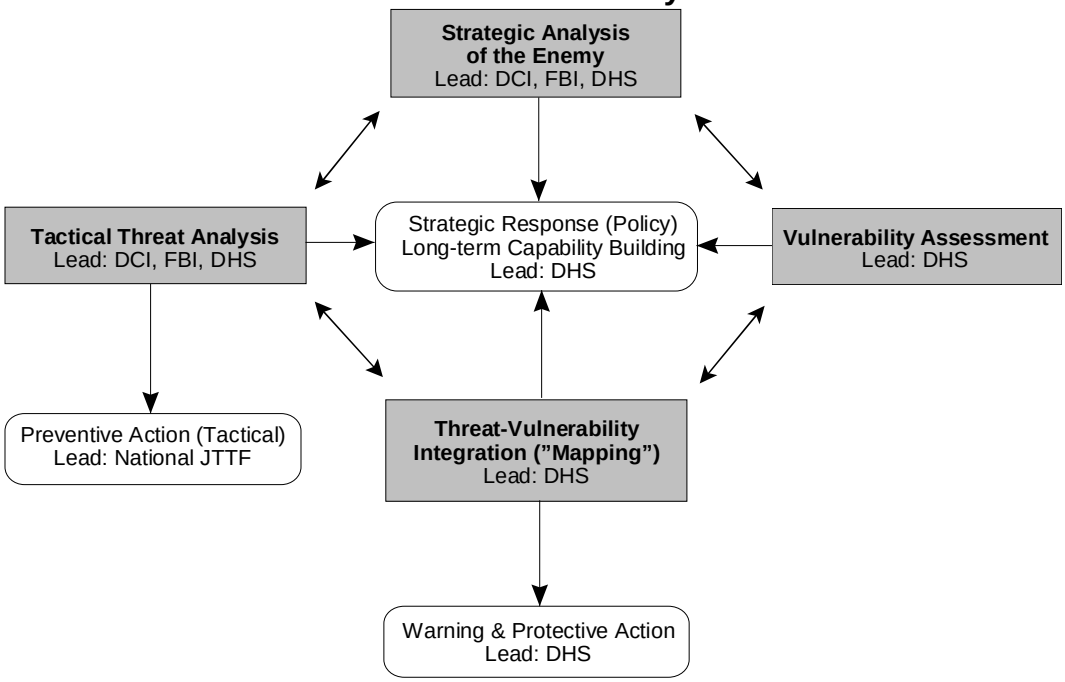
[26] While the intelligence elements of the Federal Bureau of Investigation (FBI) and Drug Enforcement Agency (DEA) are the only statutory members of the Intelligence Community within the Department of Justice (DoJ), other DoJ entities have intelligence functions. In February 2004, the Attorney General established the Justice Intelligence Coordinating Council (JICC) to, *inter alia*, "be the senior level coordination mechanism for all intelligence related activities conducted by the department and its subordinate organizations." At least initially led by the FBI Executive Assistant Director for Intelligence (a position since abolished), the membership of the JICC includes the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Bureau of Prisons; the Drug Enforcement Agency; the FBI; the National Central Bureau (INTERPOL); the Office of Intelligence Policy and Review; the Office of Tribal Justice; and the U.S. Marshals Service. See *Fact Sheet, Justice Intelligence Coordinating Council*, Feb. 25, 2004.

[27] Recent studies have supported the relative dissatisfaction among state and local homeland security and law enforcement partners with respect to information sharing. A survey of state homeland security directors conducted by the National Governor's Association, Center for Best Practices found that "A majority of homeland security directors are somewhat or completely dissatisfied with the specificity and actionable quality of the intelligence their states receive from the federal government." See *2006 State Homeland Security Directors Survey: New Challenges, Changing Relationships*, National Governors Association, Center for Best Practices, Apr. 3, 2006. Some of this dissatisfaction may be attributable to unrealistic expectations regarding the potential limitations of intelligence. For an additional assessment of the federal government's efforts to share information and intelligence related to terrorism, see *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism Related and Sensitive But Unclassified Information,* General Accountability Office (GAO), GAO-06-385, March 2006. In part, GAO found that the responsibility for the development of policies and procedures to integrate the "myriad of ongoing efforts ... to improve the sharing of terrorism-related information" has shifted "initially from the White House to the Office of Management and Budget, and then to the Department of Homeland Security ... but none has completed the task." Subsequently, and pursuant to the Intelligence Reform and Terrorism Prevention Act of 2004, an Information Sharing Environment was established. An executive branch decision led to the placement of this program within the Office of the Director of National Intelligence. For suggestions for further enhancements to information sharing, see *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment*, 3rd Report of the Markle Foundation Task Force (July 2006). See also DHS, Office of Inspector General, *Homeland Security Information Network Could Support Information Sharing More Effectively*, OIG-06-38, June 2006.

