NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE LONG AND WINDING ROAD:
POST-9/11 INTELLIGENCE REFORMS
A DECADE LATER

by

David R. Johanson II

March 2013

Thesis Advisor: Robert Simeral
Co-Advisor: Erik Dahl

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 2013	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE THE LONG AND WINDING ROAD: POST-9/11 INTELLIGENCE REFORMS A DECADE LATER	5. FUNDING NUMBERS
6. AUTHOR(S) David R. Johanson II	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The establishment of the Department of Homeland Security (DHS) and passage of the Intelligence Reform and Terrorism Prevention Act (IRTPA) shortly after the terrorist attacks of September 11, 2001, collectively constitute the most significant bureaucratic shakeup of the national security apparatus since the National Security Act of 1947. Roughly 10 years following the creation of DHS, questions linger as to whether these reforms have addressed the major domestic intelligence shortfalls identified in numerous post-9/11 congressional hearings and in the final report of the 9/11 Commission.

This thesis seeks to answer those questions by examining the performance of the U.S. domestic intelligence system since 9/11 along three fronts: intelligence fusion, institutional evolution, and intelligence prioritization. Citing the literature from current and former homeland security practitioners, academic experts, non-partisan analysts, and print media commentators, this paper concludes that while key measures of progress on these fronts have been observed, shortfalls within the domestic intelligence system do nevertheless remain, requiring further oversight and guidance from federal homeland security policymakers.

14. SUBJECT TERMS Department of Homeland Security, Office of Intelligence and Analysis, Intelligence Reform and Terrorism Prevention Act, Director of National Intelligence, National Counterterrorism Center, Intelligence Reform, Domestic Intelligence, Fusion Centers	15. NUMBER OF PAGES 79
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE LONG AND WINDING ROAD: POST-9/11 INTELLIGENCE REFORMS A DECADE LATER

David R. Johanson II
Lieutenant, United States Navy
B.A., University of California, Berkeley, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2013

Author: David R. Johanson II

Approved by: Robert Simeral
Thesis Advisor

Erik Dahl
Thesis Co-Advisor

Harold Trinkunas
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The establishment of the Department of Homeland Security (DHS) and passage of the Intelligence Reform and Terrorism Prevention Act (IRTPA) shortly after the terrorist attacks of September 11, 2001, collectively constitute the most significant bureaucratic shakeup of the national security apparatus since the National Security Act of 1947. Roughly 10 years following the creation of DHS, questions linger as to whether these reforms have addressed the major domestic intelligence shortfalls identified in numerous post-9/11 congressional hearings and in the final report of the 9/11 Commission.

This thesis seeks to answer those questions by examining the performance of the U.S. domestic intelligence system since 9/11 along three fronts: intelligence fusion, institutional evolution, and intelligence prioritization. Citing the literature from current and former homeland security practitioners, academic experts, non-partisan analysts, and print media commentators, this paper concludes that while key measures of progress on these fronts have been observed, shortfalls within the domestic intelligence system do nevertheless remain, requiring further oversight and guidance from federal homeland security policymakers.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION: EXAMINING WHERE U.S. DOMESTIC INTELLIGENCE HAS BEEN IN ORDER TO KNOW WHERE IT IS GOING 1
- A. QUESTIONS TO CONSIDER 2
- B. A FRAMEWORK FOR EXAMINING AREAS OF CONTINUING CHALLENGE IN DOMESTIC INTELLIGENCE 3
- C. METHODOLOGY 5
- D. ORGANIZATION 6

II. DHS, THE IC, AND FUSION: ONGOING CHALLENGES TO INTELLIGENCE INTEGRATION 7
- A. THE CHALLENGES OF BEING ALL THINGS TO ALL PEOPLE 8
- B. PROVIDING VALUE-ADDED TO THE INTELLIGENCE CUSTOMER 10
- C. THE SEARCH FOR EFFECTIVE MEANS OF DISSEMINATING AND COORDINATING INTELLIGENCE 12
- D. THE YOUTH MOVEMENT AND ITS IMPACT ON ANALYSIS 16
- E. CONCLUSION 18

III. INSTITUTIONAL EVOLUTION IN THE DOMESTIC INTELLIGENCE SPHERE: A SLOW AND HALTING AFFAIR 21
- A. SEARCHING FOR CLEARER DIRECTION AND ACCOUNTABILITY WITHIN DHS 22
- B. CONTINUING ISSUES OF FRAGMENTATION WITHIN THE BROADER IC 28
- C. CONCLUSION 33

IV. JACK OF ALL TRADES, MASTER OF NONE?: CHALLENGES IN DOMESTIC INTELLIGENCE PRIORITIZATION 37
- A. THE INTELLIGENCE PRIORITIZATION PROBLEM DEFINED 37
- B. DRAWBACKS OF THE ALL-HAZARDS APPROACH 38
- C. OVEREMPHASIS ON COLLECTION AT THE EXPENSE OF ANALYSIS 40
- D. LACK OF EFFECTIVE TOOLS FOR MEASURING SUCCESS OF TARGETED INTELLIGENCE DISTRIBUTION 44
- E. REDUNDANCIES, AMBIGUITIES, AND LOST ACCOUNTABILITY RESULTING FROM OVERLAPPING MISSIONS 46
- F. CONCLUSION 49

V. THE WORK HAS JUST BEGUN: CONSIDERING ALTERNATIVES FOR IMPROVING DOMESTIC INTELLIGENCE 51
- A. CONSOLIDATION 52
- B. SPECIALIZATION 53

C. THE FOREIGN-DOMESTIC INTELLIGENCE DIVIDE 55
D. ACTING LIKE THE ADVERSARY IN ORDER TO DEFEAT IT 56
E. SHOULD THE IC BE EXPANDED? 58
F. CONCLUSION 58

LIST OF REFERENCES 61

INITIAL DISTRIBUTION LIST 65

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
CBP	U.S. Customs and Border Protection
CBRN	Chemical, Biological, Radiological, & Nuclear
CIA	Central Intelligence Agency
CRS	Congressional Research Service
DHS	Department of Homeland Security
DHSI	DHS Intelligence Enterprise
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
FBI	Federal Bureau of Investigation
GAO	Government Accountability Office
HPSCI	House Permanent Select Committee on Intelligence
HSIN-CS	Homeland Security Information Sharing Network Critical Sectors Portal
HUMINT	Human Intelligence
I&A	DHS Office of Intelligence and Analysis
IC	Intelligence Community
ICE	U.S. Immigration and Customs Enforcement
IG	Inspector General
IO	DHS Intelligence Officer
IRTPA	Intelligence Reform and Terrorism Prevention Act
NCRIC	Northern California Regional Intelligence Center
NCTC	National Counterterrorism Center
SIN	Standing Information Need
TSA	Transportation Security Administration
USCIS	U.S. Citizenship and Immigration Services
WMD	Weapons of Mass Destruction

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

To Andria, a truly creative mind, treasured lifelong companion, and incredible mother, whose sacrifices as a military spouse have allowed our family to flourish and me to work in a gratifying career field. I am indebted to you for your constant love and support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION: EXAMINING WHERE U.S. DOMESTIC INTELLIGENCE HAS BEEN IN ORDER TO KNOW WHERE IT IS GOING

With the establishment of the Department of Homeland Security (DHS) in 2003 and the creation of a Director of National Intelligence (DNI) post and National Counterterrorism Center (NCTC) under the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), the national security apparatus underwent its largest reorganization since the National Security Act of 1947. Considering the significant amounts of federal budget money, congressional staff time, and executive policy planning that have gone into how best to secure the homeland after the 9/11 attacks, an analysis of how effective the U.S. government's efforts have been over the last decade is warranted. Furthermore, it is critical to examine whether the new intelligence construct has successfully addressed the primary challenges brought to light by the 9/11 Commission and others. Such an examination becomes particularly important in periods of fiscal challenge, such as the one this country is about to embark on in the face of ballooning federal deficits and slow economic growth.

Unless the American voting public is convinced that intelligence reforms have addressed the key challenges that were identified in the wake of the 9/11 attacks, it will be increasingly difficult to justify continued large appropriations to DHS and the U.S. Intelligence Community (IC). And even if budgets for DHS remain stable, it will always be in the taxpayers' interest to allocate money intelligently to the numerous and disparate functions within DHS. If, as many argue, the IC still faces systemic problems collecting, analyzing, and sharing the right kind of intelligence for the post-9/11 age, then it would be unwise to put good money after bad and continue with a system that produces uncertain returns on the public dollar. For this reason, a comprehensive analysis of the continuing challenges and shortcomings of the DHS Intelligence enterprise (DHSI) and the broader U.S. IC can be helpful in isolating those areas requiring greater congressional and executive attention going forward, which is what this paper will attempt to accomplish.

A. QUESTIONS TO CONSIDER

The key questions at hand concern expectations vs. outcomes: 1) From the vantage of a decade after the creation of DHS, what does the evidence suggest about how closely the department today resembles the vision Congress had when it created the department a decade ago? 2) Likewise, in the context of the IC as a whole, to what extent have the evolution of the office of the DNI and the functioning of NCTC met the expectations laid out in the 9/11 Commission Report and the IRTPA for a more streamlined, less stove-piped IC? 3) If any of these post-9/11 domestic intelligence reforms have exhibited shortcomings, where are they most noticeable, and what can be done to address them?

In a number of key respects, the path from enactment of legislation to implementation of effective intelligence reforms has been a rocky one, both for DHS and, to a slightly lesser extent, the broader IC. One of the challenges in proving this is the near impossibility of determining national security returns on the billions of dollars that have been spent on DHS and the IC over the last decade. One compelling argument that DHS and the IC have done an effective job since 9/11 is the simple fact that there have been no repeats of 9/11. But this assessment ignores the near-misses of December 2009 (the thwarted "underwear bombing" of a Detroit-bound airplane) and May 2010 (failed car bombing of Times Square).

These close calls are symptomatic of a structural deficiency in DHS and the IC that still leaves doubt about who is ultimately accountable for domestic intelligence performance in this country and how effectively the vast quantities of collected intelligence can be fused. The implementation of reforms at DHS has been a particularly slow and difficult process to get to the ultimate realization of a DHSI that is fully integrated with its numerous customers, including Congress, other members of the IC, other cabinet-level departments, the military, private business, and most importantly, state and local authorities at the fusion center level. Similarly, at the DNI level, there persists a sense that the office's portfolio is too large and expansive for one individual to coordinate all the diverse array of activities that the IC undertakes on a daily basis.

B. A FRAMEWORK FOR EXAMINING AREAS OF CONTINUING CHALLENGE IN DOMESTIC INTELLIGENCE

The scholarly debate on this topic can be broken down into essentially three camps: 1) In the first camp, a fairly vocal collection of scholars and commentators sees the evolution of DHSI and the IC following the landmark reforms of roughly a decade ago as significantly lacking, having accomplished very little in the way of addressing key intelligence deficiencies that were identified in the wake of 9/11. 2) In a second camp, a slightly smaller but very dedicated group of primarily former civil servants makes the argument that DHSI and the IC have gone a long way toward remedying the glaring post-9/11 problems in the community by enhancing information flows and providing a more extensive overarching structure to deal with the asymmetric threat. 3) In a third camp, a number of objective governmental and non-partisan reports, as well as Congressional testimony from members of the domestic intelligence establishment, suggests that despite progress in key areas, problems do remain. This third body of work serves as a sort of tie-breaker, shifting the balance of the arguments to the side of the skeptics of intelligence reform and painting a picture of a national intelligence system that is still largely in flux.

