The Domestic Intelligence Gap: Progress Since 9/11?

James Burch

INTRODUCTION

> *"Near-term policies have long-term consequences, and a central responsibility of grand strategy is a concern with the long term rather than merely the immediate."*
> Steven D. Biddle[1]

The purpose of a *grand strategy* is to "direct all the sources of a nation, or band of nations, towards the attainment of the political object . . . the goal defined by fundamental policy."[2] Strategic events, such as Pearl Harbor (1941) or the *Sputnik* launch (1957), can also serve as the impetus to reevaluate national policies. In other words, they can alter strategic policy in fundamental ways. The United States transitioned from an isolationist position to a global worldview as a result of Pearl Harbor; *Sputnik* was the catalyst to totally redefine the U.S. approach to space. Such events often serve as mandates for change.

The attacks on 9/11 were another strategic event and mandate for change. The inability of the U.S. intelligence community to "connect the dots" due to inefficient information-sharing mechanisms and the gap in domestic intelligence led to a significant debate about improving the nation's intelligence apparatus.[3] These attacks also served as the rallying point for reformists to improve the ability to share information. As a result, the 9/11 attacks prompted the largest reorganization of the intelligence community since 1947.[4]

Intelligence reorganization and reform since 9/11 have resulted in numerous changes. Most significant were the creation of several national organizations – the Department of Homeland Security (DHS), the Director for National Intelligence (DNI), the National Counter Terrorism Center (NCTC) – and the revamping of the Federal Bureau of Investigation's (FBI) intelligence capability.[5] These changes, coupled with an emphasis on information sharing and the development of state and local fusion centers, have resulted in the significant application of resources and effort to address the domestic intelligence gap.[6]

Reorganization and reform, however, raise other questions, particularly as they relate to domestic intelligence. First, are these changes making the nation more secure? New and major organizational changes often lead to significant implementation issues. Second, has information sharing improved as a result of these efforts? *Information sharing* can carry multiple meanings within the intelligence community, which lead to a wide variety of implementation issues and differences in consumer expectations. Lastly, have there been corresponding improvements in the intelligence oversight mechanisms to prevent domestic intelligence abuse? Domestic intelligence collection remains a very sensitive issue for the U.S. public.

While *organizational mechanisms*, *information sharing*, and *intelligence oversight* are the critical components for ensuring an effective domestic intelligence capability,[7] there is also a temporal issue. Are these efforts transforming the intelligence community over time to reach an envisioned goal? In other words, is the community meeting its projected milestones while progressing towards a well understood objective? *Transformation* is another term that can frequently be misinterpreted and is often equated with implementing technological change. For purposes of this inquiry, the question is whether the domestic intelligence community is transforming by reorganizing itself optimally, developing improved processes and implementing cutting-edge technological solutions?[8] In this case, *organizational approaches*, *process development,* and *technology* within the context of an envisioned outcome would constitute the elements of transformation.

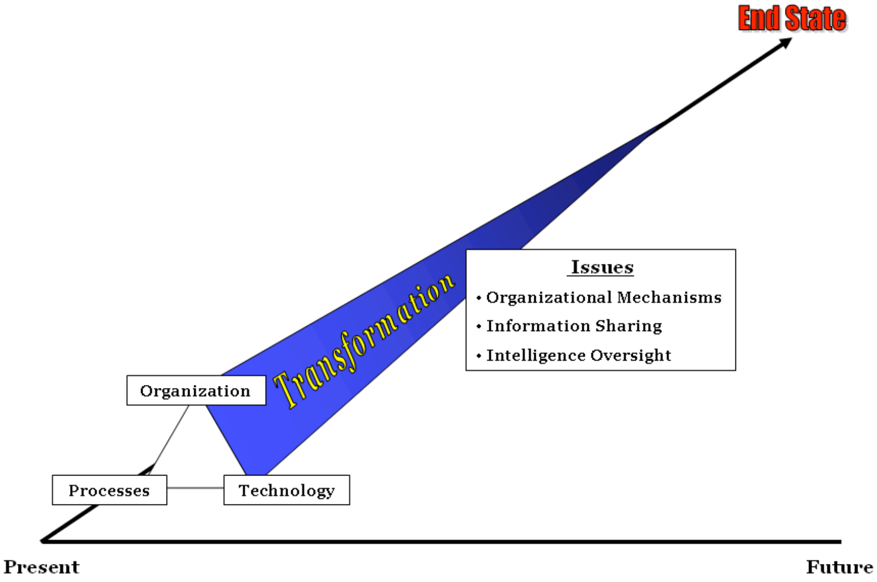

Figure 1: Transformation Framework

Examining the critical elements of domestic intelligence – organizational mechanisms, information sharing, and intelligence oversight – within the context of transformation will lead to a determination of what has been accomplished since 9/11. It will also lead to identifying key issues, gaps, and implementation obstacles. Lastly, an examination of these elements within the larger context of transformation can result in better determining the long-term effects of present policies and whether these policies are on target to eliminate the domestic intelligence gap and realize the envisioned end state for domestic intelligence.

THE COLD WAR: CENTRALIZED APPROACH TO INTELLIGENCE (1947-1992)

> *America today, as never before in time of peace, is vulnerable to sudden and possibly devastating attack. To meet an initial attack, there are no sure military weapons of defense and it may well be that our best protection lies in adequate knowledge of the character and timing of the danger.*
>
> Intelligence Survey Group (1949)[9]

To better understand the present challenges of implementing a domestic intelligence capability, it is important to note that many of today's issues are well grounded in the past. In essence, the issues of organizing, sharing information, and implementing effective intelligence-oversight mechanisms are the same issues that policy-makers have faced since the establishment of the peacetime intelligence apparatus.

The start of the Cold War represented a strategic event and mandate for structuring the U.S. intelligence community. The establishment of a standing intelligence apparatus was effected by the passage of the *National Security Act of 1947*. This act established the Central Intelligence Agency (CIA), unified the military departments under the new Department of Defense (DoD), and created the National Security Council (NSC) structure. The prevalent view at the time was that a centralized intelligence network headed by the CIA – whose director would also act as the Director of Central Intelligence (DCI) – would ensure information sharing and optimize efficiencies.[10] Despite the establishment of this model, organizational challenges, the development of information sharing mechanisms, and oversight concerns became significant policy issues for decision-makers.

Organization

Numerous commissions and studies have been chartered since 1947 to examine the role and organization of intelligence agencies. Since its inception, the authority of the DCI to orchestrate intelligence policy and actions has been limited in large part by organizational friction from other departmental intelligence agencies, most notably the Department of State (DoS) and the DoD.[11] The Intelligence Survey Group (1948-1949), an early body charged with assessing the intelligence community, found that the CIA has very little, if any, explicit authority to coordinate national intelligence activities.[12] Efforts to enhance the DCI's ability to manage the intelligence community, by creating the Intelligence Community Staff (ICS) in 1972,[13] were largely offset by the tremendous growth of other intelligence agencies and the technological complexities in collecting and processing intelligence.[14]

Other organizational issues manifested themselves and have proved to be enduring – analytic capacity, duplication of effort, and over-classification of intelligence products. The First Hoover Commission (1949) identified serious shortfalls in analytic capacity, particularly for dealing with specialized topics such as scientific, medical, chemical, biological, and nuclear intelligence.[15] The Intelligence Survey Group also identified critical shortfalls in maintaining qualified personnel to meet the new challenges of the Cold War.[16] The challenges of maintaining and developing intelligence competencies were further highlighted in the Schlesinger Report (1971) and the Church Commission (1976),[17] thirty years after this was identified as an issue.

Duplication of effort was another early organizational challenge. Concerned with matters of efficiency, the Intelligence Survey Group found "the amount of undesirable duplication among intelligence agencies is considerable and the absence of coordinated intelligence collection and production is serious."[18] Excessive duplication continued to plague the intelligence community as organizational and technological complexity increased.[19] Conversely, the need for developing and incorporating opposing analytic alternatives and differing points-of-view was not overlooked.[20] Reconciling excessive duplication and the need for opposing alternatives, however, was never addressed satisfactorily.

Over-classification – a present day issue – was also a subject of early contention. The Doolittle Report (1954) identified the tendency of intelligence agencies to over-classify their products.[21] Although the need for safeguarding intelligence through compartmentalization is and was necessary – particularly during the Cold War – over-classification places an excessive level of control on the distribution of intelligence. Agencies were likely to carefully guard their sources, methods, and data by furnishing only finished intelligence products. The resultant effect was to solidify the organizational control of primary data and provide finished intelligence via cumbersome handling caveats and processes. While technological solutions were more limited during this period, the lack of joint planning and an inability to develop common data standards and templates resulted in stovepiped systems and increased complexity.

Information Sharing

Shortfalls in information sharing and cooperation also manifested soon after the enactment of the *National Security Act*. With regard to domestic intelligence, the Intelligence Survey Group identified reluctance on the part of the FBI to attend interagency committee meetings.[22] The Second Hoover Commission (1955) also called for increased collaboration and sharing of information between the CIA and FBI on counterespionage activities.[23]

Information sharing and cooperation became increasingly difficult as organizational complexity, duplication of effort, and limitations on the DCI's span of control over intelligence activities increased. In large part, the Schlesinger Report attributed shortfalls in information sharing and cooperation to increased complexity, duplication, and poor joint-planning mechanisms.[24] The control of primary data and poor dissemination methods also contributed to these shortfalls. Competition between the CIA and other cabinet departments further compounded information sharing efforts. The Schlesinger Report concluded by recommending the establishment of a DNI to bring more coherence to the intelligence community.[25] The idea of a DNI would continue to gain momentum with other commission recommendations and studies.[26]

Intelligence Oversight

Although intelligence oversight issues did not gain public exposure until the 1970s, the ability to conduct oversight within a free society was of initial concern to senior intelligence decision-makers. The Intelligence Survey Group opined:

> It is all very well for a group with no responsibilities or authority to state that both Congress and the Bureau of the Budget [precursor to the Office of Management and Budget] must understand that the Central Intelligence Agency must be given, in effect, a blank check and a free hand. In practice, the Central Intelligence Agency must justify its demands with some reason and logic . . . .[27]

Concerns over intelligence oversight were so fundamental that the first proposal to create a Joint Senate and House Committee on Intelligence (JCI) occurred in 1948 – one year after the passage of the *National Security Act*.[28] A joint committee, consisting of senators and congressman, has been cited repeatedly as a model to streamline legislative oversight, better safeguard intelligence, and consolidate congressional jurisdiction to better focus oversight.[29] The rapid expansion of the intelligence community in the 1950s, both in terms of organizational and technological complexity, resulted in continued calls for the establishment of Congressional oversight mechanisms.[30] President Eisenhower established the precursor to the Presidential Foreign Intelligence Advisory Board (PFIAB) in 1956, to institute executive oversight mechanisms and largely as a measure to preempt further congressional inquiries into intelligence activities.[31]

The U.S. political environment changed drastically in the 1960s. Several intelligence agencies became more involved in domestic intelligence and surveillance activities as a result of the concerns over communist involvement in the civil rights movement and increasing opposition to the Vietnam War. The lack of strong and established oversight mechanisms resulted in several abuses, such as the infiltration of the CIA into student groups.[32] Several studies and commissions were enacted in the 1970s as a result of these abuses. Although not the result of an intelligence agency, Watergate further increased concerns over domestic surveillance. As a result, the Murphy and Rockefeller Commissions (1975) recommended the strengthening of the PFIAB and executive oversight mechanisms.[33] The Congressional Church and Pike Commissions, however, dramatically limited the involvement of intelligence agencies in domestic affairs and law enforcement.[34] These congressional inquiries also led to the establishment of congressional committees on intelligence in the House and Senate[35] and the passage of the *Foreign Intelligence Surveillance Act (FISA) of 1978* to provide a framework for establishing procedures for the surveillance of U.S. persons linked to foreign intelligence threats.