The National Strategy for Homeland Security and Intelligence

Although somewhat dated, the *National Strategy for Homeland Security* (July 2002) provides more detail on the broad role of intelligence in protecting homeland security. The names of the organizations have changed since then, but the functions of intelligence in support of homeland security remain the same. **Figure 2** below, depicts the functions outlined in the National Strategy.

Figure 2. Roles & Responsibilities of Homeland Security Intelligence and Information Analysis



Source: *National Strategy for Homeland Security*, July 2002.

While the agencies engaged in the functions outlined in the figure have changed (e.g., the Director of National Intelligence replacing the Director of Central Intelligence), the functions themselves remain critical elements of HSINT. However, the chart is largely focused on the analytical and dissemination stages of the intelligence cycle. Strategic counterterrorism threat analysis which integrates foreign and domestic counterterrorism intelligence largely takes place at the NCTC, an entity of the Office of the Director of National Intelligence which has numerous analytical detailees from across the IC. Tactical threat analysis and assessments of vulnerability take place across numerous agencies — it could be argued that the proliferation and centralization of intelligence analysis entities may undermine a national ability to conduct sound and high quality analysis in these two critical areas.[28] However,

---

[28] See Richard Kerr et al., "A Holistic Vision for the Analytic Unit," in *Studies in Intelligence,* Volume 50, #2, in which it is stated, "Over the past few years, proposals for (continued...)

absent from this chart are the important intelligence collection and intelligence gathering functions.[29] As will be outlined below, DHS has a substantial role to play in the gathering of intelligence that, when combined with other intelligence collected by the IC, could substantially enhance national security.

DHS Intelligence Enterprise Strategic Plan

The DHS Intelligence strategy has four main elements (1) vision, (2) mission, (3) definitions, and (4) goals and objectives.[30] While the strategy does not specifically define HSINT, it provides a vision for the DHS intelligence enterprise as being "an integrated ... enterprise that provides a decisive information advantage to the guardians of our homeland security."[31] According to the strategy, the mission of the DHS intelligence enterprise is to

> provide valuable, actionable intelligence and intelligence-related information for and among the National leadership, all components of DHS, our federal partners, state, local, territorial, tribal, and private sector customers. We ensure that information is gathered from all relevant DHS field operations and is fused with information from other members of the Intelligence Community to produce accurate, timely, and actionable intelligence products and services. We independently collate, analyze, coordinate, disseminate, and manage threat information affecting the homeland.[32]

Implicit in this strategy is the DHS adoption of the definition of homeland security information outlined in the Homeland Security Act of 2002.

---

[28] (...continued)
improving intelligence have been many and varied. Most have emphasized the overall structure and management of the Intelligence Community, with recommendations aimed at making top-down changes.... This paper argues that what is needed is a vision from the bottom up, of intelligence analysis that focuses on the working of the basic analytic unit." One perspective on the question of the extent to which analysis should be centralized or decentralized is provided by Dr. John Gannon, former National Intelligence Council Chairman, when he stated, "to some extent, the decentralized demands for analysis, demands for a distributed model for analysis in the defense community and in the intelligence community, the creation of a single point of success in something like the NCTC ... I think ... put you in a permanent tension with the decentralized demand." See 9/11 Public Discourse Project, "The Unfinished Agenda, Session 1: CIA and FBI Reform," June 6, 2005. One could posit that a similar argument could be made with respect to the demand amongst the law enforcement community for decentralized analysis, a demand which may be leading, in part, to the proliferation of intelligence fusion centers across the country.

[29] Intelligence collection and intelligence gathering are not necessarily the same. The former implies a clear and proactive linkage to nationally determined intelligence gaps, while the latter implies a more reactive gathering of intelligence on targets of opportunity.

[30] This document can be located at [http://www.fas.org/irp/agency/dhs/stratplan.pdf].

[31] Ibid.

[32] Ibid., p. 3.

Statutory Definitions of Intelligence and Homeland Security Information

Homeland security *intelligence* is not a term that is as yet defined or codified in law.[33] The term and activities associated with it include — and go beyond — the definitions of the two traditional types of intelligence commonly defined in law and executive orders: foreign intelligence and counterintelligence. And, more recently, definitions of these two types of intelligence have been supplemented by the terms "national intelligence" and "intelligence related to national security."