Amy Zegart stands as one of the most vocal critics of the IC's performance both before and after 9/11 and her observations provide a helpful baseline against which to measure the IC's progress in fixing the systemic problems that plagued it leading up to the 9/11 attacks. A good place to start when analyzing DHSI and the IC as a whole is to examine those areas that Zegart says were most lacking in the run-up to 9/11: 1) the IC's "lack of coherence or 'corporateness,'" 2) insufficient "attention to setting intelligence priorities," 3) the "need to revitalize human intelligence capabilities," and 4) "personnel and information sharing issues."[1]

Interestingly, in testimony before the House Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security on May 12, 2010, Caryn Wagner, then Under Secretary of Homeland Security

[1] Amy B. Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton: Princeton University Press, 2007), 35–38.

for Intelligence and Analysis (I&A), pointed out three of the primary areas she was focused on at the time, which all appear to overlap the areas of concern highlighted by Zegart. The areas Wagner mentioned included the need to enhance information sharing by focusing on fusion centers, the need to tailor DHS's intelligence products to the needs of its customers, and the need to manage the personnel system in a way that would professionalize DHS.[2]

That the areas highlighted by Wagner hold much in common with those areas identified by Zegart bolsters the broader argument Zegart and others have made that what concerned us about the IC immediately after 9/11 should still concern us today. The isolation of three common areas of concern—what, for the purposes of this thesis, will be termed intelligence fusion, institutional evolution, and intelligence prioritization—will form the basis of the following chapters' examination of the continuing challenges experienced by DHSI and the broader IC since the post-9/11 intelligence reforms were enacted by Congress.

Since the overarching goal of this thesis will be to examine how well DHSI and its peers within the IC are performing in light of the significant reforms of a decade ago, it makes sense to organize the thesis along functional lines. Consolidating the observations of Zegart and Under Secretary Wagner on the areas of greatest concern for DHSI and the IC as a whole, three primary functional intelligence areas emerge as the guideposts by which DHSI and the IC's performance since 9/11 will be measured: 1) intelligence fusion, which will be defined as the extent to which the domestic intelligence system is capable of integrating the flows of information on numerous levels (federal, state, local, etc.) in an effort to provide refined end-user intelligence for senior policymakers; 2) institutional evolution, defined as the degree to which new and evolving agencies within the domestic intelligence system are effective not only in leveraging their personnel in the efficient use of available manpower, but also in working with other agencies to achieve tangible homeland security successes; and 3) intelligence

[2] *A DHS Intelligence Enterprise: Still Just a Vision or Reality? Hearing Before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security*, 111th Cong. (May 12, 2010), 10.

prioritization, defined as the ability of domestic intelligence analysts at the micro-level and domestic intelligence bureaucracies at the macro-level to effectively hone in on information most relevant to the homeland security mission in a way that produces maximum results with minimally duplicative effort.

C. METHODOLOGY

The following chapters will consist of a primarily historiographic approach to the problem of evaluating the performance of the U.S. domestic intelligence system since the attacks of 9/11, which is to say primary and secondary source material will be marshaled as evidence in the construction of a narrative about the last ten years of intelligence reforms. Such an approach has its benefits as well as its limitations. On the one hand, contemporary experts and practitioners speak in their own words about their view of the effectiveness or ineffectiveness of the domestic intelligence system through such source material as congressional testimony, RAND analyses, Government Accountability Office (GAO) findings, inspector general (IG) investigations, Congressional Research Service (CRS) reports, and scholarly research. On the other hand, the use of historiography as a driving methodology admittedly lacks the hard quantifications inherent in a more social science-oriented approach, meaning that this thesis makes no pretense of constructing its argument with the help of organically produced hard data to back up its claims.

Rather, this thesis seeks to harness the words and research done by others more prominent in the field in order to tell a story about the direction of intelligence reform in this country. Nevertheless, the material drawn upon in the following chapters does manage to provide empirical evidence of its own: For example, only nine of 50 state fusion centers establishing Standing Information Needs (SINs) after several years of effort, a 55 percent contractor workforce at DHS years after its establishment, and 72 percent of aviation stakeholders having not heard of DHS' primary intelligence dissemination portal for threats to transportation infrastructure, to name just a few examples. (Each of these examples and more will be discussed in further depth and contextualized in the following chapters.)

D. ORGANIZATION

This thesis consists of a total of five chapters, with introductory and concluding chapters and one chapter focusing on each of the three functional areas described above. In addition to the three chapters examining DHSI and the IC's performance in these core functional areas since the major post-9/11 intelligence reforms, the concluding chapter will briefly explore alternatives for consideration as policymakers wrestle with how best to continue to improve the return on taxpayers' homeland security dollars.

II. DHS, THE IC, AND FUSION: ONGOING CHALLENGES TO INTELLIGENCE INTEGRATION

The failure to fuse the information available to numerous agencies in the lead-up to the 9/11 attacks constitutes one of the most significant recent failures of the domestic intelligence system. Excerpts from the 9/11 Commission Report detail concrete instances in which the FBI and CIA had relevant information about the 9/11 plotters that—if properly integrated—might have led to effective action by intelligence and law enforcement authorities to interrupt the plot before its culmination. A closer examination of the state of play today, 11 years after the 9/11 attacks, reveals an intelligence apparatus still seeking answers to that elusive fusion challenge. Significant challenges remain despite the monumental time, money, and effort that have been put toward enhancing the fusion of information into usable intelligence.

This chapter will examine four areas that stand out as presenting particularly vexing problems for DHS and the IC as a whole in their efforts to foster more effective intelligence fusion today: 1) the scale and diversity of the customer-base requiring intelligence support; 2) the occasional failure of intelligence components, particularly within DHS, to provide a distinct value-added to the information they distribute to their customers; 3) the lack of comprehensive, well-publicized databases for customers to reference for integrated threat data; and 4) the peculiar irony within the IC that along with the surge in hiring of young analysts who are particularly adept at networking, collaborating, and sharing information comes a workforce that lacks the depth of experience to fuse the vast amounts of data being collected as effectively as their more knowledgeable, and retiring, veteran colleagues.

While none of these challenges are insurmountable, they do represent significant roadblocks to the IC achieving the level of seamlessness and efficiency that the authors of the DHS and IRTPA legislation envisioned. And with constant reminders by commentators, experts, and policymakers alike that the next devastating attack could come at any moment, these kinds of delays in the IC's ability to crack the fusion problem do matter. Solving the critical problem of learning how to better fuse information into

actionable intelligence in an age when data fly across the fibers at accelerating rates is in DHS and the IC's interest and deserves continued focused attention if another catastrophic attack on the scale of 9/11 is to be avoided.

A. THE CHALLENGES OF BEING ALL THINGS TO ALL PEOPLE

Any cursory look at the DHS Intelligence enterprise's numerous masters reveals the picture of a daunting set of customers with an incredibly diverse set of intelligence needs. Under Secretary Wagner put it best in testimony before Congress shortly after assuming her role as the Chief Intelligence Officer within DHS: "After three months on the job, I can say I have never been in an organization that has the broad range of customers and requirements that I&A does. We are responsible for supporting the Secretary and senior Departmental leadership, the diverse set of DHS operational components, the state, local, tribal, territorial, and private sector partners, other federal partners, and also the intelligence community."[3] In a prepared statement that accompanied this testimony, Wagner also highlighted the diverse array of analytical efforts undertaken by the DHS Intelligence enterprise, including threat analysis and warning in the fields of counter-terrorism, infrastructure protection, border and immigration security, cyber security, health intelligence, and chemical, biological, radiological, and nuclear (CBRN) developments.[4]

In light of this combination of such a disparate group of intelligence customers with such a wide-ranging set of intelligence focus areas, it is fair to ask whether genuine fusion can exist in such a context. According to a DHS IG report examining efforts within the department to coordinate on information sharing issues with state and local fusion centers, "The term 'fusion' refers to the overarching process of managing the flow of information and intelligence across all levels and sectors of government and private industry, and through analysis, provides meaningful intelligence."[5] Given this definition,

---

[3] Ibid., 8.

[4] Ibid., 12.

[5] U.S. Department of Homeland Security, Office of the Inspector General, *DHS' Efforts To Coordinate and Enhance Its Support and Information Sharing With Fusion Centers*, OIG-12-10, November 2011, 2.

the primary challenge confronting DHS in particular is that the customer-base and mission set were so big to begin with and have only grown larger, to the point where effective fusion in certain areas has become an ideal that may not be realistically attainable. For example, DHS recently made a push to become the primary agency in the evolving cyber security mission. But given the fact that the department continues to wrestle with meeting its core competencies in the terrorism and critical infrastructure domains, does it make sense for the Executive to invest such faith in a nascent DHS to effectively fuse the complex information on cyber threats, especially when military agencies like the National Security Agency appear to have a firmer grasp of this rapidly evolving field?

Charles Allen, the former Under Secretary of Homeland Security for I&A and a highly respected intelligence practitioner in Washington circles, holds a view of the DHS Intelligence enterprise as essentially an enormous vacuum of information generated by the myriad daily interactions conducted under DHS auspices every day. In a speech to the Washington Institute for Near East Policy in 2008, Allen made a compelling case for the growing importance of DHS in the conduct of homeland security intelligence functions:

> Intelligence is not only about spies and satellites. It is about the thousands and thousands of routine, everyday observations and activities. Surveillance, interactions—each of which may be taken in isolation as not a particularly meaningful piece of information—but when fused together, gives us a sense of the patterns and the flow that really is at the core of what intelligence analysis is all about. What you may not know is that we, at DHS, actually generate a great deal of intelligence. We are virtually an "information factory" producing data based on thousands of interactions every hour at the border, in airports, and with the US Coast Guard.[6]

People like Allen deserve an immense amount of credit for being at the forefront of DHS's transition from a bureaucratic newcomer to a player on the IC stage. The job of the early DHS leadership in this regard has been far from easy. But for such a veteran

[6] Charles Allen, "Terrorism in the Twenty-First Century: Implications for Homeland Security," remarks to the Washington Institute for Near East Policy, May 6, 2008, http://www.washingtoninstitute.org/policy-analysis/view/terrorism-in-the-twenty-first-century-implications-for-homeland-security.

intelligence operative, Allen makes a key mistake by interchangeably using the words "information" and "intelligence" when describing DHS's unique niche.

Contrary to his intent, Allen's description of what DHS does with the vast amounts of data it collects serves to muddy the waters in the perception of how I&A and other members of the DHS Intelligence enterprise are able to effectively fuse this data into polished intelligence. Allen paints a picture of DHS as being very good at collection—sucking up the vast and disparate array of information out there on everything from border crossing interactions to airport screenings to Coast Guard boardings of merchant vessels. But it is one thing to collect and store this kind of data, while it is another thing entirely to apply the rigorous analysis necessary to convert this data into something that can be regarded as genuine intelligence. This is where the DHS Intelligence enterprise has failed thus far and still has a long way to go. The essential fusion required to turn information into intelligence is still not present at a scale sufficient to the task—in other words, DHS's analytical and fusion capabilities have not caught up with its collection capability. This is a problem and has implications not only for DHS's effectiveness in preventing another catastrophic terrorist attack, but also for its perception by the public as an entity that threatens privacy and civil liberties with all this data that is collected, sometimes to no apparent use.