Conclusion

The centralized intelligence network model enacted by the *National Security Act* laid the foundation and structure for the intelligence community for the duration of the Cold War. Although nominally headed by the CIA, increases in the number of organizations, their autonomy, and the proliferation of technical collection systems increased organizational complexity. Despite the creation of the ICS – the precursor to the DCI's Community Management Staff – the ability of the DCI to manage the intelligence community lessened as the span of control over various intelligence activities diminished and competition from other departments increased.

Other enduring issues, such as quality of personnel, duplication of effort, over-classification, and questions on intelligence oversight also affected the community. A consistent theme throughout these studies was the need for maintaining and improving the quality of analysis in an increasingly complex intelligence environment. Duplication of effort, as a result of increased complexity and competition, resulted in the poor management of intelligence resources. Additionally, the need to balance the minimization of duplication while incorporating opposing alternatives was not satisfied. Over-classification of intelligence products led to an increasingly cumbersome dissemination process, which further inhibited the sharing of intelligence. Lastly, domestic intelligence abuses resulted in the establishment of congressional oversight mechanisms. The unintended consequence, however, was the establishment of the "wall" between intelligence and law enforcement activities.

POST COLD WAR: OPPORTUNITY FOR TRANSFORMATION (1992-2001)

> *We must avoid the costly mistake of 1919, 1945, 1953, and 1975 in thinking that we can disengage from the world or that we can or should quickly disarm ourselves or weaken our national security institutions.*
>
> Robert M. Gates[36]

The ending of the Cold War and the diminished threat of a confrontation between super powers represented another strategic event and mandate for change. In this case, an intelligence apparatus largely designed and constructed to combat the Soviet Union now faced a different future – an opportunity to redefine itself and better focus on emerging targets. Several persistent intelligence paradigms had changed as well. First, strategic and tactical intelligence became obscured.[37] National intelligence systems were brought to bear on a large scale during the First Gulf War and tactical events on the ground took on significant strategic implications. Second, despite the lack of a peer super power, other intelligence needs quickly became apparent – international crime, weapons proliferation, and terrorism.[38] These issues, transnational and transborder in nature, required different and collaborative intelligence approaches. Lastly, the 1990s saw a proliferation of telecommunication technologies. Once contained within the purview of governmental and intelligence agencies, the increasing proliferation of telecommunications technology in the private industry and greater individual use of personal communications had significant implications to organizational and information sharing approaches. These developments would also result in profound changes to intelligence consumer expectations.

Organization

Numerous studies aimed at reforming the intelligence community were also conducted during this period. The intent of the *Intelligence Reorganization Act of 1992* was to eliminate duplication and waste while improving efficiency.[39] Better known as the Boren-McCurdy legislation, the bill proposed the establishment of a DNI along with reorganizing intelligence agencies according to function – an agency for analysis, others for human intelligence, signals intelligence, and imagery intelligence collection.[40] This bill did not pass, due to significant opposition from the DoD and the lessons learned from the use of national intelligence systems during the First Gulf War.[41]

Ironically, the question of whether a centralized intelligence network model was ideally suited to meet different problem sets – such as narcotics, crime, and terrorism – was never approached. The emphasis on streamlining, consolidating, and downsizing implied that the current organizational architecture was suited to meet the new challenges.[42] The dilemma of eliminating all duplication at the cost of alternative analysis was also not fully explored. To highlight the value of alternative analysis between intelligence agencies: "The CIA deflated military intelligence estimates of a "bomber gap" in the 1950s. In 1973, NSA analysts noticed signs of an approaching Middle East war that analysts from other agencies ignored."[43] In these cases, military intelligence and the NSA were more accurate.

Information Sharing

The events of the First Gulf War, and the use of national intelligence systems and sophisticated capabilities to support military forces coupled with vast improvements to communications technology, had significant implications for information sharing. These changes in effect led to operationalizing intelligence on an unprecedented scale. This paradigm shift – when linked to the increasing sophistication on the part of the intelligence consumer – resulted in greater demands for intelligence products and support. This increasing sophistication also resulted in the consumer being more comfortable with handling data versus being fed conclusions via finished intelligence products.[44]

The changing nature of the threat also produced new challenges to information sharing. The FISA model of processing electronic surveillance requests increasingly became more difficult as intelligence and law enforcement agencies were forced to collaborate on transnational threats – terrorism, illicit financing, and crime.[45] Legislation did not keep up with these changes. The FBI's organizational role also changed during this period. The bureau became increasingly involved in overseas activities to combat these crimes – further obscuring the roles of the CIA and FBI.[46] Other challenges to sharing information were the result of having new customers. The need to disseminate information outside the national security community – to financial experts, scientists, and law enforcement officials – further exacerbated the issues of over-classification, handling caveats, insufficient clearances, and poor dissemination methods.[47]

As a result of the changing threat and blurring of foreign-domestic mandates, the Aspin-Brown Commission (1996) identified the need for law enforcement and intelligence agencies to share information.[48] As late as 2000, the *National Commission on Terrorism*, headed by L. Paul Bremmer, identified the continuing shortfalls to integrating law enforcement and intelligence information against rising terrorism concerns.[49] These concerns, while explicitly stated, lacked the political consensus to translate into effective strategies.[50]

Oversight

Intelligence oversight concerns during the 1990s remained an issue, particularly due to the changing nature of the threat and blurring of the law enforcement and intelligence communities. The proliferation of technology was also cause for concern. Although the need to develop information sharing processes between the intelligence and law enforcement communities was recognized, there were limited attempts to improving the oversight mechanisms to facilitate these changes.[51] Of note, however, were the continued discussions whether to create a joint congressional intelligence committee to better track intelligence activities.[52]

Conclusion

The 1990s afforded a window of opportunity to reexamine existing intelligence structures and processes. The centralized intelligence network model, perhaps more suited to the Cold War, faced increasing strains in dealing with changing paradigms. The shifting of the threat from nation-based to transnational threats did not result in corresponding changes to organizational structures or processes. In fact, the opposite proved to be the case. The emphasis on streamlining, consolidating, and downsizing forced the intelligence agencies to prioritize in a resource-scarce environment. Transnational terrorism issues often received lower priorities. The consolidation efforts of different agencies also had the corresponding effect of narrowing ideas and providing poor alternative analysis.[53] The downsizing environment afforded little opportunity for change despite recommendations for significant capital investments in national security training – particularly in the linguistic and technical fields – to better meet the challenges of a new era.[54]

The FISA model continued to operate and the intelligence community was unable to capitalize on the telecommunication explosion because of its largely entrenched bureaucracy.[55] The continued adherence to cumbersome classification processes further alienated the intelligence community from its increasingly sophisticated and growing nontraditional consumer base.

The inability to streamline information sharing processes between the law enforcement and intelligence communities also proved problematic. Although numerous commissions and studies had identified the problem, the lack of political consensus and public awareness prevented any meaningful transformation efforts. The centralized intelligence network model, calcified processes, and existing oversight architectures remained in place during the 1990s and operated with no apparent change until 9/11. This would have drastic consequences on the ability to effectively conduct domestic intelligence.

POST-9/11: OPPORTUNITY FOR TRANSFORMATION? (2001-2007)

Merely solving this type of crime is not enough; it is equally important that the FBI thwart terrorism before such acts can be perpetrated.
Louis Freeh, FBI Director, in response to the 1993 World Trade Center Attack[56]

We did not disseminate information we received in early 1999 that was unexceptional in its content except that it associated the name of Nawaf al-Hamzi with Al Qa'ida [a clue that could have identified three 9/11 hijackers].
General Hayden, NSA Director, testifying before the Joint Congressional Inquiry to 9/11

The 9/11 attacks were unprecedented in terms of loss of life and destruction. These attacks, however, were not unprecedented in terms of the threat posed to the United States. The 1993 attack on the World Trade Center prompted calls for intelligence reform. Intelligence reporting beginning in 1998 through 2001 also indicated the intent of terrorists to strike in the United States,[57] however, shortfalls in information sharing and political consensus resulted in an ineffectual response. The U.S. government had also identified the terrorist use of civilian airliners as a possible weapon of mass effect.[58] Despite these indicators and rising concerns on terrorist activities in the 1990s, it was the 9/11 attacks that proved the impetus for reforming intelligence.

There have been numerous initiatives to reorganize and make the nation more secure. Reorganization, however, does not equate to reform, although reorganization efforts can provide a window of opportunity for change.[59] In terms of domestic intelligence, several arguments have been proposed regarding the viability of establishing a domestic intelligence agency. While it is not necessary to recount these arguments, a comparative analysis between the current U.S. approach – creating NCTC, establishing DHS with an intelligence charter, and bolstering the FBI – and the domestic intelligence agencies of the United Kingdom, Australia, and India illustrates the domestic intelligence agencies are not necessarily an end-all solution to solving the domestic intelligence gap.[60]

Interestingly, although the 9/11 Commission did not recommend the establishment of a domestic intelligence agency, the recommendation to not establish an agency was contingent on two issues: the effectiveness of intelligence organizations (the NCTC and FBI) to combat terrorism domestically *and* the ability to effect *meaningful change*.[61] The critical questions to ask – given seven years after the 9/11 attacks – are whether the creation of new institutions is making the nation safer and whether meaningful change is occurring. In essence, is transformation – organizational effectiveness, process development, and use of technology in new ways – changing the nature of intelligence? Are the enduring intelligence challenges that have burdened the community since 1947 also being addressed?