As with most intelligence-related terms, individuals attach their own interpretations and perceptions to HSINT. While there may be some commonly held perceptions about how HSINT is defined, it is also possible that individuals use the terms freely, but without a true common understanding of the scope and breadth of activities that may be consistent with homeland security intelligence. The primary statutory definition that applies is that which appears in the Homeland Security Act of 2002, which defines homeland security *information* as

> any information possessed by a federal, state, or local agency that (a) related to the threat of terrorist activity, (b) relates to the ability to prevent, interdict or disrupt terrorist activity, (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.[34]

---

[33] Homeland security *intelligence* could likely be defined as a more refined and finished version of homeland security *information*. The nexus to terrorism and terrorist-related events is direct and compelling. One complication of discerning what is homeland security information remains how the investigator or operator knows that the activity which they are investigating or monitoring is related to terrorism. At the early stages of an investigation, unless the predicate for the investigation is terrorism-related, e.g., "pocket litter" (names, phones numbers, emails) taken off of a terrorist suspect or gathered from a terrorist safe house, an investigator may not know the possibly criminal activity they are monitoring is in preparation for a terrorist event. As a result, information gathered though investigation of a criminal violation in the physical or cyber realm could very well be terrorism related and, as such, fall under the rubric of homeland security information. Given that there are substantial national and homeland security penalties for not sharing homeland security intelligence, at least at the policy level and to some extent at the operational level, arguably there is now a bias in favor of sharing raw intelligence across levels of government more quickly than in the past. The extent to which this information is shared systematically is an open question.

[34] See P.L. 107-296, Sec. 892(f). The House Committee on Homeland Security also defines homeland security information in a terrorism context. Under Rule IV, Subcommittees, it defines the jurisdiction of the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment as being, in part, "Intelligence and information sharing for the purpose of preventing, preparing for, and responding to potential terrorist attacks on the United States; the responsibility of the Department of Homeland Security for comprehensive, nationwide, terrorism-related threat, vulnerability, and risk analyses; the integration, analysis, and dissemination of homeland security information, including the Department of Homeland Security's participation in, and interaction with, other public and private entities for any of those purposes." See Committee on Homeland Security, U.S.

(continued...)

Subsequently, according to DHS Management Directive 8110, *Intelligence Integration and Management* issued January 30, 2006, the DHS Office of Intelligence and Analysis has adopted this definition of homeland security information. It is worthwhile to note that although DHS remains an organization designed to protect against "all hazards," the focus of homeland security information, at least as defined in law, is counterterrorism. As illustrated below, HSINT can be more broadly interpreted to involve intelligence designed to protect against the inimical activities of narcotics traffickers, organized criminals, and others having international support networks and seeking to engage in activities that could undermine U.S. national security.

Another type of intelligence defined in statute is traditional or foreign intelligence, which means [i]nformation relating to the capabilities, intentions, and activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorism activities.[35]

The methods of traditional foreign intelligence collection fall into the following five areas: imagery intelligence (IMINT), signals intelligence (SIGINT), human intelligence (HUMINT), measurement and signatures intelligence (MASINT), and open source intelligence (OSINT).[36] While the meanings of these disciplines are relatively well known and commonly understood among intelligence professionals, HSINT is more nebulous. Because HSINT is not necessarily source-specific, some would question whether it should be referred to as a collection "discipline." Although it is true that numerous unique entities are within DHS and at the state and local government levels, as well as within the private sector, that are aggressively collecting homeland security information, it is also true that many of the traditional aforementioned "INTs" collect homeland security intelligence insofar as they provide information on terrorism threats that may originate globally, yet are potentially manifested within U.S. borders. Within DHS Intelligence itself, the OSINT[37] and HUMINT[38] collection methods are likely to be most prevalent,[39] as departmental

---

[34] (...continued)
House of Representatives, *Rules and Appendix for the Committee on Homeland Security*, Committee Print 109-B, Oct. 2005.

[35] See 50 U.S.C., §401a.

[36] For a detailed description for each of these collection disciplines, see Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, CQ Press, 2003, pp. 63-83.

[37] OSINT involves collection of publicly available information from a wide variety of sources, including through media, government, and professional and academic venues. According to Mark Lowenthal, "Despite the fact that OSINT has always been used, it remains undervalued by significant segments of the Intelligence Community." See *Intelligence: From Secrets to Policy*, p. 80. See also CRS Report RL33539, *Intelligence Issues for Congress*, by Richard A. Best, Jr.

[38] For purposes of DHS intelligence collection, HUMINT is used to refer to *overt* collection of information and intelligence from human sources. DHS does not, generally, engage in covert or clandestine HUMINT.

[39] IMINT could also be leveraged to contribute to border security by providing "snapshots" (continued...)

personnel are not trained as traditional intelligence officers who use covert methods to collect intelligence.

The other type of intelligence codified in law is counterintelligence, which is defined as

> Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.[40]

With respect to counterintelligence, DHS Intelligence has as one of its objectives to "consistent with legal authorities, establish measures to protect the Department against hostile intelligence and operational activities conducted by or on behalf of foreign powers or international terrorist activities."[41] Focused as these activities may be on the Department itself, and being consistent with other laws and executive orders, this objective may be reasonable.