B. PROVIDING VALUE-ADDED TO THE INTELLIGENCE CUSTOMER

A noticeable lack of value-added inevitably stems from an insufficiently developed fusion capability, and this has been shown to often be the case in DHS interactions with its customers in the federal, state, tribal, local, and private domains. In some cases, DHS Intelligence components have failed not only in terms of the relevance of the information they have distributed to their customers, but also in terms of the perennial push-pull conundrum, in which agencies with pertinent information often fail to push that information to those who may need it, instead waiting for the pull from the customer, who often does not know the information is there to be had in the first place. Todd Masse, in his 2006 CRS study of homeland security intelligence, illustrates this point well:

> Numerous fusion center officials claim that although their center receives a substantial amount of information from federal agencies, they never seem to get the "right information" or receive it in an efficient manner. According to many state fusion center leaders, often-pertinent threat intelligence must be requested by fusion centers, rather than federal agencies being proactive in providing it. The obvious difficulty arises regarding the inability to request relevant threat information that is unknown to members of the fusion center.[7]

While this area has received a significant amount of attention from I&A's leadership since 2006 and improvements on the federal-state collaboration front have been made, Masse's observation continues to find a degree of resonance to this day. In some cases, interactions between DHS Intelligence enterprise components and their public and private customers are still characterized by a confused dissemination scheme and an occasional lack of value-added in the information that is disseminated. Transportation Security Administration (TSA) interactions with its intelligence customer base in the transportation sector provide a primary case in point.

In a November 2011 survey of stakeholders in the aviation, rail, and highway sectors, the Government Accountability Office (GAO) sought to determine the extent to which customers were happy with the intelligence support received from TSA on emerging threats to the transportation sector and the ease with which that information could be retrieved. While the survey found a general level of satisfaction with the support received, some noticeable observations about the "actionability" of the information received and challenges associated with finding that information were revealed. In a telling passage, the GAO authors pinpoint a key concern of some of the stakeholders who opted to provide additional comments in their survey responses:

> Open-ended comments collected in our survey from 18 of the 275 stakeholders provided additional context about actionability. For example, 6 aviation stakeholders reported that informational reports, specifically the TSIRs [Transportation Suspicious Incidents Reports]—which TSA phased out and replaced with the more regionally focused GRID [Global and Regional Intelligence Digest] in August 2011—would be more

[7] U.S. Library of Congress, Congressional Research Service, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, by Todd Masse, CRS Report RL33616 (Washington, DC: Office of Congressional Information and Publishing, August 18, 2006), 28.

> beneficial if they provided actionable information or additional guidance that would allow the stakeholders to adjust security measures or take other necessary actions to improve their security postures, and also identify ongoing trends to various sectors. One passenger air carrier official commented that these reports are ambiguous—often leaving him wondering what information may affect his airline and what changes should or could be made to directly counter specific threats.[8]

TSA's shortcomings in its effort to disseminate threat information to the operators of transportation networks gets to the heart of the challenges associated with fusion. As these stakeholders clearly demonstrate in their comments, effective fusion would provide the distinct value-added that would allow them to do their jobs better and more easily comprehend their operating environment. But in too many cases, not only in the TSA context but in other sectors and levels of government as well, DHS has been prone to disseminating raw information with the expectation that this alone with "scratch the itch" of its customers, so to speak. Plainly speaking, this falls short of fusion. To merely make information available to a customer base does not satisfy the intent of the legislation that created DHS in the first place. Intelligence professionals get paid to provide their spin on the tangle of often indecipherable information floating around out there, and when they fail to do that, to fuse the information into actionable intelligence, they fail to do their job.

C. THE SEARCH FOR EFFECTIVE MEANS OF DISSEMINATING AND COORDINATING INTELLIGENCE

Of course, even after tackling the problem of fusing information into finished intelligence, there remains the challenge of getting that intelligence to those who are best placed to use it in a timely and efficient manner. This represents another challenge that DHS and the broader IC continue to wrestle with long after the fevered pitch of reform that ensued immediately after 9/11. An analysis of information sharing reveals that even with a change of culture taking root, the technical mechanisms for implementing a more information sharing-friendly environment continue to confound those with the best of intentions on this front.

---

[8] U.S. Government Accountability Office, *Transportation Security Information Sharing: Stakeholders Generally Satisfied but TSA Could Improve Analysis, Awareness, and Accountability* (November 2011), 15.

Staying with the TSA example just discussed, a secondary problem identified in the GAO survey has to do with the fact that many of TSA's customers in the transportation industry did not necessarily know where to look to find threat intelligence. As the GAO authors point out, the Homeland Security Information Sharing Network Critical Sectors portal (HSIN-CS) was to be the main means of disseminating intelligence such as TSA's threat reporting, with DHS regarding HSIN-CS as "the primary information-sharing mechanism for critical infrastructure sectors, including the transportation sector," allowing for "information sharing and collaboration between the federal, state, local, and private sectors engaged in the homeland security mission."[9] Yet, as the report also notes, "almost 60 percent (158 of 266) of transportation stakeholders we surveyed had never heard of HSIN-CS," with the surprising revelation that within the aviation sector alone, "72 percent of aviation stakeholders (124 of 173) responding to the survey had not heard of HSIN-CS and 9 percent (15 of 173) were unsure, and several commented that they would be interested in accessing the system."[10] On the issue of dissemination, the report logically concludes, "Because many transportation stakeholders have not heard of HSIN-CS, do not access the system, or encounter difficulties once they log in, they may not be receiving timely information via the information-sharing mechanism that DHS has established."[11]

DHS does not face these issues of intelligence dissemination and coordination alone. The issue of how to integrate myriad information systems and databases continues to plague the IC as a whole, even though passage of the IRTPA ostensibly augured a new era of intelligence collaboration devoid of stove-pipes. While the work of previous Directors of National Intelligence (DNI) like Dennis Blair and others has gone a long way toward changing the culture within the IC toward one more amenable to information sharing, the technical challenge involved in getting databases to talk to one another is quite complex.

---

[9] Ibid., 23–24.

[10] Ibid., 24–25.

[11] Ibid., 32.

Perhaps nowhere has this challenge been more evident than at NCTC, which has grown by reputation to be regarded as the primary nerve center for counterterrorism-related intelligence. As such, NCTC must be capable of synthesizing vast amounts of data from agencies such as the Federal Bureau of Investigation (FBI) and Central Intelligence Agency (CIA), not to mention all of the subcomponents within the federal, state, and local apparatus that have a counterterrorism focus. An article in the *Los Angeles Times* in 2010 indicated that several years after NCTC's inception as part of the IRTPA legislation, officials continued to struggle to patch together the complex mosaic of information that is constantly being collected:

> There are no easy legislative or technical fixes, said Russell E. Travers, information sharing chief at the National Counterterrorism Center. The agency is pursuing solutions that will allow automated connection of related information across databases, but "my guess is that this will be a challenge into perpetuity, because we get more and more information every day," he said. One intelligence agency alone gets 8,000 terrorism messages each day with 11,000 to 15,000 names, he said.[12]

This gets to the issue of what Under Secretary Wagner refers to as the "signal to noise" problem and the challenges it poses to the fusion of information into user-friendly intelligence. As she noted to members of Congress, "I think the chief obstacle to horizontal integration tends to be, in the intelligence community side at least, what we call sort of signal to noise, which is not so much connecting the dots, but the fact that there is so much fragmentary information that it is very difficult to know at the time, until something happens to give you sort of hindsight, which of those pieces of information are significant enough to follow up on."[13]

Like NCTC, DHS's I&A must try to find ways to incorporate all of the diverse data collected in its wide net that Charlie Allen likened to a veritable DHS "information factory." Without such capabilities, fusion does not happen and that data just sits there. That kind of arrangement may be closer to the norm for law enforcement authorities who

---

[12] Ken Dilanian, "U.S. Counter-Terrorism Agents Still Hamstrung by Data-Sharing Failures," *Los Angeles Times*, October 4, 2010, http://articles.latimes.com/2010/oct/04/nation/la-naw-terrorism-data-100510.

[13] *DHS Intelligence Enterprise*, 21.

can methodically sift through that information in an attempt to build a case, but for practitioners of homeland security intelligence, it has to have predictive quality in order to be relevant. An article posted on the Homeland Security News Wire in late 2011 discussed an initiative that DHS is pursuing in an effort to find that common solution to its unwieldy data problem. Since the current system restricts data to "individual systems within various DHS components which were created to fulfill specific mission requirements," officials have turned to the concept of "an integrated database known as the 'Federated Information Sharing System'" with the goal of improving information sharing within the department.[14]

While this could potentially go some distance toward managing the unruly treasure trove of data DHS collects each and every day and perhaps aid in the effort to more effectively fuse that data, the department runs up against another concern that has dogged it since the creation of a Department of Homeland Security was merely being discussed in the wake of 9/11: the protection of civil liberties. Disregarding the enormous technical complexities involved in the creation of such an integrated database, the civil liberties issues are as relevant today as they were ten years ago. As the article further points out:

> The ACLU also asked Secretary Napolitano what measures would be taken to restrict information on innocent people. DHS currently collects a vast amount of data, including benefit information from the Federal Emergency Management Agency (FEMA), traveler information from CBP and TSA, naturalization records from USCIS, and personal information like social security number, date of birth, and email address from a wide variety of sources.[15]

Complementing the more basic question of whether DHS is *capable* of fusing the vast array of data it collects is the equally important ethical question of whether it *should* fuse that data. Regardless of technological developments in the future that may make it increasingly easy for the DHS Intelligence enterprise to do its job of all-source fusion in

---

[14] "Concern over DHS move to create giant information databank," Homeland Security News Wire, December 8, 2011, http://www.homelandsecuritynewswire.com/dr20111208-concern-over-dhs-move-to-create-giant-information-databank.

[15] Ibid.

defense of the homeland, this key question on intrusion of civil liberties will complicate the department's efforts for the foreseeable future.

D. THE YOUTH MOVEMENT AND ITS IMPACT ON ANALYSIS

After taking into account challenges associated with satisfying a vast and diverse intelligence customer base, targeting the right information to the right people at the right time, and collaborating and integrating information in a way that incorporates small bits of data into a more digestible big picture, the remaining hurdle in the effort to achieve a more comprehensive fusion comes in the form of the analytical effort that gets applied at the end of the chain. Similar to the discussion above regarding DHS's occasional failings to provide value-added in the intelligence it disseminates to its customers, issues of analytical effort center on the ability of intelligence components throughout the IC to identify the key patterns and anomalies in information that are going to help their policymaking masters make difficult decisions. In this area, too—particularly at the national, IC-wide level—effective fusion of information into end-user intelligence suffers some key challenges, one of which is the significant level of hiring that took place in the post-9/11 intelligence surge, leading to a significantly younger workforce of intelligence analysts throughout the IC today.

Without question, the status quo leading up to the 9/11 attacks failed. Analysts who had been working for 20 and 30 years in the IC studying threats emanating from the Soviet sphere were in many cases ill-equipped to shift their focus to the rapidly evolving threat from violent Islamic extremists. And perhaps the most pernicious legacy of the Cold War years in the IC was the tendency for agencies and their analysts to guard their own turf, fearful of the loss of information that was deemed proprietary to a degree. Senior intelligence leadership at the highest levels seems to have gotten the message loud and clear from the 9/11 Commission and others that the old practice of stonewalling on vital issues of intelligence collaboration is intolerable in the face of an agile terrorist threat.