Organization

Director of National Intelligence. Theorists postulate that organizations can be expected to jealously guard their own interests to achieve their goals.[62] Within the intelligence community, knowledge indeed translates into power. Due to the classified nature of intelligence, organizations are more likely to wait out an administration that is not in line with its goals.[63] The new organizations that have been instituted since 9/11 – the DNI, DHS, and NCTC – also face challenges. As Eugene Bardach states:

> The Department of Homeland Security, for instance, is poorly positioned to receive intelligence from the intelligence community agencies because it does not do intelligence collection on its own and hence will have nothing to trade. . . . Cooperation between the FBI and CIA was hampered because there was no willing enforcer . . . perhaps the Director of National Intelligence.[64]

In essence, new organizations must fight to gain access. Lastly, longstanding organizations with highly developed and mission focused cultures – such as intelligence, the military, and law enforcement – are relatively impervious to outside reform.[65]

The challenges that currently face the DNI are daunting: a community that is resistant to reform, that is secretive in nature (with a culture of guarding information),[66] and has evolved into a highly complex community since 1947. Looking at the intelligence community's past history, it is also important to remember that the power of the DCI was limited and, despite numerous recommendations, the position of the DNI was not instituted largely because none of the primary actors *wanted the change*.[67] The ability of the DNI to effect transformation and reform will depend on three issues: the authorities linked to the DNI's span of control (i.e. control over budget and resources), bipartisan political support, and the ability to sustain transformation over an extended period of time.

Post 9/11 Intelligence Reform. The centerpiece to implementing an effective domestic intelligence capability lies largely with the ability of the FBI to implement reform and transform itself into a premier intelligence organization. Although there have been numerous initiatives to implement reforms and institutionalize an effective intelligence capability within the FBI,[68] there remain questions whether progress is in fact taking place. Intelligence personnel assigned to the FBI still find themselves performing secondary and supporting tasks.[69] At the heart of the intelligence issue is also the crucial question of whether the FBI is effectively linking its intelligence collection efforts to clearly articulated intelligence gaps.[70] Most importantly, information sharing problems still exist between the CIA and FBI – an enduring intelligence issue.[71]

Effecting FBI intelligence reform will also be difficult in a culture predominantly based on law enforcement – one highly resistant to change. It is important to remember that the FBI received additional funding and attempted reforms after the first World Trade Center attack (1993) and the Oklahoma City bombings (1995) with very little evidence of change.[72] Transforming the FBI will also require the DNI, acting as the head of the intelligence community, and the FBI senior leadership to focus resources and sustain efforts over a long period. Sustained executive and Congressional scrutiny will also be required.

Centralized versus Decentralized Intelligence Community. Since 9/11, a singularly unique development has occurred within the intelligence community – one that is contrary to the centralized intelligence network model – namely, the development of state and local fusion centers. Christopher Hood offers an interesting viewpoint of what can be gleaned from the 9/11 attacks depending on one's perspective. A hierarchist stresses centralized control, vertical structures, detailed procedures, and the importance of extensive checks. An egalitarian seeks to change the complexity of the intelligence community by deemphasizing standard controls over information and implementing protocols that promote sharing of intelligence.[73]

While one perspective is not necessarily better or "more correct" than the other, the two perspectives represent differing views. One represents the need for better strategic direction and span of control – the hierarchical or vertical perspective. The other represents the need to rapidly share pertinent information across various organizations and domains – the egalitarian or horizontal perspective. Better strategic control, the ability to direct resources, and effecting change across the intelligence community are arguments for establishing a DNI. The 9/11 Commission's approach to resolving many of the intelligence shortcomings is based largely upon the development of these hierarchical structures.[74]

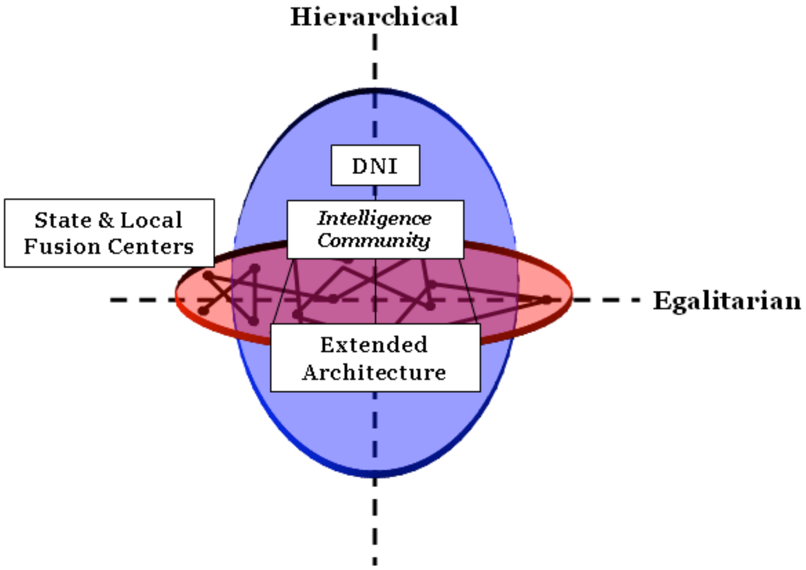

Figure 2: Hierarchical versus Egalitarian Perspectives

The growth of state and local fusion centers, however, is not a federal phenomenon or one initiated by national strategy. These centers grew in response to state and local initiatives as a result of the 9/11 attacks. Federal funding did not materialize until 2004 and FBI and DHS liaison officers did not arrive until 2006.[75] This is a stark departure from the traditional methods of dealing with intelligence matters and one that capitalizes on the changing nature of the threat – a threat that requires a combined and cooperative approach and is based on a multi-agency construct. It also capitalizes on the concept of federalism and using regional and local approaches to resolving issues. State and local fusion centers are now recognized as key elements of the homeland security enterprise.[76]

The development of these centers, however, raises other transformational challenges. The first is organizational. The philosophy behind the development of these centers lies in their ability to be networked.[77] Networking more than 17,000 law enforcement departments with individual fusion centers and then linking the fusion centers with each other and with federal agencies is a significant task.[78] Second, establishing uniform and well-understood processes is also a long-term task. This initiative will be more challenging if it lacks coordination. In large part, the federal response to integrating these fusion centers has resulted from individual agency interactions, leading to duplicative and often contradictory strategies.[79] Lastly, there is the very real risk of being unable to sustain this effort. State and local fusion centers are largely funded at the sub-federal level.[80] Additionally, federal grant funding is not a future guarantee[81] and the obligation to allocate federal funds within a short time frame with no overarching guidance results in several disconnects.[82]

Duplication of Effort vs. Alternative Analysis. There exists a natural friction between the need to eliminate excessive duplication of effort while ensuring the inclusion of alternative analysis. As Gregory Treverton states:

> Alternative analysis seeks to challenge assumptions and widen the range of possible outcomes considered. Its purpose is to hedge against "groupthink" or premature consensus, and the natural tendency for analysts, like others, [is] to search too narrowly, looking more intently for information that would confirm their prior hypotheses than data that would discredit them.[83]

Despite the mandate in the *Intelligence Reform and Terrorism Prevention Act of 2004* requiring red teaming and ensuring alternative analysis,[84] the natural friction that exists between duplication and the need for alternative analysis to challenge assumptions will continue. Merely mandating the need for alternative analysis and not addressing organizational roles and relationships will result in continued inability to reconcile duplication versus the development of alternate views.

A new dynamic is at play in the post-9/11 environment. The hierarchical model concentrated within the beltway has to interact with a new dynamic to the intelligence community – state and local fusion centers – organizationally and architecturally centered within an egalitarian framework. By virtue of their unique perspective, these fusion centers are singularly placed with regional and local knowledge.[85] The post-9/11 challenge is to incorporate this new dynamic and to reconcile these perspectives.[86] To date, the perspective of local authorities is that the exchange of ideas has been slow and often one-way, with information only flowing to federal agencies.[87]

Training. Another vital intelligence issue is the need for quality personnel. The ability to train and maintain quality intelligence professionals has been an enduring issue identified by numerous government commissions – most notably the Intelligence Survey Group in 1947. Although every generation of analysts has faced its challenges, a unique aspect of the post-9/11 environment is the necessity to sift through vast amounts of data and use varying intelligence techniques driven by a multitude of technological tools.

The need for quality analysis will continue. Driven by their own intelligence needs, state and local fusion centers are also significant competitors for quality analysis. They require strategic intelligence to develop regional threat assessments as well as event-driven tactical intelligence.[88] The analytic foundations required to drive these needs are based on two elements: explicit knowledge, which is gained via different sources and databases, versus implicit knowledge, which comes via experience and interaction.[89] The challenge to analysts in gaining explicit knowledge is duplication and the wide variety of tools and databases that exist in the post-9/11 environment. System proliferation and the variety of individual federal systems – Homeland Security Information Network (HSIN) versus others – are excessively duplicative, disjointed, and bureaucratic.[90] Developing quality intelligence personnel to build implicit knowledge also requires time and sustained focus under a sound human capital strategy.[91] Training initiatives, however, are largely a result of informal and "on-the-job" training and not the result of any defined or prioritized overarching program.[92]

Establishing a professional cadre of personnel to support the wide variety of homeland security customers and divergent intelligence disciplines – strategic, tactical, law enforcement, critical infrastructure, and others – will a require a sustained commitment.[93] Training programs will continue transforming cultural mindsets and staying ahead of the procedural changes when laws or statutes are revised.[94] The challenge in the post-9/11 environment is the limited federal direction regarding training initiatives.[95] There is also a limited availability and standardization of training programs that teach critical thinking and analytic techniques. As highlighted in the Markle Report: "The rich variety of analytic methods is seldom taught formally . . . . Capabilities analysis, Intelligence-target modeling, Pattern or trend analysis, Link analysis, Temporal analysis, Financial analysis, Poll-based analysis."[96] Lastly, homeland security consumers lack the access to the sparse training opportunities that exist.[97]

Given these limitations, the question then becomes an issue of transformation. The challenge to developing and expanding the number of quality intelligence professionals is a critical capacity building issue. Developing professionals with the right skills and in sufficient numbers to meet stated requirements is a large undertaking. The long lead-times required for developing these skills and creating an environment that encourages the analysis of opposing alternatives, divergent views, and risk taking are other critical factors.[98] Further complicating the issue are the challenges to recruiting and maintaining personnel with highly sought after skills. Of note, a recent FBI audit showed that approximately 65 percent of analysts might stay with the bureau for at least five years, but were uncertain because of concerns over insufficient retention strategies.[99]