To some extent, however, at least for semantics if not necessarily for jurisdictional purposes, the differences between foreign intelligence and counterintelligence were attenuated with the passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458). The IRTPA sought to remedy numerous problems uncovered by the 9/11 Commission, one of which was the aforementioned gap between foreign and domestic intelligence. The IRTPA amended the National Security Act of 1947 (50 U.S.C. §401a) to read,

> The terms 'national intelligence' and 'intelligence related to national security' refer to all intelligence, regardless of source from which derived and including information gathered within or outside the United States that (a) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and (b) that involves - (I) threats to the United States, its people, property, or interests; (ii) the development,

---

[39] (...continued)
of U.S. borders. Unmanned Aerial Vehicles (UAVs) have been used for purposes of border surveillance. See CRS Report RS21698, *Homeland Security: Unmanned Aerial Vehicles and Border Surveillance*, by Christopher Bolkom. For an assessment of DHS's border intelligence strategy, see "Intelligence and Border Security," a hearing held by the House Homeland Security Committee, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, June 28, 2006. Among others, testimony was provided by Charles Allen, DHS Chief Information Officer, and the directors of the intelligence entities with DHS's Bureau of Customs and Border Protection, Bureau of Immigration and Customs Enforcement, as well as the U.S. Coast Guard. See also Chris Strohm, "Border Intelligence Plan Still in 'Early Stages' Official Says," in *Government Executive.com*, June 28, 2006.

[40] See 50 U.S.C., §401a.

[41] See *DHS Intelligence Enterprise Strategic Plan*, p. 11. DHS points out that its counterintelligence authorities are "limited to those of the United States Coast Guard."

> proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on U.S. national or homeland security.[42]

As such, HSINT could be interpreted as synonymous with intelligence related to national security, or some subset thereof.

A framework for outlining the scope of HSINT, or at least the criteria by which it might be framed could prove helpful. While there are numerous approaches to framing homeland security intelligence, three possible approaches are discussed below.

Approaches to Framing Homeland Security Intelligence

There are at least three different constructs that could be used to frame HSINT: (1) geographic (2) structural, and (3) holistic. **Table 1** summarizes some of the limits and boundaries of these three possible approaches to framing HSINT. Beyond geographic bounds, another set of differentiating factors between these approaches is the extent to which, if at all, one believes homeland security intelligence is the sole purview of the federal government, or a more inclusive and cooperative federal, state, local, tribal, and private sector model.

Table 1. Approaches to Defining Homeland Security

Approach	Geographic Bounds	Government Level Bounds
Geographic	Yes	No
Structural/Statutory	No	Yes
Holistic	No	No

Geographic Approach

Homeland security intelligence can be viewed, some might argue rather simplistically, in geographic and federal/state/local government terms. That is, if the intelligence collection activity takes place within the United States — whether it be by a federal agency or a state, local, tribal, or private sector actor, it would be considered HSINT. Under this approach, while HSINT's activities are constrained by borders, the yield from homeland security's collection and analysis could be combined with foreign intelligence to develop a more complete picture of homeland security threats. Others might counter that the problem with this type of approach is that, as the events of September 11, 2001, demonstrated clearly, national borders increasingly have little meaning in determining threats to U.S. national and homeland

[42] See Section 1012, Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) codified at 50 U.S.C. §401a.

security. As has been well documented by numerous studies,[43] the planning for the events of 9/11 took place largely overseas, but the acts were executed within U.S. borders. An intelligence approach that considered only activities associated with homegrown threats, without a more integrated, global perspective on the threat, would miss one of the central lessons learned from 9/11 — the importance of integrating intelligence related to threats to national security regardless of the geographic location of the source.

Structural/Statutory Approach

Homeland security intelligence could be viewed as primarily a federal activity. Geography is not as important under this approach, as the federal entities that engage in homeland security intelligence may, directly or indirectly, collect information outside the United States. For example, the FBI, through its Legal Attache Program, has more than 50 Legal Attache offices around the world through which it collects largely criminal information through open liaison with international law enforcement counterparts. More specifically, under this approach, HSINT is a federal activity that is engaged in by certain statutory members of the Intelligence Community. Thus, of the 16 agencies that are statutory members of the IC, under this approach perhaps only four would engage in domestic intelligence activities — the intelligence elements of the Federal Bureau of Investigation (FBI)[44]; the intelligence elements of

---

[43] See *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, a report of the U.S. Congress, Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, S.Rept. 107-351; H.Rept. 107-792, Dec. 2002, pp. xv, xvi, 37-39, 337-338. (Hereafter cited as *JIC Inquiry*.) See also *Final Report of the National Commission on Terrorist Attacks Upon the United States* and *The Commission of the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 2005.