To this end, former DNI Blair and other leaders within the community have successfully pushed initiatives that have helped replace the entrenched culture of secrecy

with one of openness and dialogue not only between intelligence agencies, but between individual analysts as well. As Blair himself pointed out in a *Washington Post* op-ed, "Thousands of analysts form groups spontaneously, in real time, on A-Space, post insights in Intellipedia, retrieve relevant analyses from the Library of National Intelligence and interact with the tribal database for Afghanistan. These tools, among others, ensure that each piece of analysis takes advantage of work being done and that new insights are immediately available to those who need them."[16] This cultural shift within the IC should not be underestimated and represents a significant improvement on pre-9/11 practices.

But greater sharing and collaboration alone will not achieve greater fusion per se, and the change in age demographics of the intelligence workforce over the last ten years has introduced a new challenge to effective fusion, notwithstanding the strides made in virtual integration through the use of such tools as A-Space, Intellipedia, and the like. Robert Cardillo puts the importance of this more recent youth movement in perspective:

> Our workforce is forcing us to change. Almost a quarter of the DIA Directorate for Analysis workforce is 30 years old or younger. Whether we believe in generalizations about the generations or not, we have to acknowledge that those who have grown up with the Internet are used to having information available at their fingertips, collaborating online, and networking as a way of life. We baby boomers in leadership have been able to keep up with them, though barely, with technology that leverages these strengths.[17]

Cardillo, the Deputy Director of National Intelligence for Intelligence Integration, is quite high on this change in the workforce. Embracing the fact that the "newest generation of analysts brought on during this last decade knows no other way" than to integrate in an intensely collaborative environment, he argues that the DNI is leading a cultural change within the broader IC.[18]

---

[16] Dennis C. Blair, "Strengthening Our Front Line of Defense," *Washington Post Op-Ed*, December 18, 2009, http://articles.washingtonpost.com/2009-12-18/news/36806239_1_intelligence-reform-intelligence-agencies-national-intelligence.

[17] Robert Cardillo, "Intelligence Community Reform: A Cultural Evolution," *Studies in Intelligence* 54 (2010): 4.

[18] Ibid., 7.

While IC-wide collaboration is the wave of the future and veteran analysts and leaders need to accept rather than resist this inevitability, the craft of intelligence analysis—whereby an oftentimes overwhelming amount of data is fused together into a more comprehensible understanding of a given problem—necessitates that greater collaboration alone cannot be an end in itself. In an age of smart phones and Wi-Fi-connected tablets that give the user instant access to a large volume of information anytime, an individual's ability to effectively process all of that information has only become more challenging. The fact that today's consumer typically enjoys greater access to raw information than ever before does not automatically equate to the ability to make sense of it, and in this sense, the IC might be heading down a similar path to society at large. Despite IC leadership pushing buzzwords like "integration" and "collaboration," the art of intelligence fusion runs the risk of getting lost in the shuffle. While many veteran analysts were caught off-guard by the developments of 9/11, their skill-sets should still be valued. Learning how to fuse information and turn it into useful intelligence for policymakers often requires a significant amount of time simply sitting in an analyst's chair and being exposed daily to the ebbs and flows of international affairs and large volumes of intelligence reporting. While the younger generation of analysts undeniably possesses the collaborative tools and mindsets to push fusion forward in many key respects, those analysts still have a significant amount of on-the-job learning to do to become expert at the process of comprehensive fusion. That simply takes time and exposure to long-running global trends and no amount of technological prowess can make up for that fundamental fact.

E. CONCLUSION

Fusion constitutes the vital final step in the process of converting mere information into predictive intelligence that can effectively inform important matters of policymaking. Despite the four primary challenges to fusion detailed above, the DHS Intelligence enterprise and the Intelligence Community as a whole have made strides in addressing deep-seated shortcomings that were identified in the immediate aftermath of 9/11. The culture among many intelligence agencies has changed to one of more interconnectedness and an open exchange of information, and DHS has grown and

adapted since its inception to place a greater focus on supporting its myriad customers through the freer, yet more targeted, dissemination of intelligence.

However, there lingers an overarching sense that the DHS and IC architecture that has developed over the last decade still suffers from a large degree of fragmentation. DHS has taken measures to address numerous shortcomings raised by congressional subcommittees and GAO reports, but to a certain degree, the enormity of the task facing the good people working in the various DHS intelligence components just does not lend itself to an easy solution to the problem of effective intelligence fusion. Likewise in the IC, a cultural shift is indeed occurring, but the vastness of the data to be collected and processed in an effort to never be caught off-guard again by a major terrorist attack is a daunting task that will only be made more difficult as the IC develops the means to collect yet more data.

Simply put, fusion at the highest levels of the national intelligence apparatus down to the beat cop on the street continues to be a work in progress. Part of the answer is that agencies with a stake in the homeland security mission need to continually refine their processes and procedures in order to get more adept at a counterterrorism mission that is still relatively new. But part of the answer is also the requirement for more time for this vast new homeland security infrastructure to take root and form into a more seamless machine. The key question obviously is whether the nation has time for this inevitable evolutionary process to play out. With the exception of near-misses on a Detroit-bound airliner and at Times Square, the record is fairly strong thus far. But time will tell whether DHS and the IC can meet the challenges facing them before the threat catches up, potentially forcing a serious reconsideration of how the country's leaders have chosen to tackle these very complex problems of bureaucratic reform.

This leads to consideration of the critical question of institutional evolution, which serves as the subject of the next chapter. Ironically, in a race against time and the possibility of a dramatic follow-on attack by asymmetric forces who hope to do the United States homeland harm, history demonstrates that the kind of large-scale bureaucratic change initiated by the establishment of DHS and passage of the IRTPA does take significant time to come to fruition. While there has been no lack of personal

effort by leaders and rank-and-file members of the IC alike to effect positive change, some signs point to the institutional evolution taking place within DHS and the IC as on more of marathon trajectory, rather than taking the form of a sprint, despite the urgency of the homeland security challenges faced.

III. INSTITUTIONAL EVOLUTION IN THE DOMESTIC INTELLIGENCE SPHERE: A SLOW AND HALTING AFFAIR

While the process of conceiving a new intelligence structure within the United States and then passing the related legislation to establish that structure occurred in a relatively condensed timeframe following the 9/11 attacks, the process of executing the mandates set forth in the legislation has been a work in progress for a solid decade. It was one thing for representatives, senators, and White House aides to negotiate a statutory solution to the country's apparent intelligence shortcomings; it has proven to be quite another task to effectively carry out the domestic counterterrorism intelligence reforms envisioned in the legislation creating DHS, as well as those reforms initiated by the IRTPA, which set out to usher in a new era of more clearly defined authority and responsibility vested in the DNI.

As Amy Zegart points out, numerous commissions established prior to the 9/11 attacks to examine structural challenges facing the IC in the post-Cold War world found consensus around a core of issues, one of which was the obvious lack of "corporateness" within the IC.[19] The disjointedness stemming from this lack of "corporateness" appears to have been a major contributor to the intelligence failures surrounding the 9/11 attacks. In an ideal world, the creation of DHS, with its homeland security intelligence component, in addition to the establishment of NCTC and the post of DNI under the IRTPA, would directly address this major deficiency.

However, as numerous GAO reports, IG investigations, and exchanges before congressional subcommittees demonstrate, the road to achieving a more comprehensive level of accountability and integration among the agencies within both DHS and the broader IC has been a long and challenging one. Much effort has been expended, and in numerous instances tangible progress made, but the evidence suggests that DHS and the IC find themselves in more of a marathon of bureaucratic evolution than a sprint to quick-fixes of long-standing intelligence challenges. This chapter will examine in more depth the institutional evolutionary challenges faced by DHS and the IC. The first half of the chapter will focus specifically on

[19] Zegart, *Spying Blind*, 35.

DHS issues, followed by a broader examination of the IC's challenges in this area, and concluding with an analysis of what the current state of evolutionary change is within the domestic intelligence system as a whole.

A. SEARCHING FOR CLEARER DIRECTION AND ACCOUNTABILITY WITHIN DHS

In his opening statement at a hearing before the Subcommittee on Terrorism, HUMINT, Analysis, and Counterintelligence of the House Permanent Select Committee on Intelligence, the Ranking Member, Representative Mike Thompson, commented that "DHS' place in the U.S. intelligence architecture has been a topic of congressional oversight since its creation and remains a work in progress without final resolution."[20] The phrase "work in progress" probably best describes the status of organizational evolution within DHS. Conceptually, a strong, independent DHS intelligence element acting as a vital conduit between federal, state, and local intelligence and law enforcement entities makes a lot of intuitive sense. The real challenges, of course, have come in the execution of this vision over the last decade.

A key word that surfaces again and again in the literature on DHS's integration efforts is "accountability." How to foster accountability within an organization that is the newest bureaucratic player in the high-tempo, high-stakes world of homeland security counterterrorism? One of the primary forces hampering accountability within DHS is the sheer complexity of the bureaucratic evolution that occurred in the first place. As the authors of the National Security Preparedness Group's *Tenth Anniversary Report Card* point out:

> Over the past 10 years, our government's response to the challenge of transnational terrorism has been dramatic. At the federal level, we have created major new institutions. The Department of Homeland Security itself was a massive reconfiguration of government, combining 22 agencies into a new department, with a workforce of 230,000 people and an annual budget of more than $50 billion. In total, some 263 organizations have been established or redesigned.[21]

---

[20] *The Role of DHS in the IC: A Report by the Aspen Institute. Hearing Before the Subcommittee on Terrorism, HUMINT, Analysis, and Counterintelligence of the House Permanent Select Committee on Intelligence*, 112th Cong. (January 18, 2012), 1.

[21] National Security Preparedness Group, *Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations* (Washington, DC: Bipartisan Policy Center, September 2011), 6.

In an important respect, the concentration of a disparate collection of mission-sets under the DHS umbrella achieved what some critics advocated for in the weeks and months following the 9/11 attacks: a full-fledged effort to wrangle together diverse elements within the domestic security sphere in an attempt to compel them to work as one.

But as Charles Perrow observes, this kind of concentration of such a wide array of focus areas ran the risk of muddling the picture, which served as a significant bureaucratic challenge for DHS's early leadership from the start: "The new department merged agencies that, along with their security roles, had responsibilities for such activities unrelated to terrorism as fisheries, river floods, animal diseases, energy reliability, computer crime, citizenship training, tariffs on imports, drug smuggling, and the reliability of telephone networks. The potpourri of unrelated activities was to exceed that of any previous large government mergers."[22]

While this was certainly not a fatal flaw, it has had implications that reverberate to this day, which is where the accountability issue comes into play. One of the consequences of such an abrupt consolidation of previously-unrelated functions under a new cabinet-level department has been the uneven pace of bureaucratic evolution across DHS's 22 component agencies. Within DHS' wide-ranging family of agencies exists a more staid organization like the Coast Guard, whose long tradition and solid establishment within the federal bureaucracy stands in stark contrast to the newly-established TSA, which in terms of institutional evolution is still in the process of establishing its Beltway credentials, not to mention its basic business practices and links with other federal agencies, both inside and outside of DHS.