Over-classification. Over-classification of intelligence products remains problematic. Despite attempts at reforming this process through numerous executive directives and findings, the number of classifications has doubled since September 2001.[100] Sensitive but unclassified (SBU) designations – of particular importance to homeland security – are misapplied and disjointed. A Government Accountability Office (GAO) study in 2006 found that federal agencies are using fifty-six different SBU designations – with sixteen of the designations belonging to one agency.[101]

A serious impediment to resolving this issue is the lack of an overarching government policy and procedure that delineates the purpose, designation, and use of SBU caveats.[102] Of twenty-three agencies interviewed as part of the GAO survey, eighteen did not have procedures to review how SBU designations were being used or who was making the designations.[103] Another issue lies with pseudo-classification – information that should not have been classified in the first place.[104] Lack of understanding on classifying information, who can classify or declassify, and the processes involved remain serious obstacles to sharing information. As stated by Congressman Simmons, chairman of the Subcommittee on Emergency Preparedness, Science and Technology, in a recent congressional hearing:

> Even when our fusion centers get information and our police chiefs get information, they can't pass it on to those commanders and patrol officers and detectives that need to use it because they don't have the ability, one, to declassify it; it can't be done rapidly; tear lines simply aren't working; and the system is designed to keep information secret, not to put it forward.[105]

Although not an over-classification issue, one factor that impedes information sharing and collaboration lies with the various agency security certifications and clearances. State and local consumers contend that this as a major impediment as they seek to certify their centers for handling and processing classified information.[106] Despite numerous attempts to achieve a community standard, before and after 9/11, there is still no accepted and common approach – seven years after 9/11.

Information Sharing

The inability to share information has remained an endemic issue within the intelligence community. The main reason is that the term *information sharing* carries multiple meanings depending on one's perspective. Additionally, the obstacles to sharing information have centered largely on the desire of the originating agency to control dissemination of the information they produce, processes involved in handling information, and technological systems that have been utilized in the past. Given the lack of external checks, informational monopolies can also severely limit the flow of information. NSA's mandate to "Prescribe . . . operating practices, including the transmission, handling, and distribution of SIGINT material within and among the elements under his control; and exercise the necessary monitoring and supervisory control to ensure compliance with the regulations"[107] is an excellent example of exercising end-to-end control over information. These obstacles persist today.

What is Information Sharing? Gregory Treverton notes that "while *information sharing* has become a mantra in the war on terror, existing procedures, with each intelligence agency controlling the information it produces, make it hard enough to share across U.S. intelligence, let alone get information to state and local authorities."[108] One definition for information sharing is "making information available to participants (people, processes, or systems)."[109] The *Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004* also defines the term, *terrorism information*, as:

> All information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to:
>
> - the existence, organization, capabilities, plans, intentions . . . of domestic groups or individuals involved in transnational terrorism;
> - threats posed by such groups or individuals to the United States . . .
> - groups or individuals reasonably believed to be assisting or associated with such groups or individuals.[110]

Absent in these definitions is discussion of the distinction between *information* and *data*.

Herein lies the crux of the issue: does information consist solely of finished intelligence? Does it also include the sharing of raw data? Should agencies be expected to share both finished and raw intelligence? Should producers control the totality of the information they create? The answers to these questions stem directly from the shortcomings identified by the 9/11 Commission. Intelligence agencies can choose to share finished intelligence, but if certain threat streams are found to be too sensitive, these same agencies can choose to impose further restrictive handling caveats.[111] Agencies can state *information sharing* as part of their essential mission, but only share when asked.[112] Lastly, agencies can choose to share information only when asked the right question.[113] If the right question is not asked, the information is not shared. Under each scenario, each agency is "sharing" its information.

At its most fundamental level, the intelligence fusion process exists to address gaps in knowledge by integrating disparate streams of intelligence and data, thereby leading to greater precision in targeting intelligence efforts.[114] The fusion process is also predicated on the speed and facility of access to information. The purpose of a fusion center is to "break down bureaucratic cultures that, because they resist sharing information, keep those who need to know in the dark and Americans in general vulnerable."[115] Simply put, information sharing should include the proactive sharing of both finished intelligence – the sharing of analytic conclusions – *and* raw data – the vital pieces of information used to develop link, social, temporal, and network analysis.

This is a significant and fundamental paradigm shift for the intelligence community, where control of sources, methods, and raw data translates into power. Beginning largely with the First Gulf War, and coupled with increasing sophistication on the part of the intelligence consumer, people in the post-9/11 environment have become uncomfortable with group-vetted conclusions and positions. The intelligence community has not kept pace with this dynamic and does not "produce intelligence based on how government officials and people in general really use information today."[116]

Lessons from the 9/11 attacks and the post-9/11 environment have shown that no one agency or information stream is sufficient when combating the terrorism problem.[117] An information-sharing domain that makes finished intelligence and raw data available may also be of particular benefit to state and local fusion centers due to their intimate knowledge of the local environment.[118] The danger of sharing only conclusions and not the corresponding raw data is that analysts will likely omit vital pieces of information that will end up on "the cutting room floor."[119] Additionally, sharing information in isolation with selected organizations with the "need-to-know" is not sharing information effectively. As the 9/11 Commissioners stated:

> A system that requires a demonstrated "need-to-know" before sharing assumes it is possible to know, in advance, who will need to use the information. Such a system implicitly assumes that the risk of inadvertent disclosure outweighs the benefits of wider sharing. Those Cold War assumptions are no longer appropriate.[120]

Establishing an environment where information is shared proactively will require overcoming some of the most significant cultural obstacles that reside within the intelligence community. At the very least, data owners in the post-9/11 environment need to understand that they no longer control the information they produce.[121]

Post-9/11 Information Sharing Implementation. The *Homeland Security Act of 2002* and the ITRPA established the groundwork for information sharing in the post-9/11 era.[122] The legislation called for three initiatives: the establishment of an Information Sharing Enterprise (ISE), a program manager under the DNI to spearhead the ISE, and an Information Sharing Council to facilitate stakeholder buy-in. These organizational mechanisms were tasked to resolve information sharing shortfalls.[123] Additionally, the new *National Strategy for Information Sharing* issued in 2007 established the following core principles:

- Effective information sharing comes through strong partnerships.
- Information acquired for one purpose, or under one set of authorities, might provide unique insights when combined, in accordance with applicable law, with seemingly unrelated information from other sources.
- Information sharing must be interwoven into all aspects of counterterrorism activity.

Explicitly stated in the strategy is the need and importance of including state and local fusion centers as a centerpiece of the strategy.[124]

Although there is a clear need to establish policies, governance boards, and regulations to promote efficient mechanisms as part of fundamental business practices,[125] significant implementation hurdles remain. These hurdles stem from insufficient resources and commitment. The ISE program manager testified before Congress that insufficient funding and manpower resources – eleven federal employees and six contractors –were hindering the implementation of the ISE. The program manager subsequently resigned from his position.[126] Despite new efforts on the part of the DNI to push information sharing and integration, there remain numerous questions on the varying interpretations of sharing information and the mechanisms that will be employed to facilitate the sharing of information.[127] Given the complexity and the enormity of the task, implementing information-sharing mechanisms will require the dedication of focused resources, realistic milestones, and senior-level scrutiny over a prolonged period.

System Proliferation and Duplication. There has been a significant push to share information as a result of the 9/11 attacks. The large number of agencies involved and their well-meaning attempts to pass information have inhibited sharing by creating information overload.[128] Merely implementing systems and technological solutions will not solve the variety of information-sharing shortfalls.[129] The mismatch between cleared personnel and the corresponding system architecture used to receive the information, the lack of common training, and variance among fusion centers result in further obstacles to sharing information.[130]

The DHS implementation of HSIN offers an excellent case study of the complexities involved in fielding new systems. DHS considers HSIN as the primary means to pass homeland security information. It includes thirty-five communities of interest, ranging from law enforcement to private sector domains.[131] The issue with HSIN's implementation was the preexistence of other collaborative systems, such as the Regional Information Sharing System (RISS), the Joint Regional Information Exchange System (JRIES), Law Enforcement Online (LEO), and the insufficient pre-planning that was involved in incorporating these systems.[132] The planning shortfalls stemmed largely from the time limitations involved in rushing the fielding of the system.[133]

Although DHS has developed an HSIN integration strategy that includes the use of feedback mechanisms, process teams, and a coordinating committee,[134] the addition of another system to the inventory of homeland security collaborative tools has resulted in further confusion. Some state and local agencies find other collaborative tools like RISS more flexible,[135] while others find that having to monitor multiple systems is turning into a significant resource issue.[136] Additionally, in the rush to field HSIN, insufficient training programs and user guides compounded the inefficient use of the system.[137] As of January 2008, there were reports of canceling the HSIN program altogether.[138]

The implementation of new systems as technologies become more advanced will continue to create obstacles. Providing sufficient resources to the ISE program manager, ensuring stakeholder buy-in, establishing governance boards, and implementing common data standards under a well-defined process significantly contribute to streamlining system implementation. It will also require senior-level scrutiny and focused sustainment over time.

Oversight

The FISA construct that has governed the intelligence community since 1978 has become increasingly cumbersome due to the changing nature of the threat and the rise of transnational and transborder problem sets. The 9/11 attacks provided the impetus to pass significant antiterrorism legislation – the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of* 2001 (USA PATRIOT Act) – to overcome the obstacles posed by the "wall" that inhibited coordination between law enforcement and intelligence.

There remain significant challenges in the post-9/11 era. The oversight of intelligence activities continues to be at the forefront of the political debate. As Kim Taipale states: "The policy debate . . . is not about preemption itself – even the civil libertarians concede the need to identify and stop terrorists before they act – but instead revolves around what methods are to be properly employed in this endeavor."[139] There is also rising concern about the lack of clear and concise guidelines regarding the processing and handling of personally identifiable information.[140] Overly intrusive methods and the lack of proper safeguards can quickly erode public confidence in law enforcement and intelligence efforts; perhaps more radically than any other homeland security issue.