[44] The intelligence elements of the FBI generally include the following four elements under the purview of the recently established National Security Branch: (1) the Directorate of Intelligence, (2) the Counterterrorism Division, (3) the Counterintelligence Division, and (4) the Weapons of Mass Destruction Directorate. If one defines "intelligence" as including criminal intelligence, then the FBI's Criminal Investigative and Cyber Divisions may also have an intelligence role, but they are not formally part of the National Security Branch, as directed by the President. See "Strengthening the Ability of the Department of Justice to Meet Challenges to the Security of the Nation," a *Presidential Memorandum*, June 29, 2005. The Presidential Memorandum approves the related recommendation from the Weapons of Mass Destruction Commission. It can be found at [http://www.whitehouse.gov/news/releases/2005/06/20050629-1.html]. For an assessment of the FBI's implementation of intelligence reforms, see *Report on the Status of the 9/11 Commission Recommendations — Part II: Reforming the Institutions of Government*, Oct. 20, 2005; CRS Report RL33033, *Intelligence Reform Implementation at the Federation Bureau of Investigation: Issues and Options for Congress*, by Alfred Cumming and Todd Masse; U.S. Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Efforts to Hire, Train and Retain Intelligence Analysts*, May 2005; National Academy of Public Administration, *Transforming the FBI: Progress and Challenges*, Feb. 2005; 9/11 Public Discourse Project, *FBI Reform*, Prepared Statement of Lee H. Hamilton, Former Vice Chair, National Commission on Terrorist Attacks Upon the United States, before the Senate Committee on the Judiciary, July 27, 2005. The 9/11 Public Discourse Project, in its final report assigned

(continued...)

the Department of Homeland Security (having information analysis responsibilities) and the U.S. Coast Guard; the intelligence elements of the Treasury Department; and the intelligence elements of the Energy Department. Others might argue this approach is too parochial, as it discounts the important homeland security intelligence roles played by other statutory members of the IC and non-federal actors, such as state and local intelligence fusion centers and the private sector.

Holistic Approach

Under this approach, HSINT is not bounded by geographic constraints, level of government, or perceived mutual mistrust between public and private sectors. That is, the approach recognizes no borders and is neither "top down" nor "bottom up." It involves and values equally information collected by the U.S. private sector owners of national critical infrastructure, intelligence related to national security collected by federal, state, local, and tribal law enforcement officers, as well as the traditional "Ints" collected by statutory members of the IC. It involves strategic and tactical intelligence[45] designed to prevent attacks on the U.S. homeland, as well as highly tactical and event-driven information coordination that must take place in response to a terrorist attack or national disaster.[46] Yet such an approach also implies a level

---

[44] (...continued)
the FBI a grade of "C" with respect to the erstwhile Commission's recommendation that the FBI establish a national security workforce.

[45] Strategic analysis provides a broad scope of analytical activities designed to assess national threats, threat trends, and the *modus operandi* of individuals or groups that threaten U.S. national security. As defined by the 9/11 Commission, the role of strategic (counterterrorism) analysis is to "look across individual operations and cases to identify trends in terrorist activity and develop broad assessments of the terrorist threat to U.S. interests." See "Law Enforcement, Counterterrorism, and Intelligence Collection in the United States Prior to 9/11," Staff Statement No. 9, p. 8. Although strategic analysis can be highly useful to operational personnel, its intended consumer set includes, but is not limited to, national-level policy and decision makers. Tactical analysis, on the other hand, is generally thought of as analysis which provides direct support to an ongoing intelligence operation or investigation. Tactical and strategic intelligence analyses are mutually supportive.

[46] Pursuant to HSPD-5, *Management of Domestic Incidents*, the Secretary of Homeland Security is the "principal federal official for domestic incident management." Under certain circumstances, the Secretary of Homeland Security "shall coordinate the federal government's resources utilized in response to or recovery from terrorist attacks, major disasters, or other emergencies." Part of such coordination is the management of information or intelligence sharing both within the federal government and between level of governments, as well as the private sector. The management of information relative to Hurricane Katrina has generally been assessed as poor. The 9/11 Public Discourse Project assigned a grade of "C" for the government's effort to establish a unified incident command system. The report concluded that, "although there is awareness of and some training in the Incident Command System (ICS), Hurricane Katrina demonstrated the absence of full compliance during a multi-jurisdictional/statewide catastrophe — and its resulting costs." See *Final Report of 9/11 Commission Recommendations*, Dec. 5, 2005, p. 1.

of information sharing between federal, state, local, tribal, and private sector information collection entities that does not appear to exist currently.[47]