As one of six intelligence elements within the DHS Intelligence enterprise, TSA carries with it an important responsibility to remain integrated and relevant in DHS's efforts to build a streamlined and effective network of cross-communicating organizations. But as a GAO report recently revealed, TSA may be holding itself back from reaching its full organizational potential by failing to lay out its intelligence

[22] Charles Perrow, "The Disaster after 9/11: The Department of Homeland Security and the Intelligence Reorganization," *Homeland Security Affairs* II (2006): 12.

responsibilities more clearly. As the report notes, "Because TSA has not clearly defined and documented roles and responsibilities for disseminating security-related information and the full range of its information-sharing efforts, TSA may not be consistently providing security-related information products to external stakeholders and divisions within TSA may not be held fully accountable for performing their information-sharing activities."[23] For a DHS subcomponent like TSA which is not formally part of the IC—in addition to its fellow subcomponents, including CBP, ICE, and the Secret Service—this definition of roles and responsibilities is vitally important to avoid misperceptions by outside agencies about just what DHS intelligence elements can and cannot do.

The challenge of creating greater accountability in a bureaucracy such as DHS that is new and sprawling is not limited strictly to TSA. Another GAO report focusing on the relationship between DHS's I&A and state fusion centers recommends, "Defining and documenting the specific programs and activities I&A's components and divisions will be held responsible for implementing so that I&A collectively can meet its state and local mission could help to establish clear direction and accountability."[24] Again, the accountability piece of the equation seems to suffer most when there is bureaucratic ambiguity over who is responsible for what. What these reports and others find is that in many cases DHS and its components have been slow to define more clearly roles and responsibilities within their organizations, often leading to continued bureaucratic confusion nearly a decade after the department's establishment. These kinds of challenges were understandable in the first few years following the transition, but they are becoming less and less acceptable. The outlining of roles and responsibilities in the service of creating a culture of accountability constitutes one of the fundamental tasks confronting an organization searching for its identity. DHS' progress in this regard has been notably slow.

---

[23] GAO, *Transportation Security Information Sharing*, 36.

[24] U.S. Government Accountability Office, *Information Sharing: DHS Could Better Define How It Plans to Meet Its State and Local Mission and Improve Performance Accountability* (December 2010), 33.

As other evidence indicates, the general slowness with which DHS components have identified specific roles and responsibilities has had an adverse impact on organizations outside of DHS's immediate sphere of influence. A recent DHS IG report noted the continuing uncertainty on the part of state fusion centers with regard to what exactly DHS's components can bring to the table by observing, "SLPO [State and Local Program Office] is also soliciting comments from fusion centers regarding which DHS components and federal departments and agencies they would find most useful in their centers. However, many fusion centers do not have a clear understanding of DHS components' capabilities, missions, and information collection areas."[25] The report goes on to say, "Although DHS components are aware that cooperation with and support of fusion centers is a departmental priority, none of the component field staff we spoke with recalled seeing formal written instructions or guidelines for supporting fusion centers from their headquarters management."[26]

DHS' I&A could help clarify areas where significant ambiguity over component capabilities and missions still exists, but even in those circumstances where DHS is providing adequate resources to the fusion centers, confusion at the state level can add to the problem as well. Take, for example, the DHS Intelligence Officers (IO) who are assigned by DHS headquarters to the numerous fusion center locales. In this regard, DHS has arguably done a satisfactory job of providing state fusion center leaders with a single point of contact with whom they can consult on issues relating to DHS-fusion center coordination. What some of the literature points out, however, is that failure to properly define roles and responsibilities at the state level can have a detrimental effect on operations as well.

The same DHS IG report, while identifying actions DHS headquarters can take to clear the muddy waters on this subject, also sees problems caused by the divergent ways fusion center leaders envision use of the IO position:

---

[25] DHS IG, *DHS' Efforts*, 27.

[26] Ibid., 29.

> At some fusion centers, IO roles and responsibilities are unclear, causing misunderstandings among both DHS and fusion center staff. For example, some fusion center directors believed that IOs would train analysts or write analytical products, while other directors anticipated that their IOs would have expertise in specific topics of interest to the state, such as maritime or border issues. Defining roles and responsibilities would make relationships among IOs, components, and fusion center staff more productive and improve information sharing.[27]

The primary risk being run here is that when areas of gray exist concerning which organization has responsibility for this or that part of the homeland security mission, ultimate accountability will be lost in the confusion. This state of affairs then has the potential to bring the nation's homeland security apparatus back to square one, to a pre-9/11 environment where many people from many different organizations were working diligently on the counterterrorism/homeland security problem set, yet no clear seams demarcated where one agency's responsibilities dropped off and another's began.

It would be hyperbole to state that shortcomings in domestic intelligence reform since 9/11 have brought the IC essentially back to where it started; that is not the intent of this thesis. In fact, the creation of DHS, along with its continually developing intelligence capabilities, has established cross-links between federal, state, and local agencies that were nearly non-existent in some respects prior to the 9/11 attacks. If nothing else, the introduction of DHS on the scene has motivated people in the community to talk to one another, with an awareness that resources exist at the national level for state and local authorities to draw upon. This has been an important development over the last decade and will continue to mature and develop as time goes on.

But it is prudent to ask where the seams still are not clear and where more can be done to further reduce ambiguity within the homeland security intelligence infrastructure. One way to identify which practices are having the intended effect and which are falling short would be a more rigorous implementation of performance measures. But as the GAO has observed, some of the ambiguity that characterizes roles and relationships

[27] Ibid., 35.

within DHS and the state fusion centers also affects the way homeland security components grade themselves on how they're doing, which has an adverse impact on fostering greater accountability:

> We also have recognized and reported that it is difficult to develop performance measures that show how certain information-sharing efforts have affected homeland security. Nevertheless, we have recommended that agencies take steps towards establishing such measures to hold them accountable for the investments they make. We also recognize that agencies may need to evolve from relatively easier process measures that, for example, count the number of products provided to more meaningful measures that weigh customer satisfaction with the timeliness, usefulness, and accuracy of the information provided, until the agencies can establish outcome measures that determine what difference the information made to state or local homeland security efforts.[28]

As suggested above, it is not enough to simply quantify how much production DHS components are generating. Especially in the field of intelligence, this kind of quantification is near meaningless. Rather, DHS and its components will need to continue to develop their performance measures over time, so that their intelligence collection and analysis can become that much more focused. These are understandable challenges for a fledgling bureaucracy with such a disparate mission set, but dealing with them properly and expeditiously is essential if DHS is going to create the kind of intelligence accountability the 9/11 Commission saw so clearly lacking in its analysis of pre-9/11 events.

One final obstacle to DHS creating the kind of culture of accountability it seeks stems from the somewhat transient nature of its workforce over the first decade of its existence. As a congressional hearing in May 2010 revealed, DHS leadership has struggled to establish a workforce with the requisite degree of stability and permanence one might expect in a department so vital to national security. Speaking on behalf of the Chairman of the Committee on Homeland Security, Representative Jane Harman, Chair of the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, directed an important personnel question to Bart Johnson, principal deputy

[28] GAO, *Information Sharing*, 32.

under secretary of Homeland Security for I&A: "The second question that the chairman would have asked is about the use of outside federal contractors. I remember being appalled to learn that the ratio was 60/40, outside to inside, or maybe even worse. Mr. Johnson, you pledged eight months ago to help fix that. I think the goal was to get to 40/60, which is still not terrific. Where are we?"[29]

Under Secretary for I&A Caryn Wagner's response is instructive in illustrating the myriad challenges DHS leadership has had to confront while building the foundations of a competent domestic intelligence capability. Citing problems with obtaining Office of Personnel Management hiring authorities and the persistence of "too many vacant billets," Wagner conceded that reduction of the contractor ranks within the DHS Intelligence enterprise was a slow process, resulting in a relatively small reduction from 60 percent to 55 percent of the total workforce.[30] In a line of work where analyzing threats to the homeland over a long period of time in order to identify big picture trends and subtle anomalies is of enormous importance, the presence of such a substantial contractor force counteracts that institutional drive toward stability and permanence that is so crucial in DHS's early evolution. It may seem like a relatively minor detail, but a workforce that is in flux and experiences the kind of turnover typical of temporary contract positions makes the issue of generating a viable culture of accountability all the more difficult. DHS leadership has enough challenges in getting peer agencies and state and local component agencies to collaborate; the last thing they need is an ongoing struggle over the stability of their own personnel.

B. CONTINUING ISSUES OF FRAGMENTATION WITHIN THE BROADER IC

Just as DHS continues to suffer from ambiguities in roles and responsibilities, the IC suffers from a degree of fragmentation of its own that can lead to competition, multiplicity of effort, and ambiguous authority at the national level, as well. Integrating the disparate capabilities of the IC in the service of greater homeland security has proven

[29] U.S. House, *DHS Intelligence Enterprise*, 28.

[30] Ibid., 28-29.

to be a nuanced undertaking with a political element that has made breaking with historic norms of doing business particularly difficult. What has resulted in some areas looks like an incoherent whole, much as Amy Zegart discusses in a pre-9/11 context in *Spying Blind*. While progress has been made in certain key respects, longstanding issues of uncertainty over who is ultimately in charge at the national level remain.

Perhaps nowhere is this more evident than in the analytical realm. As numerous observers point out, even today the IC appears to lack a comprehensive unity of effort in terms of counterterrorism/homeland security intelligence production. Conducting a study for RAND and DHS in which he interviewed current and former homeland security experts concerning the structure of domestic intelligence in the United States, Gregory Treverton noted the common view among participants that domestic intelligence analysis is "fragmented and sometimes conflicting," adding:

> At the federal level, individuals we spoke with during this study captured many of these concerns by posing the seemingly simple question—"Where is the center of analytical capability for domestic counterterrorism intelligence efforts supposed to be in the federal government?" NCTC is the central node for terrorism analysis at the federal level, but the main customer for its analytical efforts was characterized as "up"—the President—rather than "down"—the rest of the organizations involved in homeland security.[31]

As Treverton points out, even in the case of NCTC, which many have seen as a big success since its creation under the IRTPA, uncertainty remains regarding what should be considered the proper center of gravity in the analytical effort. If NCTC is serving the President well at the expense of greater local knowledge of the threat picture, the domestic intelligence architecture will still be prone to deficiencies. The soon-to-be-defunct Interagency Threat Assessment Coordination Group (ITACG) was established to address this up-only orientation of NCTC by acting partly as an expeditor for state and local agencies to receive counterterrorism intelligence from NCTC, but there remains a continuing feeling by some that the world of counterterrorism intelligence is still

[31] Gregory F. Treverton, *Reorganizing U.S. Domestic Intelligence: Assessing the Options* (Santa Monica: RAND, 2008), 27, 32–33.

somewhat top-heavy and skewed more toward the decision makers in Washington at the expense of local authorities' situational awareness.

Treverton invokes a sports analogy from one of his study participants that resonates in other literature on the subject to make a broader point about the structural ambiguity that still remains at the national level:

> Some expert panel participants (and interviewees as well) were particularly critical of the complex structure of the current domestic intelligence enterprise, even at the federal level, let alone reaching out to the states and localities. One asserted that it has "no structure" and creates significant confusion for the domestic counterterrorism intelligence mission. Another described domestic intelligence as "a pickup ballgame without a real structure, leadership, management, or output."[32]

Part of the problem could stem from the fact that the general response by the federal government to the intelligence shortcomings evident in the successful 9/11 attacks was equal parts reorganization and resource augmentation. This is an interesting feature of post-9/11 intelligence reform at the national level because what the 9/11 Commission Report seemed to be saying is that venerated organizations like the FBI and CIA were on the right path leading up to the attacks, but their way of doing business was antiquated and more suited to a territorial Cold War mentality. There did not appear to be a significant outcry for more resources per se, but the outcome seen in the immediate years following the 9/11 attacks was one of significantly more analysts devoted to the effort with the resulting increase in bureaucratic overhead and greater confusion over lines of authority.