<u>A Brave New World: Oversight Challenges in the Post-9/11 Era</u>. The telecommunications explosion in the 1990s totally transformed the way people communicate and receive information. Unlike any other time in history, the ability to communicate has become truly global. New challenges have manifested

themselves with this globalization. For example, it is becoming technically difficult to determine if calls are being initiated within the United States or whether the caller is a U.S. person.[141] Additionally, because of the U.S. telecommunications dominance, much of the world's communications traffic physically passes through the United States – both a challenge and strength. This further increases the difficulty of identifying U.S. persons,[142] while at the same time affords better surveillance access.

Central to information-sharing concepts is the idea that "one person's data is another person's information. What is vital information to one is just data to another."[143] The ability to share raw data via networks to monitor a variety of activities that support varied analytic techniques – traffic analysis, social networking, etc. – can greatly improve the understanding and interdiction of terrorist networks.[144] The development and embedding of cutting-edge anonymizing technology that protects personally identifiable information and use of audit logs can facilitate and safeguard this process.[145] The continuing lack of clear guidance, well understood protocols, and accountability, however, make the use of these techniques a high-risk proposition.[146] The controversies over NSA's post-9/11 surveillance programs and other data-mining initiatives can quickly erode any consensus that was gained after the 9/11 attacks on the necessity to gain better intelligence.[147]

Post-9/11 Oversight Risk Areas. A key and enduring challenge within the intelligence community is the necessity and importance of oversight, both executive and congressional. The 9/11 Committee identified congressional oversight reform as a key recommendation.

> Of *all* [author's emphasis] our recommendations, strengthening congressional oversight may be among the most difficult and important. So long as oversight is governed by current congressional rules and resolutions, we believe the American people will not get the security they want and need.[148]

The numerous calls for establishing a joint congressional intelligence committee with appropriate staff and accesses – prior to and after 9/11 – have not been realized or translated into an improved process. Senior decision-makers, particularly those empowered with oversight responsibilities in Congress, are critical to ensuring that intelligence reform and wider homeland security initiatives are being executed.[149] The present congressional committee construct makes this difficult. Bottom line, intelligence reform will not be realized without significant and sustained congressional oversight. It is a vital and fundamental function.[150]

Another key risk area lies with the inability to implement an effective Intelligence Sharing Enterprise (ISE). Dealing with the difficulty of articulating an effective enterprise, gaining stakeholder buy-in, and making difficult implementation decisions not only inhibit information sharing, but jeopardize the establishment of a well understood system that ensures the protection of civil liberties. Most importantly in the post-9/11 era, the ISE implementation challenges may be resulting in a loss of momentum for the overall effort.[151]

Lastly, the state and local homeland security response since 9/11 also represents a challenge. State and local fusion centers are recognized as valuable partners in homeland security and ideally should be networked into a larger framework.[152] The critical oversight issue is that most fusion centers are not operating under specific or recognized legal authorities.[153] Unclear legal guidance can bring into question many of the activities that occur in these centers.

State and local fusion centers also face other oversight challenges. Internal procedures are often informal and are not reflected in standardized processes. Additionally, most of the oversight mechanisms within the center rest solely within the executive function – without independent oversight processes.[154] The establishment of governance boards with clear mandates and processes for reviewing information will greatly improve oversight measures at state and local fusion centers.[155]

Effective oversight mechanisms are critical to implementing sound homeland security and intelligence measures. The risk to not implementing oversight procedures can lead to societal "chilling effects." Without proper safeguards and oversight, data inaccuracies, false positives, processing shortfalls, and mission creep issues will become more public and contentious.[156] Any homeland security effort, information sharing strategy, intelligence architecture, or policy that is not accompanied by effective oversight will hamper efforts to "connect the dots." Lack of bipartisan cooperation and support for oversight issues will also inhibit these efforts.[157]

CONCLUSION

When we engage in a pursuit, a clear and precise conception of what we are pursuing would seem to be the first thing we need, instead of the last we are to look forward to.

John Stuart Mill[158]

The End State for Homeland Security and Domestic Intelligence. It is easy for decision-makers and the public to lose sight of the ultimate goal, or end state, given the proliferation of new strategies, directives, and initiatives. It is also understandable for the organizations charged with implementing these initiatives to focus on shorter-term problems and lose sight of the ultimate goal.[159] A homeland security strategy that seeks to implement improved intelligence capabilities to address the domestic intelligence gap should address the circumstances and challenges – enduring intelligence issues and post-9/11 realities – while clearly articulating the envisioned end state.

As stated by Steven Biddle: "Ambiguous goals never promote strategic coherence."[160] One critique of the *National Strategy for Homeland Security* is that it contains numerous descriptions of major mission areas, outlines goals and initiatives, and includes suggested policies and objectives, yet falls short of "connecting the dots in a way that conveys a strategy."[161] In other words, the envisioned end state is not defined or well understood. Although the strategy was updated in October 2007 and identifies concerns over home-grown Islamic radicalization,[162] there is very little new language that conveys a vision. This continued ambiguity results in unclear and disjointed approaches to resolving the nation's domestic intelligence issues within the larger homeland security initiatives.

Accomplishments since 9/11. Despite this lack of clarity, decision-makers can point to an impressive list of accomplishments. The intelligence community now has an undisputed head: the DNI. The creation of DHS has consolidated multiple organizations that were only loosely connected with homeland security issues prior to 9/11. The NCTC – chartered to fuse foreign and domestic intelligence – has been institutionalized. Intelligence reform has focused on revamping the FBI, and information sharing has been enshrined as part of an independent strategy and an ISE.[163] Most importantly, the United States has not been attacked.

The absence of a successful terrorist attack, however, should not be the primary measure of success. Terrorist threats to the United States have been thwarted since 9/11. The true measure, however, of what has been accomplished since 9/11 is the degree to which progress – organizational, process development, and technological – has been made towards making the nation more secure. At the most fundamental level, have these changes afforded a better approach to identify and thwart terrorist attempts to attack the homeland, or have the attempts been thwarted in spite of any changes?

It can be argued that measuring that progress is difficult because the government's response has been disjointed and incomplete.[164] The lack of a clearly understood end state contributes further to this difficulty. All that said, progress has been made and the nation can point to some areas of success in developing a sound domestic intelligence capability while addressing some of the enduring issues that have faced the intelligence community since 1947.

First, after more than fifty years of trying, there is finally an undisputed head of the intelligence community. The intelligence community is a large and complex endeavor that requires strong leadership. The DNI is the necessary institutional mechanism to provide this leadership. The DNI's effectiveness will continue to depend on the actual span of control that he exercises, the extent to which he can direct resources, and the ability to counter organizational opposition and friction within the beltway. The DNI must also develop the following critical capabilities:

- The ability to identify and understand problems quickly while considering the long view on implementation issues. Quick fixes usually result in implementation failures.
- Improved and sustained analytic quality – an endemic intelligence issue.
- Effective information sharing.[165]

Second, intelligence needs to be reconceptualized versus reorganized.[166] The development of state and local fusion centers was not a federal phenomenon, but rather an initiative undertaken at the sub-federal level. The inability to effectively incorporate this initiative, network the capability, ensure the two-way sharing of information, and, most importantly, sustain these initiatives over time will result in reverting to business as usual – a hierarchical intelligence community typified by large bureaucracies, centered in the beltway, and cut off from its customer base. Additionally, other innovative approaches need to be incorporated. For example, the creation of the Directorate of Science & Technology within DHS envisioned capitalizing on a significant American strength – the scientific community. This organization has largely been underutilized and disconnected from wider homeland security efforts.[167]

Third, the establishment of an ISE headed by the DNI represents another unique effort. Extending the intelligence enterprise – beyond the traditional intelligence community players – based on trusted partnerships and networks can result in enormous dividends in the future. The key factors in realizing this objective are the dedication of sufficient resources, maintaining senior-level scrutiny, and sustaining the implementation effort over time.

Lastly, the passage of the USA PATRIOT Act represented a necessary legislative step to breaking down the information-sharing barriers between law enforcement and intelligence – characterized as the "wall."[168] The corresponding policy and practical guidelines for applying this legislation at the organizational level have not been developed. While changes in policy typically lag behind the implementation of technology,[169] a real danger exists of jeopardizing the use of the tools afforded by the legislation due to unclear guidance, misperceptions, and concerns over domestic surveillance. To highlight the PATRIOT Act's impact, one state agency individual stated that the legislation "had not impacted his agency's internal guidelines in any way."[170] This is unsatisfactory seven years after 9/11.

Defining the End State. Defining an end state for the conduct of domestic intelligence activities is a difficult proposition. On an organizational level, the envisioned end state must seek to address the linkages between the largely hierarchical and beltway-centric intelligence apparatus with the newer initiatives of state and local fusion centers. Simply superimposing traditional intelligence mechanisms and their extensions – Field Intelligence Groups and Joint Terrorism Task Forces – on state and local initiatives, without considering process development and technological implementation, results in falling short of the envisioned goal for homeland security. Will state and local fusion centers serve as the lead elements in the homeland security enterprise? Will domestic intelligence initiatives revert to a federal-only enterprise? These are key questions that decision-makers need to resolve. Intelligence reforms that do not look beyond the symptomatic issues and delve into the harder questions will result in disjointed approaches to domestic intelligence.[171] As James Carafano states:

> Policymakers must carefully consider a strategy before acting. Winning a long war requires a strategy to keep America safe, free, and prosperous—a "lifeline of a guiding idea" to focus effort, attention, and resources in pursuit of national objectives.[172]

The Murphy Commission (1975) offered three standards of performance for the intelligence community that remain true for the post-9/11 era. They are:

- Intelligence must respond to the evolving needs of decision-makers.
- Intelligence must function within economic constraints.
- Intelligence must operate in a way that maintains public confidence.[173]

First, the envisioned end state for domestic intelligence – and the larger community – should be one that is flexible and capable of meeting evolving needs. For the shorter term, is the community postured to meet the possible growth and radicalization of home grown cells? The attacks in Madrid (2004) and London (2005) should dispel the notion that fighting terrorists in Afghanistan and Iraq make us totally secure in the homeland.[174] For the longer term, is the community postured to meet new homeland threats? Drawing on the United Kingdom's experience, Military Intelligence Five (MI5) – their premier domestic intelligence agency – was postured historically to combat the Irish Republican Army (IRA). Was MI5 postured for, and did the organization anticipate the problems with, an increase in Islamic radicalism in the United Kingdom – a radicalization that had occurred over a period of decades? More importantly, if the threat was recognized, was there sufficient political will to meet the rising threat? Intelligence flexibility and adaptability coupled with the need for policy-level decisions and solutions must be factored into any envisioned end state.