Although information sharing between levels of government is widely held to be an undisputable public "good,"[48] information flows between levels of government appear to remain unequal.[49] Former Vice Chair of the 9/11 Commission, Lee H. Hamilton, recently testified that despite enactment of certain elements of the Intelligence Reform and Terrorism Protection Act of 2004 (P.L. 108-458), "We have made minimal progress toward the establishment of a seamless information sharing system. You can change the law, you can change the technology, but you still need to change the culture; you need to motivate institutions and individuals to share information."[50] William Crowell, a member of the Markle Task Force on National Security in the Information Age, recently testified that, "Meetings with state and local officials have led us to believe that the federal government has not yet realized the value of information identified by state and local entities. A system to integrate this information has not been developed. Much more attention must be paid to this gap, because we as a government are ignoring a critical component of national security."[51] Administration officials recognize the need for two-way information flow, as demonstrated by the statement of John Russack, former Program Manager,

---

[47] See National Governor's Association, Center for Best Practices, *2006 State Homeland Security Directors Survey*, Apr. 3, 2006.

[48] There are, however, some valid arguments for not sharing all intelligence with all stakeholders. Information security, operational security, counterintelligence, and the "need to know" principle remain valid concerns in the national security community. Moreover, some would argue that there may be limited utility to sharing classified information with stakeholders that don't have appropriate dedicated resources to enable them to take security and other countermeasure actions based on the intelligence provided.

[49] For a critical assessment of the current status of information sharing between the federal government and state, local, and private sector law enforcement and security officials, see *Beyond Connecting the Dots: A VITAL Framework for Sharing Law Enforcement Intelligence Information*, An Investigative Report by the U.S. House Committee on Homeland Security Democratic Staff Prepared for Congressman Bennie G. Thompson, Ranking Member. See also *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism Related and Sensitive But Unclassified Information*, General Accountability Office, GAO-06-385, March 2006. For an assessment of the Homeland Security Information Network, one of the DHS tools to share information with state and local counterparts, see *Homeland Security Information Network Could Support Information Sharing More Effectively*, Department of Homeland Security, Office of Inspector General, Office of Information Technology, OIG-06-38, June 2006.

[50] See testimony of Lee H. Hamilton, Former Vice Chair 9/11 Commission, before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Committee on Homeland Security, U.S. House of Representatives, Nov. 8, 2005, p. 2.

[51] See testimony of William P. Crowell, member Markle Task Force on National Security in the Information Age, before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Committee on Homeland Security, U.S. House of Representatives, Nov. 8, 2005, p. 6.

Information Sharing Environment[52] that, "The *'environment'* we create needs to provide better access to federal terrorism information at the state and local levels — however, and of equal importance, it must also provide mechanisms to allow valuable information gathered by state and local officials to be used by federal agencies."[53] It is, however, one thing to recognize the need for change, and another to implement such change in an efficient and effective manner.

Under the holistic approach, the HSINT community might include the 16 statutory members of the IC (as each collects national intelligence, or intelligence related to national security which could have a profound impact on homeland security); the National Counterterrorism, National Counterintelligence, National Counter Proliferation, and Open Source Intelligence Centers; the 14 existing private sector Information Sharing and Analysis Centers,[54] scores of state and local law

---

[52] The establishment of the Information Sharing Environment (ISE) was mandated under Section 1016 of P.L. 108-458. The ISE is to be led by a Program Manager who has a term of two years; John Russack, a career Central Intelligence Agency official, was chosen as the first ISE Program Manager. Mr. Russack was succeeded by Ambassador Thomas E. McNamara. For an update on ISE progress, see "Building on the ISE: Addressing Challenges of Implementation," testimony of Ambassador McNamara before the House Homeland Security Committee, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, May 10, 2006. The 9/11 Public Discourse Project provided a grade of "D" to the federal government for implementing the Commission's recommendation to enhance incentives for information sharing. According to the Project, "The office of the program manager for information sharing is still a start-up, and is not getting the support it needs from the highest level of government." See *Final Report of 9/11 Commission Recommendations*, Dec. 5, 2005, p. 3. Some observers believe the executive branch decision to place the Program Manager for the Information Sharing Environment under the Office of Director of National Intelligence was a diminution of the Program Manager's effective authority. The argument has been made that the authority of the Program Manager to facilitate information sharing across federal, state, local governments, as well as between the federal government and the private sector, would be enhanced if it was placed within the Executive Office of the President.

[53] See Statement for the Record of John A. Russack, Program Manager, Information Sharing Environment, Office of the Director of National Intelligence, p. 7.