Robert Cardillo extends the sports analogy theme in his discussion of the historically competitive nature of the IC and the necessity for different elements of the community to focus on their core competencies rather than compete with one another for resources and visibility:

> We still work in a free-for-all environment: agencies are writing on what they want to write. We are still competing against one another on many issues, the proverbial kids' soccer game. While competitive analysis is good to some degree, we cannot afford to compete in everything. With

[32] Ibid., 25-26.

> ever-expanding requirements and likely declining resources, we need to think now about how to task-organize ourselves better.[33]

Cardillo and Treverton's comparison of the U.S. domestic intelligence effort to a disorganized, jumbled ball game has some merit, primarily in terms of how it conveys a fundamental lack of stewardship by a central figure or body. It helps the reader visualize the irony within domestic intelligence circles whereby there exist numerous agencies with enormous energy and level of effort, but at times pursuing different and occasionally contradictory agendas based upon the varied needs of their customer bases and the competing visions of their leadership. It is precisely this state of affairs that has led to some consternation on the part of long-time practitioners who feel a sense of institutional aimlessness, even despite the significant inflow of resources over the last decade. And as Cardillo points out, even that seemingly endless flow of resources can no longer be considered a permanent part of the budgetary landscape in these times of fiscal uncertainty.

Theoretically, the IRTPA was supposed to address the challenges of a lack of ultimate accountability and lack of a central directing authority within the broader IC with the establishment of the post of DNI. But as the *Tenth Anniversary Report Card* highlights, the DNI's status within the IC constitutes one of the lingering areas deserving executive-level attention to remedy persistent confusion over big picture authority and direction:

> It still is not clear, however, that the DNI is the driving force for intelligence community integration that we had envisioned. Some ambiguity appears to remain with respect to the DNI's authority over budget and personnel. Strengthening the DNI's position in these areas would advance the unity of effort in intelligence, whether through legislation or with repeated declarations from the president that the DNI is the unequivocal leader of the intelligence community.[34]

The report card's emphasis on the need to more clearly designate the DNI as the President's chief intelligence adviser is simply one of the more recent echoes of what

---

[33] Cardillo, "Intelligence Community Reform," 6.

[34] NSPG, *Tenth Anniversary Report Card*, 17.

many in the community have been critiquing since passage of the IRTPA, namely, the continued fractured and disjointed state of the domestic intelligence architecture. Former CIA officer and White House aide, Bruce Riedel, has commented, "You have a very large posse and no real sheriff running it."[35] A fellow former CIA officer, Henry Crumpton, echoes this view with his observation that "America relies on a deeply fractured and rudimentary domestic intelligence community, one that has growing but still insufficient links to the U.S. external intelligence systems."[36] And Luis Garicano and Richard Posner have detected "the sense that nobody is in charge," asserting, "We have an unwieldy multiplicity of agencies that operate largely independently."[37] They capture a sense of institutional inertia predominating in the domestic intelligence sphere when they state, "The national intelligence apparatus of the U.S. has fewer employees than GM had in its prime, yet it consists officially of 16 separate agencies, and unofficially of more than 20. Each of these agencies is protected by strong political and bureaucratic constituencies, so that after each intelligence failure everything continues pretty much the same and usually with the same people in charge."[38]

The collective suggestion seems to be that the domestic intelligence apparatus is in need of a good floor manager, someone who has been granted unambiguous authority by Congress and the President to be the go-to person for accountability and strategic direction. But as the current status of competing responsibilities and authorities persists, one gets the increasing sense that the U.S. intelligence system lacks the necessary rudder mechanism to maintain a focused course. While new capabilities have been added since the 9/11 attacks and everyone has seemingly gotten the talking points down about working more collaboratively in defense of the homeland, the organizational evolution that was supposed to be ushered in by the creation of DHS and passage of the IRTPA has

---

[35] Daniel Dombey, "U.S. Intelligence: Tribal Warfare," *Financial Times*, March 12, 2010, http://www.ft.com/intl/cms/s/0/0a252d6e-2c6e-11df-be45-00144feabdc0.html#axzz2MoM0XvR7.

[36] Henry A. Crumpton, "Intelligence and Homeland Defense," in *Transforming U.S. Intelligence*, ed. Jennifer E. Sims and Burton Gerber (Washington, DC: Georgetown University Press, 2005), 199.

[37] Luis Garicano and Richard A. Posner, "What Our Spies Can Learn From Toyota," *Wall Street Journal Op-Ed*, January 12, 2010, http://online.wsj.com/article/SB10001424052748704586504574654261998633746.html.

[38] Ibid.

been at times halting and occasionally hindered by legacy turf wars and the resistance by some to relinquishing bureaucratic power.

Journalist Daniel Dombey illustrates this stunted institutional evolution well in his discussion of the bureaucratic turf war that ultimately led to former DNI Dennis Blair's decision to step down from the post in May 2010:

> Part of the blame for the confusion may belong to legislators and the current administration. When the 9/11 commission proposed the position of director of national intelligence, it envisaged a clear hierarchy in which the CIA director would serve as the DNI's number two. That never happened. Instead, the CIA remains an independent power base – a fact emphasized late last year when Mr. Obama sided with Mr. Panetta rather than Mr. Blair in a dispute over whether CIA station chiefs overseas, rather than representatives from other agencies, would always be the senior US intelligence officials in foreign countries.[39]

As this passage touches on, in some respects passage of the IRTPA has not been as transformative as envisioned. To a degree, this is about strong personalities within the Beltway who have shown an ability to engage in bureaucratic warfare with notable skill in the service of protecting the status quo. But perhaps to a larger degree, the kind of institutional evolution envisioned by the sponsors of the IRTPA just takes a lot of time. The National Security Act of 1947 and the Goldwater-Nichols Act of 1986 are exhibits A and B in this regard. Big, set-in-their-ways intelligence institutions are like glaciers, requiring not only tremendous political force to move, but also time—measured in decades, not months or years. This has been perhaps the toughest reality for would-be intelligence reformers to confront: despite clear and cogent calls by the members of the 9/11 Commission and others to truly remake the U.S. domestic intelligence structure, when push has come to shove, political considerations and long-standing bureaucratic rivalries have overshadowed the reform effort since 9/11.

C. CONCLUSION

The challenge of institutional evolution is a long-term one with deep historical precedents in the U.S. national security arena. The legislation that created DHS and the

[39] Dombey, "U.S. Intelligence."

legislation that established NCTC and the DNI position have attempted to accomplish two distinct, but related, goals. In the case of DHS, the overarching goal has been to redefine the parameters of the domestic intelligence effort within the U.S. government, whether officials choose to use the words "domestic" and "intelligence" in the same sentence or not. This effort involved the introduction of a whole new structural design in the form of a new cabinet-level department incorporating 22 separate agencies that had existed independently or under different bureaucratic umbrellas prior to the advent of DHS.

The IRTPA, on the other hand, attempted to do something wholly different but no less difficult. Building largely on capabilities and institutions already in place within the IC, the IRTPA set about changing cultural norms by imposing what was supposed to be a new ultimate level of authority and accountability in the Office of the DNI. It is hard to say which endeavor has been more challenging. Getting agencies and individuals to better communicate with one another in the context of DHS has proven challenging because of the large number of moving parts and the addition of wholly new offices and positions of leadership. Doing the same in the context of the DNI has proven challenging because of the decades of institutional inertia that had built up during the Cold War years.

In each case, the lessons to be learned have been the same: such large transformations take time and one cannot reasonably expect instantaneous institutional responsiveness, given the magnitude of the challenge and the number of actors involved. But given the urgency of the problem—the critical drive to prevent a second 9/11 of potentially even greater destruction and disruptiveness—the question remains: Is there sufficient time to allow natural institutional evolution of the kind Americans have grown accustomed to over the years to take place? The herculean efforts of the men and women on the front lines of the myriad DHS mission sets and the DHS and DNI leadership notwithstanding, the clock continues to tick.

Certain metrics may suggest that the government is winning this battle against time and prevailing in the effort to prevent another major terrorist attack on U.S. soil, but what seems a good track record over the last decade could be negated a day, a week, a month, or a year from now by a successful attack. And in such a dreaded scenario,

people will ask whether the new institutions and ways of doing business that were ushered in under the landmark intelligence reforms discussed in this chapter sufficiently encapsulated the sense of urgency that was present in the warnings of the 9/11 Commission and others. My hope is that the pace of institutional reform in the U.S. domestic intelligence community has been sufficient to meet the terrorism challenge of the times, but I am concerned that the needed changes that were articulated in the wake of the 9/11 attacks continue to take too long to fully implement.

One of the consequences of a homeland security infrastructure that continues to suffer from a significant degree of fragmentation is a lack of effective intelligence prioritization, which is the subject of the following chapter. As efforts have been ramped up to collect greater and greater amounts of information about anything that may pertain to the security of the homeland, it has become imperative for DHS and the IC at large to do a better job of prioritizing those areas of greatest concern and targeting more precisely their collection and analysis efforts. Hampered by a need to serve many different masters and a desire to demonstrate the ability to function in a wide array of emerging threat areas—including cyberspace, infrastructure protection, counternarcotics, and counterterrorism—DHS in particular has struggled with how best to prioritize where it allocates its resources so as to get the best bang for the buck. At times it has seemed that the department has chosen a strategy of spreading itself thin over many different areas of homeland security concern rather than concentrating its efforts in a handful of core-capability areas, which may emerge as a significant constraint on its ability to more effectively ensure domestic security in the future.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. JACK OF ALL TRADES, MASTER OF NONE?: CHALLENGES IN DOMESTIC INTELLIGENCE PRIORITIZATION

Just as challenges associated with fusion and the slowness of institutional evolution have hampered efforts within both DHS and the broader IC to develop a more robust, seamless domestic intelligence infrastructure, so too has the issue of intelligence prioritization. Intelligence prioritization comes in many forms, but for the purposes of this paper will be considered an organization's ability to focus collection and analytical resources on those mission areas deemed within that organization's core competency and which contribute in fundamental ways to the preservation of homeland security. With this baseline in mind, a review of the diverse primary and secondary source literature over the past few years suggests that DHS and the IC continue to struggle with how best to not only divvy up domestic intelligence tasks and mission sets between agencies, but also how best to hone in on those more specific areas of focus requiring collection and analytical effort.

This chapter will provide an examination of how DHS and the IC as a whole have struggled with intelligence prioritization—including challenges associated with mapping the domestic intelligence landscape and determining who is ultimately in charge—with analysis focusing on four particular areas: 1) the drawbacks of an increasingly popular shift toward taking an all-hazards approach; 2) an overemphasis on collection of information at the expense of complementary analysis; 3) a continuing lack of effective tools for measuring the success of targeted intelligence distribution to customers; and 4) the persistence of redundancies, ambiguities, and lost accountability that has resulted from overlapping mission sets between competing agencies.

A. THE INTELLIGENCE PRIORITIZATION PROBLEM DEFINED

Identifying intelligence prioritization as one of the core areas of underperformance to have emerged from a series of blue ribbon studies conducted throughout the 1990s examining the IC and the government's counterterrorism efforts, Amy Zegart finds that, in the words of the President's National Performance Review of

1993, "the system for establishing intelligence collection and analysis priorities [was] a 'jumble of loosely connected processes' that did not satisfy the needs of policymakers."[40] This apparent lack of an IC-wide system for establishing clear intelligence priorities was something that would need to be addressed in the series of post-9/11 intelligence reforms examined in this paper. Ideally, the establishment of DHS and passage of the IRTPA would be seen to have instituted a prioritization process whereby the most important mission sets not only rose to the top of DHS and the IC's agendas, but were then allocated among the different specialty agencies within the domestic intelligence system so as to de-conflict efforts and avoid redundancy.