Second, economic considerations and constraints are realities that cannot be assumed away. To reiterate the finding of the Intelligence Survey Group, a "blank check" will not suffice. Another admonition of the 9/11 Commission was the danger of pork-barrel politics and spending.[175] Lamentably, pork-barrel spending has risen significantly since 9/11. In FY1999, there were 1,000 pork-barrel projects contained in thirteen appropriations bills.[176] In FY2006, there were 9,963 pork-barrel projects contained in eleven appropriations bills totaling approximately $29 billion.[177] Although the level of pork spending lessened in FY2007, continued high levels of pork spending will limit intelligence initiatives and recapitalization efforts. Current deficit spending also leaves little flexibility to pursue ambitious initiatives across multiple fronts. As one report said regarding the state of federal budget deficits: "[B]y 2030 absent changes in the structure of Social Security and Medicare, there would be virtually no room for any other federal spending priorities, including national defense, education, and law enforcement."[178] Any ability to sustain current intelligence reforms and capabilities – capabilities and proficiencies that cannot be built overnight[179] – will be undermined by economic realities.

Lastly, public confidence must be maintained. Although effective oversight mechanisms are integral to improving public confidence, the issue is much larger. The public must be engaged to effectively prepare and respond to events. The inability to articulate an effective public engagement strategy results in the loss of confidence.[180] Implementing quick fixes in accordance with election timelines is also a disservice to the public.[181] Conversely, the inability to deal with substantive issues due to gridlock and inertia results in further loss of public confidence.[182] Garnering public support and implementing the oversight mechanisms to maintain that support and oversee intelligence efforts will result in greater social stability – the necessary ingredient for sustaining any effort over a long period.

Articulating an end state that accounts for intelligence flexibility, consideration of economic realities, and strategies that promote public confidence will contribute greatly to aligning current efforts and initiatives. It will also provide the framework for scoping the necessary transformation efforts – organizational approaches, process development, and technological implementation issues – to achieve the envisioned goal of homeland security within the larger confines of a grand strategy.

Managing Transformation. The development of national strategies and directives without articulating the practical steps necessary to fulfilling those strategies results in an increasingly disjointed approach. Under these circumstances, "the possibility of strategic failure increases as the gap between strategy and capability widens."[183] It is further compounded by the lack of a defined end state.

As identified by Deborah Barger, successful transformation has three common elements:

- A period for stakeholders to focus on the issue.
- A group of reformists that organize and manage a new idea.
- A method to evaluate change.[184]

The time to focus on developing a viable domestic intelligence capability is now. The 9/11 attacks represented a strategic event and *mandate for change*. The window of opportunity to effect meaningful change begins to close as we move away from the events of 9/11. At the strategic level, the intelligence community failed to reorganize and reengineer itself after the Cold War. This was in large part due to the inability of policy-makers to clearly articulate national security interests.[185] In the post-9/11 environment, business as usual will result in another missed opportunity.

While there are multiple stakeholders, there are three critical groups that are integral to transformation. The reformist elements in these groups need to recognize that a window of opportunity exists, but that the window is closing. The first is the DNI – the responsible party and titular head of the intelligence community. The DNI must take control of transformation. Although several obstacles continue to limit the DNI's authority, it is the organizational body within the intelligence community that must align the disparate federal elements involved in domestic intelligence under a common vision.

Second, Congress must oversee transformation efforts and change. Although the *Goldwater-Nichols Act* is viewed by some as a fluke,[186] the passage of that legislation and subsequent follow-on congressional steps to oversee change did result in transforming the military to make it a joint-capable fighting force. The strategic window of opportunity still exists for implementing further intelligence reforms. The real danger exists, however, that Congress will drift off course.[187]

The third group of stakeholders are the state and local fusion centers. These centers are closer to the constituents they serve. The development of these centers is also a unique approach to developing a domestic intelligence capability. Continued advocacy for developing this capability will be necessary to effect true reforms. The danger to this effort is the uncertainty as to whether it can be sustained.

Lastly, the method to evaluate change is contingent on the efficiency of the oversight mechanisms to oversee and manage change. Does the DNI possess the span of control and the necessary executive oversight mechanisms to manage the disparate and often competitive elements within the intelligence community? Does the DNI possess the sufficient political clout and authority to effect change?

Has Congress reformed its committee system for exercising oversight? Will state and local fusion centers operate as part of a loosely organized and haphazard approach to homeland security? The reform and effectiveness of the oversight mechanisms are directly linked to managing transformation and evaluating change.

LCDR James Burch has been in the Navy for nineteen years and is currently assigned to U.S. Northern Command. From 1998-2000, Burch was assigned to the National Security Agency and subsequently participated in Operation NOBLE EAGLE and IRAQI FREEDOM with the GEORGE WASHINGTON Battle Group. Burch is a graduate of the U.S. Merchant Marine Academy. He holds two master degrees; one in national strategic studies (homeland security) from the Naval Postgraduate School and the other in history.

[1] Steven D. Biddle, "American Grand Strategy After 9/11: An Assessment," *Strategic Studies Institute* (April 2005): 18. http://www.carlisle.army.mil/ssi.

[2] B.H. Liddell Hart, *Strategy* (New York: Frederick A. Praeger, Inc., 1968), 335-336.

[3] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton & Company, 2003), 408; U.S. Congress, House, Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001*, 107th Congress, 2nd Session, December 2002, S. Rept. No. 107-531, H. Rept. No. 107-792, 45, http://www.gpoaccess.gov/serialset/creports/pdf/fullreport_errata.pdf. Testimony provided to the Joint Inquiry revealed that the FBI had not conducted an assessment of the terrorist threat facing the United States.

[4] Office of the President, *National Strategy for Homeland Security* (Washington DC: GPO, July 2002), vii, http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

[5] U.S. Congress, Senate, *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law 108-458 (Washington DC: GPO, December 17, 2004), 3644, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ458.108.pdf. Section 101(a) established the Office of the DNI. The act also codified the NCTC; Congressional Research Service, *FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress* (Washington DC: The Library of Congress, August 4, 2004), 5-6; http://www.fas.org/irp/crs/RL32336.pdf.

[6] The development of the *National Strategy for Information Sharing* and the creation of the Information Sharing Enterprise (ISE) under the DNI emphasize this point; United States Government Accountability Office, *Homeland Security: Preliminary Information on Federal Actions to Address Challenges Faced by State and Local Fusion Centers*, GAO-07-1241T (Washington, DC: September 27, 2007), 4, http://www.gao.gov/new.items/d071241t.pdf. There are approximately fifty-eight fusion centers.

[7] James Burch, "A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and Their Implications for Homeland Security." *Homeland Security Affairs* III, no. 2 (June 2007), 1, http://www.hsaj.org/pages/volume3/issue2/pdfs/3.2.2.pdf.

[8] Williamson Murray and Allan R. Millet, eds., *Military Innovation in the Interwar Period* (Cambridge University Press, 1996), 3. Murray and Millet identify changes to organization,

doctrine (i.e. processes) and technology as the key elements to successful innovation; commonly known as "transformation" in today's vernacular.

[9] Intelligence Survey Group, *The Intelligence Problem in the United States*, Chapter I (Washington DC: National Security Council, January 1, 1949), 18; Intelligence Survey Group, *The Responsibility of the Central Intelligence Agency for the Coordination of Intelligence Activities*, Chapter IV (Washington DC: National Security Council, January 1, 1949), 41; http://foia.state.gov/documents/cia/3f33.PDF.

[10] Bruce D. Berkowitz, "Information Age Intelligence," *Foreign Policy* (Summer 1996): 41-2.

[11] Congressional Research Service, *Proposals for Intelligence Reorganization, 1949-2004*, RL32500 (Washington, DC: Library of Congress, August 4, 2004), 1, http://www.fas.org/irp/crs/RL32500.pdf.

[12] Intelligence Survey Group, *The Intelligence Problem in the United States,* Chapter IV, 41.

[13] James Schlesinger, *A Review of the Intelligence Community* (Washington DC: National Security Council, March 10, 1971), 29-31, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB144/document%204.pdf.

[14] The growth of the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the National Reconnaissance Center (NRO), the National Photo Interpretation Center (NPIC), the Defense Mapping Agency (DMA), and individual military intelligence services under the DoD to operate complex collection systems and military operations limited the DCIs' ability to manage the entire intelligence community.

[15] Congressional Research Service, *Proposals for Intelligence Reorganization, 1949-2004*, 5.

[16] Intelligence Survey Group, *The Organization and Administration of the Central Intelligence Agency*, Chapter III (Washington DC: National Security Council, January 1, 1949), 36-38, http://foia.state.gov/documents/cia/3f32.PDF.

[17] Schlesinger, *A Review of the Intelligence Community,* 22.

[18] Intelligence Survey Group, *Organization and Administration of the CIA,* Chapter IV, 54.

[19] Schlesinger, *A Review of the Intelligence Community,* 4-5.

[20] Intelligence Survey Group, *The Responsibility of the Central Intelligence Agency for National Intelligence Estimates*, Chapter V (Washington DC: National Security Council, January 1, 1949), 75, http://foia.state.gov/documents/cia/3f34.PDF.

[21] Congressional Research Service, *Proposals for Intelligence Reorganization, 1949-2004*, 11.

[22] Intelligence Survey Group, *Comments by the Central Intelligence Agency on the Conclusions and Recommendations of the Report to the National Security Council* (Washington DC: National Security Council, February 28, 1949), 15, http://foia.state.gov/documents/cia/3de0.PDF.

[23] Congressional Research Service, *Proposals for Intelligence Reorganization, 1949-2004*, 7.

[24] Schlesinger, *A Review of the Intelligence Community,* 20.

[25] Ibid., 25-27.

[26] Most notably the draft *National Intelligence Reorganization and Reform Act* (1978), Admiral Turner's intelligence proposals (1985), and the draft Boren-McCurdy legislation (1992).

[27] Intelligence Survey Group, *Comments by the Central Intelligence Agency,* 5.

[28] Congressional Research Service, *A Joint Committee on Intelligence and Alternatives: Proposals from the 9/11 Commission and Others*, RL32525 (Washington DC: Library of Congress, February 15, 2007), 1, http://www.fas.org/sgp/intel/RL32525.pdf.

[29] Ibid., 5.

[30] Congressional Research Service, *Proposals for Intelligence Reorganization, 1949-2004*, 2.

[31] Ibid., 12.

[32] E. Drexel Godfrey, Jr., "Ethics and Intelligence," in *Strategic Intelligence: Windows Into a Secret World* (Los Angeles, CA: Roxbury Publishing Company, 2004), 401-402. Godfrey offers an excellent case study on the CIA's Operation Chaos – its involvement into investigating communist influence into student groups and pressure from the Executive Branch to the CIA to "turn over every rock."