[54] ISACs were initially established in 1998 pursuant to Presidential Decision Directive 63 (PDD-63) *Protecting America's Critical Infrastructures.* PDD-63 has been superceded by Homeland Security Directive-7 (HSPD-7), *Critical Infrastructure Identification, Prioritization and Protection,* Dec. 17, 2003. The 17 critical infrastructure/key resources sectors are as follows: agriculture, food (meat, poultry, egg products); public health and healthcare, food (other than meat, poultry, and egg products); drinking water and waste water treatment systems; energy, including the production, refining, storage, and distribution of oil and gas and electric power (except for commercial nuclear power facilities); banking and finance; national monuments and icons; defense industrial base; information technology; telecommunications; chemical; transportation systems; emergency services; postal and shipping; dams; government facilities; commercial facilities; and nuclear reactors, materials, and waste. See *Interim National Infrastructure Protection Plan*, Feb. 2005, Exhibit 1, p. 3. The definition of critical infrastructure was codified in P.L. 107-56 (42 U.S.C §5195c) as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating

(continued...)

enforcement entities charged with gathering criminal intelligence, numerous state and regional "intelligence fusion" centers,[55] and federal entities with law enforcement responsibilities which may collect intelligence related to national security. This holistic approach implies an interdependency between the diverse players of the statutory IC and the broader HSINT Community. As Ambassador Henry A. Crumpton, a former CIA case officer and current Coordinator for Counterterrorism at the State Department states, although there are differences between intelligence and law enforcement,

> the primary customer for domestic foreign intelligence on near-term threats is law enforcement. And law enforcement can provide valuable leads for intelligence officers. The intelligence collector and the law enforcement consumer, therefore, must strive for more than information sharing; they must seek interdependence.[56]

Calls for interdependence between foreign intelligence and security or criminal intelligence today mirror those made nearly thirty years ago by Dr. Kent, who wrote

> The real picture of the diversity in kinds of intelligence... lies in this truth: a very great many of the arbitrarily defined branches of intelligence are interdependent. Each may have its well-defined primary target which it makes its primary concern, but both the pursuit of this target and the byproducts of pursuing it bring most of the independent branches into some sort of relationship with the others.

---

[54] (...continued)
impact on security, national economic security, national public health or safety, or any combination of those matters."

[55] According to the National Governor's Association Center for Best Practices, as of July 7, 2005, a survey of the state homeland security directors revealed that there were, as of the date of publication, 24 state intelligence "fusion centers." States were allowed to self-select — that is — if they believed they had a fusion center, they reported it. Since then, numerous states have established or are in the process of establishing fusion centers, bringing the number of such centers to over 40. See Joe Trella, *State Intelligence Fusion Centers: Recent State Actions*, National Governors Association, Center for Best Practices, July 7, 2005. See also National Criminal Intelligence Resource Center, *State and Regional Intelligence Fusion Center: Contact Information*, Mar. 8, 2006.

[56] See Henry A. Crumpton, "Intelligence and Homeland Defense," in Jennifer E. Sims and Burton Gerber, *Transforming U.S. Intelligence*, (Georgetown University Press, 2005), p. 210. Ambassador Crumpton differentiates domestic *foreign intelligence* from domestic *security intelligence*. The former, according to Ambassador Crumpton, would best be collected by formally trained intelligence case officers analogous to those within the Central Intelligence Agency's Directorate of Operations. By contrast, domestic security intelligence, according to Crumpton, would best be undertaken by a new hybrid of professional, the special agent-case officer (SACO). Ambassador Crumpton recommends the establishment of a domestic security intelligence corps "with its own budget and personnel, preferably as part of the FBI but under the explicit direction of U.S. intelligence leadership." Some would argue that the establishment of the National Security Branch at the FBI, pursuant to a recommendation of the WMD Commission, represents a step in this direction.

> Intelligence as an activity is at its best when this fact is realized and acted upon in good faith.[57]

The challenge, then as now, is to implement such a vision where all players in the de facto HSINT Community would be treated as partners with value to add. What has changed substantially since Dr. Kent's seminal work is the addition of state, local, and private sector actors as both producers and consumers of intelligence. It is here — in the interaction with these relatively new players — that DHS Intelligence has a great role to play. The clear elucidation of HSINT role and responsibilities and implementation, particularly between the FBI and DHS Intelligence, remains an evolving process. A broader understanding of the members and functions of the HSINT Community and the DHS members of the community may be helpful in assessment of these matters.