On the contrary, what appears to have occurred over the last decade is a kind of mashing up of resources and agency focus areas so that, with a few notable exceptions, intelligence prioritization within the homeland security community today is as elusive as it was in the post-Cold War/pre-9/11 interregnum. Concerns raised by the Hart-Rudman Commission in the late 1990s over "dangerous tradeoffs between coverage of important countries, regions, and functional challenges" still largely ring true today.[41] One of the main challenges has been the inability to take a significant influx of financial and human resources in the years immediately after the 9/11 attacks and evenly distribute them across the system so as to maximize their effectiveness in key areas of concern. Instead, the prevailing philosophy around Washington since 9/11 has seemed to be that if you do more of everything—more collection, more analysis, more staff hiring—the security of the homeland will be better off for it. But my view is that if you act in such a way where you are essentially prioritizing everything, in reality you end up prioritizing nothing.

B. DRAWBACKS OF THE ALL-HAZARDS APPROACH

As the country has gotten further away from the events of 9/11 in terms of both memory and time, the counterterrorism mission has begun to take a back seat in some local jurisdictions for which the terrorism threat has never appeared that clear and present. As the Senate's Permanent Subcommittee on Investigations (PSI) of the

---

[40] Zegart, *Spying Blind*, 27, 36–37.

[41] Ibid., 37.

Committee on Homeland Security and Governmental Affairs recently pointed out in an examination of fusion centers, even the larger "statewide fusion centers and fusion centers in major cities indicate that they emphasize anti-crime efforts and 'all-hazards' missions over an explicit focus on counterterrorism."[42] This is an understandable adjustment by these fusion centers to the reality that the terrorist threat at home has not proven to be the all-consuming threat over time that had so gripped the nation's psyche in the weeks and months immediately following the 9/11 attacks. However, opening the fusion centers up to an all-hazards approach brings some perils of its own.

As the PSI report further points out, a 2010 Baseline Capabilities Assessment conducted by the Program Manager for the Information Sharing Environment (PM-ISE) indicated that terrorism had slid down the priority list of many fusion centers and been replaced by a myriad of assorted focus areas more purely criminal in nature:

> Most [fusion] centers focus on the priority mission of the law enforcement agency that owns/manages them; primarily analytical case support to drug, gang, and violent crime investigations for the geographic area of responsibility. As a result many centers struggle to build the necessary capabilities required to support Federal counterterrorism mission requirements, specifically in the areas of intelligence analysis and information sharing beyond their jurisdictions.[43]

This atrophying of counterterrorism-related analytical and information sharing skills constitutes one of the more worrisome consequences of the shift to an all-hazards approach by many fusion centers. While the fusion center directors cannot be faulted for looking for the best ways to leverage the resources available to them to tackle the most important issues in their regions—like drugs and gang violence—this trend does nevertheless serve as a notable deviation from the original conception of how fusion centers would fit into the broader homeland security network.

The key problem lies in the fact that by widening their nets, so to speak, fusion centers run the risk of skewing intelligence prioritization toward more of a law

---

[42] U.S. Senate, *Federal Support for and Involvement in State and Local Fusion Centers*, Majority and Minority Staff Report for the Permanent Subcommittee on Investigations of the Committee on Homeland Security and Governmental Affairs, October 3, 2012, 93.

[43] Ibid., 96.

enforcement focus, which in many cases has already occurred. The Northern California Regional Intelligence Center (NCRIC), for instance, functions under a High Intensity Drug Trafficking Area (HIDTA) construct, with a logical focus primarily on counternarcotics work. As a result, the NCRIC is likely one of the more competent counternarcotics-oriented fusion centers within the national network, but likely lacks the level of counterterrorism expertise of the New York or Washington, D.C.-area fusion centers, where the threat of terrorism occupies much more of their attention. Again, this branching out to take on more focus areas runs the risk of diluting the overall effort, to the point where, by prioritizing a myriad of issues like counternarcotics, gangs, and immigration, fusion centers run the risk of losing an essential homeland security focus as envisioned in the original legislation creating DHS. There really has not been a clear prioritization of counterterrorism or any other particular area across the board nationally, but rather a continual expansion of mission sets to the point where fusion center competence in various homeland security areas is widely variable throughout the national network.

C. OVEREMPHASIS ON COLLECTION AT THE EXPENSE OF ANALYSIS

What has happened with fusion centers in this regard is emblematic of how DHS as a department has chosen to deal with intelligence prioritization more broadly. From the earliest days of the nascent DHS intelligence capability, there seems to have been a drive to collect as much information as possible (without the requisite link to clearly defined intelligence requirements) in the hope that the level of awareness generated by such collection would catch up over time. This was reflected in comments made in 2008 by the then-under secretary of Homeland Security for I&A, Charles Allen. Speaking of the thousands of customs enforcement interactions conducted every day by representatives of DHS's component agencies, Allen stated, "These encounters generate a treasure trove of data that we are just now learning how to report, collate, and share. This means that DHS is a collector, producer, and consumer of intelligence, which makes my work that much more challenging."[44]

[44] Allen, "Terrorism in the Twenty-First Century."

On the one hand, Allen's understanding of DHS's I&A as having a hand in virtually all forms of intelligence passing through the components' hands is admirable and in line with what good intelligence officers do. They constantly seek to expand their knowledge of the threat environment by gaining access to greater quantities of information so they can stay apprised of the threat and keep their bosses informed. Allen, as one of the influential early figures at I&A, was doing the right thing by trying to get DHS intelligence out of its shell and into the fight. But a long-term consequence of this ethos about DHS being simultaneously a "collector, producer, and consumer of intelligence" is that, by not prioritizing any one of those functions, DHS has remained somewhat mediocre at all of them.

The reason for this, much like the reason for DHS's challenges in the areas of fusion and institutional evolution, has to do with the problem of scale. As DHS has turned the spigot that has unleashed this deluge of information flowing from its numerous and diverse components—TSA, the Coast Guard, CBP, to name a few—I&A has never really learned how to prioritize collection and analysis efforts among the components and within DHS headquarters to the point where greater sense can be made of the overwhelming mass of homeland security information. Discussions surrounding an Aspen Institute report on DHS's role within the broader IC help illustrate this point.

In her opening statement at a January 2012 hearing on the contents of the Aspen Institute report, Representative Sue Myrick, chairwoman of the Subcommittee on Terrorism, HUMINT, Analysis, and Counterintelligence of the House Permanent Select Committee on Intelligence (HPSCI), summed up the prioritization issues DHS's I&A has dealt with from its inception: "This Committee has encouraged I&A to focus its mission on the areas where it can provide a unique value added. In years past, the office has attempted to gain relevance through its involvement in a wide variety of issues. While I certainly can understand the pressure on I&A to spread its arms far and wide, I firmly believe that it will gain relevance, and contribute most effectively to the intelligence mission, by zeroing in on its core mission."[45] She wholeheartedly endorses the key

[45] *Role of DHS*, Subcommittee Chairwoman's Opening Statement.

Aspen Institute observation that, "In an age of budget constraints, pressure on DHS to focus on core areas of responsibility and capability—and to avoid emphasis on areas performed by other entities—may allow for greater focus on these areas of core competency while the agency sheds intelligence functions less central to the DHS mission."[46]

Some observers have highlighted the consequences of DHS and its components having an unwieldy intelligence collection capability with inadequate coordination. Gregory Treverton of RAND notes that one of the key problems associated with the challenge of domestic intelligence collection is that "too many agencies are collecting information with too little coordination. While there can be benefits to decentralization and diversity in activity, having many individual actors operating independently can create duplication and conflict."[47] This problem of "duplication and conflict" applies both to DHS specifically and the IC as a whole. Touching briefly on shortcomings observed in the coordination of intelligence collection at places such as the FBI's Field Offices and U.S. Attorney's offices, Treverton brings his focus to DHS:

> Similar questions were raised during the internal DHS review about the potential for "multiple points of collection without coordination" within the Department's component agencies intelligence efforts. Broadening from coordination of federal efforts to the domestic intelligence enterprise overall, state and local organizations have criticized the lack of a consolidated requirements process for homeland security intelligence to ensure that collection matches the needs of the relevant consumers.[48]

Treverton points out an important trend seen within DHS over its first decade of existence whereby its collection efforts have often preceded any kind of strategic plan for how to steer that collection in the direction of maximum effectiveness. The problem of "collection without coordination" has seemed to be a secondary concern for planners and leadership at DHS, who have appeared to prioritize getting the immense and complex

---

[46] Ibid.

[47] Treverton, *Reorganizing U.S. Domestic Intelligence*, 29–30.

[48] Ibid., 30.

DHS bureaucracy in motion first, and then de-conflicting redundant and duplicative efforts within the organization later.

Perhaps nowhere has this confused sequence of prioritization surfaced more vividly than in the manner in which DHS has worked with state fusion centers to establish Standing Information Needs (SINs). After a study concluded that "fusion center leaders at pilot sites did not believe that DHS intelligence products fully met their mission needs by providing information of operational importance to state and local law enforcement," I&A set about rectifying the problem in 2007 by beginning the process of clearly identifying fusion centers' information needs.[49] But as a GAO report released in December 2010 notes, "As of August 2010, 9 states had completed efforts to identify their information needs, 12 states had completed drafts that were awaiting final state approval, and 20 states were in the process of drafting their needs."[50]

This kind of slow, overly deliberate, urgency-defying process is indicative of the haphazard way in which DHS has approached the problem of identifying collection requirements and, by extension, prioritizing where to place its resources for maximum effect. Admittedly, the state fusion centers themselves must shoulder some of the blame for the long delay in identifying their own SINs. But the fact that I&A was producing intelligence for its state and local customers without these SINs being finalized by the summer of 2010 is a fact that requires greater scrutiny in its own right. That essentially means that roughly seven years after DHS's establishment, the organization still had not fully taken the basic step of identifying the information that would help its local partners—who are often regarded as serving on the front lines in the Global War on Terrorism—gain greater awareness of the multivariate asymmetric threat. This paints a picture of DHS over those first five years or so of its existence as having rushed to get as much intelligence product out to as many customers as possible, without a clear picture of how relevant, timely, or enlightening that intelligence was in the eyes of the customer base. This constitutes one of the fundamental failures of intelligence prioritization on the part of DHS.

---

[49] GAO, *Information Sharing*, 13.

[50] Ibid., 15.

D. LACK OF EFFECTIVE TOOLS FOR MEASURING SUCCESS OF TARGETED INTELLIGENCE DISTRIBUTION

Just as it is vitally important for an intelligence-producing organization to clearly understand the needs of its intelligence consumers, so too is it critical that an organization have in place metrics or feedback mechanisms that allow it to alter course in the event that its customers are not satisfied with the intelligence being distributed. This stands as the third area in which DHS has shown a need to better hone how it allocates resources in the pursuit of more effective intelligence prioritization. In numerous instances, it appears that DHS or its components have failed to properly self-assess in a way that would allow them to become more aware of how well they are doing their job of providing domestic intelligence to federal, state, and local customers.