[33] Commission of the Government for the Conduct of Foreign Policy (The Murphy Commission), *The Organization of Intelligence*, Chapter VII (Washington DC: GPO, June 1975), 99, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB144/document%209.pdf. Commission on CIA Activities Within the United States (The Rockefeller Commission), *External Controls*, Chapter 7 (Washington DC: GPO, June 6, 1975), 81, http://www.history-matters.com/archive/church/rockcomm/pdf/RockComm_Chap7_External.pdf. The Rockefeller Commission also recommended a Joint Congressional Committee for Intelligence Oversight.

[34] Congressional Research Service, *Proposals for Intelligence Reorganization, 1949-2004*, 21-25.

[35] Congressional Research Service, *A Joint Committee on Intelligence and Alternatives*, 2.

[36] Robert M. Gates, *Statement by the Director of Central Intelligence on Change in the CIA and the Intelligence Community* (Washington DC: April 1, 1992), 5, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB144/document%2018.pdf

[37] Ernest R. May, "Intelligence: Backing into the Future," *Foreign Affairs* 71, no.3 (Summer 1992): 64.

[38] Ibid., 64.

[39] U.S. Senate, Senate Select Committee on Intelligence, *Explanatory Statement: Intelligence Reorganization Act of 1992* (Washington DC: 1992), 1. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB144/document%2017.pdf.

[40] May, "Intelligence," 68.

[41] David Jablonsky, Ronald Steele, Lawrence Korb, Morton H. Halperin, and Robert Ellsworth, "U.S. National Security: Beyond the Cold War," *Strategic Studies Institute* (July 26, 1997): 25, http://www.strategicstudiesinstitute.army.mil/pdffiles/pub319.pdf.

[42] Berkowitz, "Information Age Intelligence," 40.

[43] May, "Intelligence," 69.

[44] Berkowitz, "Information Age Intelligence," 42.

[45] Congressional Research Service, *Sharing Law Enforcement and Intelligence Information: The Congressional Role*, RL33873 (Washington DC: Library of Congress, February 13, 2007), 3-4, http://www.fas.org/sgp/crs/intel/RL33873.pdf.

[46] U. S. House of Representatives, Permanent Select Committee on Intelligence, *IC21: The Intelligence Community in the 21st Century*, Chapter XIII: Intelligence and Law Enforcement, 104th Congress (April 9, 1996), 2, http://www.access.gpo.gov/congress/house/intel/ic21/ic21013.html.

[47] May, "Intelligence," 71.

[48] Congressional Research Service, *Proposals for Intelligence Reorganization, 1949-2004*, 31.

[49] National Commission on Terrorism (the Bremmer Commission), *Countering the Changing Threat of International Terrorism*, 105th Congress (June 7, 2000), 15, http://www.gpo.gov/nct/nct7.pdf.

[50] Congressional Research Service, *Sharing Law Enforcement and Intelligence Information*, 10.

[51] May, "Intelligence," 71.

[52] U.S. House of Representatives, *IC21: The Intelligence Community in the 21st Century*, Chapter XV: Congressional Oversight, 104th Congress (April 9, 1996), 6, http://www.access.gpo.gov/congress/house/intel/ic21/ic21015.html.

[53] Berkowitz, "Information Age Intelligence,"46.

[54] U.S. Commission on National Security for the 21st Century (the Hart-Rudman Commission), *Roadmap for National Security: Imperative for Change*, Phase III (Washington DC: GPO, February 15, 2001), xiv-xviii, 124, http://www.fas.org/man/docs/nwc/phaseiii.pdf.

[55] Ibid., 45.

[56] *The 9/11 Commission Report*, 76.

[57] Congressional Research Service, *Intelligence Issues for Congress*, RL33539 (Washington DC: Library of Congress, October 19, 2007), 9, http://www.fas.org/sgp/crs/intel/RL33539.pdf.

[58] *The 9/11 Commission Report*, 344-346. There were several intelligence indicators revealing Al Qaeda's interest in using airliners laden with explosives as weapons of mass effects. Additionally, NORAD planners had explored the possibility of having to interdict hijacked aircraft under these particular circumstances. These indicators and planning, however, did not translate to wider processes and techniques to combat the issue.

[59] Julianne Smith and Thomas Sanderson, eds, *Five Years After 9/11: An Assessment of America's War on Terror* (Washington, DC: Center for Strategic and International Studies Press, 2006), 32.

[60] Burch, "A Domestic Intelligence Agency," 17.

[61] *The 9/11 Commission Report*, 423-424.

[62] Max Weber, *The Theory of Social and Economic Organization*, translated by A.M. Henderson and Talcott Parsons (New York: Oxford University Press, 1947), 329-332.

[63] Department of Defense, *DoD Roles and Missions in Homeland Security* (Washington DC: Defense Science Board, September 2004), 31.

[64] Eugene Bardach, "How Do They Stack Up? The 9/11 Commission Report and the Management Literature," *International Public Management Journal* 8, no.3 (2005): 356.

[65] Ibid., 352.

[66] Admittedly, there are sound reasons for safeguarding intelligence: to ensure the quality of the data, operational security, counterespionage, and the protection of sources and methods.

[67] Gregory F. Treverton, *The Next Steps in Reshaping Intelligence* (Santa Monica, CA: RAND Corporation, 2005), 9, http://www.rand.org/pubs/occasional_papers/2005/RAND_OP152.pdf.

[68] Congressional Research Service, *FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress*, RL32336 (Washington DC: Library of Congress, August 4, 2004), 5-6, http://www.fas.org/irp/crs/RL32336.pdf; Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the WMD Commission), *Report to the President of the United States* (Washington, DC: GPO, March 31, 2005), 30, http://www.wmd.gov/report/wmd_report.pdf. The report specifically called for the consolidation of the FBI's counterterrorism and counterintelligence function under the Directorate of Intelligence. It also identified several other shortfalls with the FBI's progress in transforming its organizational culture and intelligence reforms. See Chapter 10 of the report for further details.

[69] Congressional Research Service, *Intelligence Reform Implementation at the Federal Bureau of Investigation: Issues and Options for Congress*, RL33033 (Washington DC: Library of Congress, August 16, 2006), 21, http://www.fas.org/sgp/crs/intel/RL33033.pdf.

[70] National Commission on Terrorist Attacks upon the United States, "Reforming Law Enforcement, Counterterrorism, and Intelligence Collection in the United States," *9/11 Commission Staff Statement*, No. 12., 4-5, http://www.policyalmanac.org/world/archive/terrorism_reforming.pdf.

[71] Department of Justice, Office of Inspector General, *A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks* (November 2004), 353, http://www.usdoj.gov/oig/special/0506/final.pdf.

[72] Congressional Research Service, *FBI Intelligence Reform Since September 11, 2001*, 21.

[73] Christopher Hood, "Which Organization, Whose Theory? The 9/11 Commission Report and Organization Theory," *International Public Management Journal* 8, no.3 (2005): 392.

[74] Bardach, "How Do They Stack Up?" 357.

[75] Congressional Research Service, *A Summary of Fusion Centers: Core Issues and Options for Congress*, RL34177 (Washington DC: Library of Congress, September 19, 2007), 13, http://www.fas.org/sgp/crs/intel/RL34177.pdf.

[76] John Rollins and Tim Connors, *State Fusion Center Processes and Procedures: Best Practices and Recommendations* (New York: Center for Policing Terrorism, 2007), 4.

[77] Congressional Research Service, *A Summary of Fusion Centers*, 2.

[78] Rollins and Connors, *State Fusion Center Processes,* 1.

[79] Director of National Intelligence, *Information Sharing Environment Implementation Plan Security* (Washington DC: Program Manager, Information Sharing Environment, November 2006), 18.

[80] Rollins and Connors, *State Fusion Center Processes,* 7.

[81] Congressional Research Service, *A Summary of Fusion Centers*, 8.

[82] U.S. Congress, Senate, Committee on Intelligence, Intelligence Reform Hearing, *Statement of James W. Spears – West Virginia Homeland Security Advisor* (January 25, 2007), 3, http://ftp.fas.org/irp/congress/2007_hr/012507spears.pdf.

[83] Treverton, *Next Steps in Reshaping Intelligence,* 20.

[84] U.S. Congress, Senate, *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law 108-458 (Washington DC: GPO, December 17, 2004), 3671, http://travel.state.gov/pdf/irtpa2004.pdf. Section 1019 mandates the necessity of incorporating alternative analysis.

[85] K. Jack Riley, Gregory F. Treverton, Jeremy M. Wilson and Lois M. Davis, *State and Local Intelligence in the War on Terrorism* (Santa Monica, CA: RAND Corporation, 2005), ix, http://www.rand.org/pubs/monographs/2005/RAND_MG394.pdf.

[86] *The 9/11 Commission Report*, 273-276. The inability to incorporate "local" perspectives was singled out by the 9/11 Commission. Of note, see the discussion regarding the Phoenix Memo and Zacharias Moussaoui.

[87] Senate Committee on Intelligence, *Statement of James W. Spears*, 8.

[88] Ibid., 8.

[89] Tom Eucker, "Maintaining Levels of Expertise at Intel," *Knowledge Management Review* (July/August 2007): 28-30.

[90] U.S. Congress, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Statement of William Harris – Delaware Information & Analysis Center Commander* (May 10, 2007), 3; http://homeland.house.gov/SiteDocuments/20070510132259-40476.pdf.

[91] Department of Defense, *DoD Roles and Missions in Homeland Security*, 42.

[92] Treverton, *Next Steps in Reshaping Intelligence,* 22.

[93] Lee S. Strickland, "The Information Shortcomings of 9/11," *Information Management Journal* 38, no.6 (November/December 2004): 37.

[94] The Markle Foundation, *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment*, 3rd Report (July 2006), 30, http://www.markle.org/downloadable_assets/2006_nstf_report3.pdf.

[95] U.S. Congress, Senate Committee on Intelligence, *Statement of James W. Spears*, 7.

[96] The Markle Foundation, *Mobilizing Information to Prevent Terrorism*, 53-55.

[97] Riley, et al., *State and Local Intelligence,* 38.

[98] Congressional Research Service, *Intelligence Issues for Congress*, 12, http://www.fas.org/sgp/crs/intel/RL33539.pdf.

[99] U.S. Department of Justice, Office of the Inspector General, Audit Division, *Follow-Up Audit of the Federal Bureau of Investigation's Efforts to Hire, Train, and Retain Intelligence Analysts*, Audit Report 07-30 (April 2007), iii, http://www.justice.gov/oig/reports/FBI/a0730/final.pdf.