The Homeland Security Intelligence Community

The federal IC is defined in law, yet the homeland security intelligence community (HSIC) remains a somewhat nebulous entity. As defined with the *DHS Intelligence Enterprise Strategic Plan*, the HSIC "includes the organizations of the stakeholder community that have intelligence elements."[58] The Homeland Security Stakeholder Community is defined broadly 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.[59]

Notwithstanding the fact that a HSIC is not statutorily defined, and may not necessarily be a useful construct from a managerial perspective, such a community, as traditionally defined, exists. The members and collective responsibilities of this community depend, to some extent, on how one bounds the function of HSINT. As mentioned above, the broader the definition of HSINT, the wider the range of players in the community. If one adopts the holistic model of HSINT, the HSIC would include a broad range of agencies, many of which are hybrid agencies undertaking homeland security, law enforcement, defense, and/or traditional foreign intelligence functions. These entities include, among others, the intelligence elements of, the Department of Defense, Northern Command,[60] and Counterintelligence Field

---

[57] See Sherman Kent, *Strategic Intelligence* (Archon, 1965), p. 220.

[58] See U.S. Department of Homeland Security, *DHS Intelligence Enterprise Strategic Plan*, Jan. 2006.

[59] Ibid., p. 4.

[60] The Department of Defense, some would argue, has traditionally been the IC's one thousand pound gorilla, and has, according to others, expanded its role in domestic intelligence. See Walter Pincus, "Pentagon Expanding Its Domestic Surveillance Activity," in *Washington Post*, Nov. 27, 2005, p. A6. The Department of Defense's Northern Command (NORTHCOM) differentiates its mission, homeland *defense*, from homeland

(continued...)

Activity; the Department of Justice's Federal Bureau of Investigation, Bureau of Alcohol, Tobacco, Firearms, and Explosives, and Drug Enforcement Agency; the Central Intelligence Agency's National Resources Division; the Department of Treasury's Office of Terrorism and Financial Intelligence, and the Department of Energy's Intelligence and Counterintelligence entities. Numerous state and local law enforcement entities, and state-based intelligence "fusion centers" that collect largely criminal intelligence, would fall under a broad interpretation of homeland security intelligence. Finally, the private sector, particularly those sectors outlined as being part of the U.S. critical national infrastructure (as defined under Homeland Security Presidential Directive/HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003) would also fall into a broadly defined concept of a homeland intelligence community.

An interesting comparison can be drawn between the HSIC and the statutory IC, as defined in the National Security Act of 1947, as amended (50 U.S.C. note 401) and in subsequent Executive Orders. One general definition of the IC is a "federation of Executive Branch agencies and organizations that conduct intelligence activities necessary for the conduct of foreign relations and protection of national security."[61] A federation differs from a community insofar as the constituent elements of a federation, by definition, give up some degree of authority to a more central body. A community, by contrast, implies a group of persons or entities merely having common interests, but not necessarily bound together by any formal power sharing arrangements or agreements. While the IC has arguably moved more in the direction of a federation with the establishment of a Director of National Intelligence (DNI),[62] one could argue the HSIC, broadly defined, remains very much a community spread across federal, state, local government sectors, as well as the private sector. The diffuse nature of a broadly defined HSIC may be dictated by the very nature of the function itself. That is, if state, local, tribal and private sector members are valued and contributing members of the HSIC, an attempt at centralization may undermine the community's effectiveness and efficiency. Planned decentralization, with a clear understanding of the roles played by each level of organization, and the parameters

---

[60] (...continued)
security by stating that homeland security is a national effort that begins with local, state and federal organizations, yet homeland defense is "the protection of U.S. territory, domestic population and critical infrastructure against military attacks emanating from outside the United States." It provides further that NORTHCOM's domestic activities are guided by numerous laws, including the Posse Comitatus Act (PCA). While PCA prohibits direct military involvement in domestic law enforcement activities, there are a number of exceptions to this general prohibition.
See [http://www.northcom.mil/index.cfm?fuseaction=s.homeland]. See also CRS Report RS21012, *Terrorism: Some Legal Restriction on Military Assistance to Domestic Authorities Following a Terrorist Attack*, by Charles Doyle and Jennifer Elsea.

[61] See [http://www.intelligence.gov/1-definition.shtml].

[62] See CRS Report RS22112, *Director of National Intelligence: Statutory Authorities*, by Richard A. Best, Jr., Alfred Cumming, and Todd Masse.

of how information is shared bi-directionally, is one model of organization for the HSIC.[63]

[63] An organization's structure and business processes influence its performance. Large organizations with dispersed operations continually assess the appropriate balance between decentralized and centralized elements of their operations. Although the mission of National Aeronautics Space Administration (NASA) is unrelated to that of HSINT, NASA also has dispersed operations. In a review of the causes of the 1986 Columbia shuttle accident, the board investigating the accident found that "The ability to operate in a centralized manner when appropriate, and to operate in a decentralized manner when appropriate, is the hallmark of a high-reliability organization." See *Columbia Accident Investigation Report*, vol. I, Aug. 2003, at [http://www.caib.us/news/report/volume1/default.html].