[100] Jane's Intelligence Digest, *To share or not to share, that is the problem* (London: Jane's Information Group, 2006), 3.

[101] United States Government Accountability Office, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO 06-385 (Washington, DC: March 2007), 5, http://www.gao.gov/new.items/d06385.pdf.

[102] Ibid., 5.

[103] Ibid., 26.

[104] Jane's Intelligence Digest, *To share or not to share,* 2.

[105] U.S. Congress, House Select Committee on Homeland Security, *State and Local Fusion Centers and the Role of DHS* (Washington DC: GPO, September 7, 2006), 13, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_house_hearings&docid=f:35568.pdf.

[106] Ibid., 18.

[107] Department of Defense Directive, *The National Security Agency and the Central Security Service*, S-5100.2023 (Washington DC: Department of Defense, December 1971), 5, http://www.fas.org/irp/doddir/dod/d5100_20.pdf.

[108] Treverton, *The Next Steps in Reshaping Intelligence*, 27.

[109] Department of Defense, Office of the Chief Information Officer, *Department of Defense Information Sharing Strategy* (Washington DC: Department of Defense, May 4, 2007), 3, http://www.defenselink.mil/cio-nii/docs/InfoSharingStrategy.pdf.

[110] *Intelligence Reform and Terrorism Prevention Act of 2004.* See Section 1016(a).

[111] *The 9/11 Commission Report*, 80.

[112] Ibid., 353.

[113] Department of Defense, *DoD Roles and Missions in Homeland Security*, 19.

[114] Congressional Research Service, *A Summary of Fusion Centers: Core Issues and Options for Congress*, RL34177 (Washington DC: Library of Congress, September 19, 2007), 5, http://www.fas.org/sgp/crs/intel/RL34177.pdf.

[115] Dana R. Dillon, "Breaking Down Intelligence Barriers for Homeland Security," *The Heritage Foundation: Backgrounder* 1536 (April 15, 2002): 3, http://www.heritage.org/Research/HomelandSecurity/BG1536.cfm.

[116] Berkowitz, "Information Age Intelligence," 42.

[117] Office of the President, *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (Washington DC: GPO, 2007), 2, http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf.

[118] The Markle Foundation, *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment*, 3rd Report (July 2006), 49, http://www.markle.org/downloadable_assets/2006_nstf_report3.pdf.

[119] Department of Defense, *DoD Roles and Missions in Homeland Security*, 13.

[120] *The 9/11 Commission Report*, 417.

[121] The Markle Foundation, *Mobilizing Information*, 5.

[122] U.S. Congress, Senate, *Homeland Security Act of 2002*, Public Law 107-296 (Washington DC: GPO, November 25, 2002), 2252, http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf, Section 891; *Intelligence Reform and Terrorism Prevention Act of 2004*, Section 1016.

[123] *Intelligence Reform and Terrorism Prevention Act of 2004*, Section 1016.

[124] Office of the President, *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*, 2-3.

[125] United States Government Accountability Office, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO 06-385 (Washington, DC: GPO, March 2007), 12, http://www.gao.gov/new.items/d06385.pdf; Department of Defense, *Department of Defense Information Sharing Strategy*, 11.

[126] Government Accountability Office, *Information Sharing: The Federal Government Needs to Establish Policies and Processes*, 19.

[127] Congressional Research Service, *A Summary of Fusion Centers: Core Issues and Options for Congress*, RL34177 (Washington DC: Library of Congress, September 19, 2007), 18-19, http://www.fas.org/sgp/crs/intel/RL34177.pdf.

[128] Riley, et al., *State and Local Intelligence,* 46.

[129] Department of Defense, *Department of Defense Information Sharing Strategy*, 13.

130 Congressional Research Service, *A Summary of Fusion Centers: Core Issues and Options for Congress*, 12, 18.

[131] United States Government Accountability Office, *Homeland Security Information Network needs to Be Better Coordinated with Key State and Local Initiatives*, GAO 07-822T (Washington, DC: GPO. May 10, 2007), 5, http://www.gao.gov/new.items/d07822t.pdf.

[132] Department of Homeland Security, Office of the Inspector General, *Homeland Security Information Network Could Support Information Sharing More Effectively*, OIG 06-38 (Washington DC: GPO, June 2006), 11-12, http://www.fas.org/irp/agency/dhs/hsin0606.pdf.

[133] Ibid., 3.

[134] Government Accountability Office, *Homeland Security Information Network needs to Be Better Coordinated with Key State and Local Initiatives*, 13.

[135] U.S. Congress, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Statement of William Harris – Delaware Information & Analysis Center Commander* (May 10, 2007), 3, http://homeland.house.gov/SiteDocuments/20070510132259-40476.pdf.

[136] U.S. Congress, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Statement of Lee Miller – Virginia State Police* (May 10, 2007), 2, http://homeland.house.gov/SiteDocuments/20070510132259-40476.pdf.

[137] Department of Homeland Security, *Homeland Security Information Network Could Support Information Sharing More Effectively*, 18.

[138] Spencer S. Hsu and Robert O'Harrow, Jr, "DHS to Replace 'Duplicative' Anti-Terrorism Data Network: $90 Mission System Aimed to Aid State, Local Agencies," *Washington Post*, January 18, 2008, A03.

[139] Kim Taipale, "Rethinking Foreign Intelligence Surveillance," *World Policy Journal* (Winter 2006/2007): 78.

[140] The Markle Foundation, *Mobilizing Information to Prevent Terrorism*, 7.

[141] Taipale, "Rethinking Foreign Intelligence Surveillance," 79.

[142] The Markle Foundation, *Mobilizing Information to Prevent Terrorism*, 33.

[143] Department of Defense, *DoD Roles and Missions in Homeland Security* (Washington DC: Defense Science Board, September 2004), 9.

[144] Taipale, "Rethinking Foreign Intelligence Surveillance," 79-80.

[145] Shawn Harris, "How They Connect the Dots," *Government Executive* (September 1, 2007), 40.

[146] The Markle Foundation, *Mobilizing Information to Prevent Terrorism*, 33.

[147] Congressional Research Service, *Sharing Law Enforcement and Intelligence Information*, 14.

[148] *The 9/11 Commission Report*, 419.

[149] Julianne Smith and Thomas Sanderson, eds, *Five Years After 9/11: An Assessment of America's War on Terror* (Washington, DC: Center for Strategic and International Studies Press, 2006), 46.

[150] CSIS, "Guiding Principles for Intelligence Reform," 3.

[151] The Markle Foundation, *Mobilizing Information to Prevent Terrorism*, 17.

[152] Office of the President, *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*, 2-3.

[153] Congressional Research Service, *A Summary of Fusion Centers*, 9.

[154] Riley, et al., *State and Local Intelligence,* 33-34.

[155] Congressional Research Service, *A Summary of Fusion Centers*, 6.

[156] Frans A.J. Birrer, "Data mining to combat terrorism and the roots of privacy concerns," *Ethics and Information Technology* 7 (2005): 216.

[157] Congressional Research Service, *Sharing Law Enforcement and Intelligence Information*, 15.

[158] John Stuart Mill, *The Basic Writings of John Stuart Mill: On Liberty, The Subjection of Women & Utilitarianism* (New York: The Modern Library, 2002), 234.

[159] Joan Magretta and Nan Stone, *What Management Is: How It Works and Why It's Everyone's Business* (New York: The Free Press, 2002), 23.

[160] Biddle, "American Grand Strategy After 9/11," 28.

[161] Michael B. Donley, "Reading Strategy Between the Lines," *Journal of Homeland Security* (August 2002): 1-2; http://www.homelandsecurity.org/newjournal/Commentary/displayCommentary2.asp?commentary=18.

[162] Homeland Security Council, *National Strategy for Homeland Security* (Washington DC: GPO, October 2007), 22.

[163] Office of the President, *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information* Sharing, 7.

[164] Smith and Sanderson, *Five Years After 9/11*, 16.

[165] CSIS, "Guiding Principals for Intelligence Reform," 2.

[166] Deborah G. Barger, "It Is Time to Transform, Not Reform, U.S. Intelligence," *SIAS Review* 24, no.1 (Winter 2004): 24.

[167] Smith and Sanderson, *Five Years After 9/11,* 19.

[168] U.S. Congress, Senate, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (USA PATRIOT Act), Public Law 107-56 (Washington DC: GPO, October 26, 2001), 278, http://fl1.findlaw.com/news.findlaw.com/cnn/docs/terrorism/hr3162.pdf. See Section 203.

[169] Barger, "It Is Time to Transform," 29.

[170] Riley, et al., *State and Local Intelligence,* 33.

[171] Ibid., 23.

[172] James Jay Carafano, "Six Years After 9/11: Are We Safe Yet?" *The Heritage Foundation: Backgrounder* 1609 (September 11, 2007):1 http://www.heritage.org/Research/HomelandDefense/upload/wm_1609.pdf.

[173] The Murphy Commission, *The Organization of Intelligence,* 91.

[174] Smith and Sanderson, *Five Years After 9/11*, 2.

[175] *The 9/11 Commission Report*, 396.

[176] Ronald D. Utt, "How Congressional Earmarks and Pork-Barrel Spending Undermine State and Local Decisionmaking," *The Heritage Foundation: Backgrounder* 1266 (June 2, 1999): 1, http://www.heritage.org/ Research/Budget/upload/18432_1.pdf.

[177] Citizens Against Government Waste (CAGW), *2006 Congressional Pig Book Summary* (Washington DC: CAGW, 2006), 1, http://www.cagw.org/site/DocServer/2006PigBookSummary.pdf?docID=1541

[178] GAO, *Homeland Security: Challenges and Strategies in Addressing Short and Long-Term National Needs*, 11.

[179] Barger, "It Is Time to Transform,"27.

[180] Smith and Sanderson, *Five Years After 9/11*, 21.

[181] CSIS, "Guiding Principals for Intelligence Reform," 1.

[182] Carafano, "Six Years After 9/11: Are We Safe Yet?"3.

[183] Smith and Sanderson, *Five Years After 9/11*, 43.

[184] Barger, “It Is Time to Transform,”29.

[185] Mark W. Lowenthal, *Intelligence: From Secrets to Policy*, 3rd ed (Washington, DC: CQ Press, 2006), 232.

[186] Bardach, “How Do They Stack Up?” 353.

[187] Carafano, “Six Years After 9/11: Are We Safe Yet?”1.