As the GAO noted in its December 2010 report on information sharing within DHS, "According to standard program management principles, time frames or milestones should typically be incorporated as part of a road map to achieve a specific desired outcome or result."[51] This was a not-so-subtle admonishment of I&A's leadership for taking roughly three years to finalize the SINs of only nine state fusion centers, as discussed above. Unfortunately, the lack of clearly defined goals and effective mechanisms for DHS to determine whether it is meeting its goals appears to be a long-running problem for the department as a whole and its intelligence function in particular. But as the GAO report also demonstrates, DHS and its components certainly do not suffer from any lack of production:

> From June 2009 through May 2010, I&A disseminated thousands of Homeland Intelligence Reports to its state and local partners through fusion centers. I&A officials noted that the number of reports disseminated has increased over time because of the overall increase in the number of submissions from DHS components, such as U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement, as well as greater reporting by state and local partners.[52]

---

[51] Ibid.

[52] Ibid., 12.

Rather, the real problem is that such significant production has less often been distributed in a targeted fashion that would allow I&A and its components to more precisely tailor intelligence to specific constituencies. Challenges faced by TSA in this regard illustrate the point well.

As the GAO noted in its November 2011 report on information sharing among TSA and its transportation sector stakeholders, despite general agreement by those stakeholders that TSA provides valuable intelligence, there remains room for improvement in how TSA continually monitors whether its transportation sector customers are getting the intelligence they need. The GAO observed that the lack of a more "targeted outreach" approach was limiting TSA's efforts to reach as many customers as possible, resulting in an uneven familiarity among stakeholders with TSA's primary dissemination tool, the Homeland Security Information Sharing Network Critical Sectors portal (HSIN-CS):

> The absence of measurable outcomes for targeted outreach to different transportation sectors hinders DHS efforts to ensure dissemination of security-related information to all appropriate stakeholders. DHS's outreach efforts have not resulted in widespread HSIN-CS awareness and use among transportation stakeholders who we surveyed, and therefore conducting targeted outreach to stakeholders, and measuring the effectiveness of this outreach, could help to increase awareness and use of this mechanism.[53]

As the GAO analysis suggests, it is very difficult as an organization to know whether your efforts are on the right track if there is a lacking or nonexistent mechanism in place for understanding whether those on the receiving end of your work are better able to do their jobs as a result of it. This is a problem that has plagued not only TSA but various elements throughout DHS's I&A since inception. The argument is not with a lack of effort but with an occasional lack of "targeted" effort that would allow I&A's components to more effectively prioritize their intelligence collection and analysis and the allocation of human resources toward those ends. This is likely merely the result of nascent bureaucratic practices still in their evolutionary infancy, but it is a problem that

[53] GAO, *Transportation Security Information Sharing*, 28.

DHS needs to address nonetheless. I&A's intelligence-producing components cannot genuinely know where they are going until they know where they have been, and right now they have demonstrated an uneven awareness of just how effectively they have supported their stakeholders over the last decade of their work. Until that gets rectified, effective and consistent intelligence prioritization—whereby the right resources are allocated in the right places at the right times—cannot occur.

E. REDUNDANCIES, AMBIGUITIES, AND LOST ACCOUNTABILITY RESULTING FROM OVERLAPPING MISSIONS

One of the primary challenges to effective intelligence prioritization within DHS has been the prevalence of duplicative responsibilities among component agencies, resulting in blurred lines of authority, redundant effort, and decreased accountability. With a more precisely defined set of responsibilities allocated among its components, DHS could get greater bang for its intelligence buck while pinning sole accountability for specific mission areas on a smaller but potentially more responsive set of actors. In the end, this would be a good prioritization move to the extent that it would preserve precious resources in a tightening fiscal environment while promoting greater de-confliction of effort among its myriad collection and analytical endeavors.

As Representative Myrick stated in January 2012 at the aforementioned congressional hearing on the contents of the Aspen Institute report on DHS, "I&A historically has suffered from a lack of focus in its mission. This challenge partially stems from vague or overlapping authorities in some areas."[54] Discussing areas of overlap between DHS and other federal agencies such as the FBI, she went on to add, "It is clear that in these areas overlapping authorities and responsibilities created by federal law and policy have contributed to confusion and duplicative efforts. Moreover, the vagueness of some of DHS's responsibilities and authorities has allowed for some interpretation by I&A with regard to its mission."[55] This basic theme threads through analysis of DHS from other quarters as well.

---

[54] *Role of DHS*, Subcommittee Chairwoman's Opening Statement.

[55] Ibid.

The GAO points out the results of a study conducted by the Homeland Security Institute (HSI) in 2009 in which it was noted that the "lack of a strategic plan hindered I&A's efforts to conduct any type of officewide program or resource planning that could be appropriately tied to its mission, goals, and objectives."[56] The report goes on to discuss the consequences of this lack of strategic guidance:

> As a result, HSI found that various I&A components had developed their own goals, priorities, processes, and procedures and, in some cases, may be working at cross-purposes. HSI also found that the lack of I&A efforts to allocate resources to support strategic goals and objectives prevented managers from organizing their efforts for long-term effectiveness, which left them unable to plan for growth or to adapt to emerging issues.[57]

That last point about I&A's resulting inability to adequately "adapt to emerging issues" is an important one when considering the broader issue of intelligence prioritization. As this passage from the GAO report indicates, the fact that individual components within I&A resorted to generating their own priorities and procedures suggests that the components were allocating resources and conducting their collection and analytical work irrespective of what their peer agencies were doing. When such a situation exists, and the overall construct is defined more by the lack of coordination than its prevalence, the ability of the organization to adapt—a critical requirement in effective intelligence prioritization—is severely compromised.

However, the responsibility for this prevailing ambiguity and confusion over what specific I&A components own which pieces of the intelligence pie does not rest solely with I&A planners and leaders themselves. As last year's *Tenth Anniversary Report Card* points out, Congress must shoulder some of the blame for pulling DHS in numerous directions in the course of its oversight efforts. Responding over the last few years to thousands of briefing requests and hundreds of requests for testimony from over 100 congressional committees, DHS has remained significantly occupied with the mere process of keep Congress abreast of its work. But as the *Report Card* pointedly suggests, "The result is that DHS receives conflicting guidance and Congress lacks one picture of

---

[56] GAO, *Information Sharing*, 26–27.

[57] Ibid.

how that enormous organization is functioning. Congress should be helping integrate the sprawling DHS; a fragmented oversight approach defeats that purpose."[58]

Whether due to congressional oversight issues, the sprawling nature of its bureaucratic makeup, or the relative newness of its domestic intelligence mission, DHS continues to wrestle with the challenge of how best to prioritize the allocation of its resources so as to maximize the security of the homeland. This is no easy task with 22 competing agencies under one umbrella, but there persists this sense that occasionally within DHS the right hand does not fully know what the left hand is doing. While this is not due to any lack of effort on the part of agencies or components to contribute to the overall homeland security mission—I&A, for example, has produced steadily more intelligence for its customers over the last several years—that effort continually lacks the strategic direction that would allow the department as a whole to more effectively allocate its resources to those areas of highest priority and reduce some of the duplicative effort and ambiguous authority that is increasingly characteristic of how DHS operates.

Similar issues of ambiguous authority and redundant lines of effort have become an obstacle to more streamlined intelligence prioritization within the broader IC as well. Highlighting some of the areas of concern that were identified by the group of experts and practitioners he interviewed for his RAND report on alternative organizational options for the U.S. domestic intelligence system, Treverton noted prevailing concerns over "confusion," "ambiguity," and uncertain responsibility at the national level: "Interviewees and panel members highlighted concerns that similar activities are proliferating at different places within the domestic intelligence system. Participants cited this as a result of confusion and ambiguity about the roles of particular agencies within the domestic intelligence enterprise and uncertainty about who is responsible for what parts of the effort."[59]

Treverton sees reinforcement of these concerns in the 2005 WMD Commission Report. Citing the negative effects of duplicative analytical efforts at the national level

---

[58] NSPG, *Tenth Anniversary Report Card*, 16.

[59] Treverton, *Reorganizing U.S. Domestic Intelligence*, 26.

on the ability of state and local authorities to fulfill their domestic intelligence responsibilities, he enlists as evidence one of the WMD Commission's key findings:

> The redundant lines of communication through which terrorism-related information is passed—for example, through the Joint Terrorism Task Forces, Anti-Terrorism Advisory Councils, Homeland Security Information Network, TTIC Online, Law Enforcement Online Network, Centers for Disease Control alerts, and Public Health Advisories, to name just a few—present a deluge of information for which state, local, and tribal authorities are neither equipped nor trained to process, prioritize, and disseminate.[60]

The multiplicity of agencies and networks devoted to terrorism-related intelligence distribution reflects the overarching challenge to intelligence prioritization posed by the vastness of the national domestic intelligence infrastructure. State and local law enforcements authorities, as the front line in the domestic security effort, have access to such a large amount of information that it has become difficult for them to prioritize one source of intelligence over another. The domestic intelligence system as currently constructed places the bulk of the burden on local entities to decide what information is of highest priority. In the case of state fusion centers with limited manning and whose analysts are not always career intelligence professionals but are often law enforcement or public safety officials trained in intelligence analysis as a collateral duty, this extra burden is no trivial matter. The current system has placed a premium on the notion that the federal government should never be the last to hold vital information. But in doing so, there has not been a sufficient emphasis on the local consumer side to allow the end users of the federal government's vast intelligence resources to more effectively prioritize need-to-know intelligence over good-to-have information.

F. CONCLUSION

Both DHS and the broader IC have improved by leaps and bounds in terms of their collective ability to push information to the customer at the end of intelligence chain. Through DHS's I&A and its component intelligence elements, the domestic

[60] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States*, March 31, 2005, 287.

intelligence infrastructure is far more robust than it was before the 9/11 attacks. Likewise in the IC, the establishment of NCTC has helped create a culture of terrorism-related information sharing among federal departments and agencies that was in desperate need of improvement in the aftermath of 9/11. But the point has come where it is now time to move on from the general attempt to stand up new institutions and begin to focus on process refinement and more effective prioritization. The domestic intelligence system has shown an ability to gather large quantities of information and distribute it across a broad collection of federal, state, and local organizations. Unfortunately, that alone will no longer be sufficient over the next ten years of DHS and the IC's evolution.

Representative Mike Thompson, Ranking Member of HPSCI's Subcommittee on Terrorism, HUMINT, Analysis, and Counterintelligence, said simply of the future of DHS, "It now makes sense to step back from daily oversight and consider the pros and cons of expansion of the DHS intelligence mission to other areas, such as cybersecurity. […] The question is not just what DHS Intelligence **should** do in the future, but whether DHS is **able** to do it."[61] This encapsulates perfectly well the crossroads at which the U.S. domestic intelligence system as a whole currently finds itself. Instead of constantly seeking additional missions and looking for more ways to make itself relevant, it is time for DHS and the numerous domestic security-related agencies within the IC to begin looking within to determine how better to prioritize their efforts and become more user-friendly for the thousands of frontline responders around the country who rely on their information. The final chapter, which follows, will explore alternative approaches that DHS and the IC can employ to create a more honed-in, efficient domestic security enterprise.

[61] *Role of DHS*, Subcommittee Ranking Member's Opening Statement.

V. THE WORK HAS JUST BEGUN: CONSIDERING ALTERNATIVES FOR IMPROVING DOMESTIC INTELLIGENCE

Having discussed the myriad challenges posed for DHS and the IC by issues associated with domestic intelligence fusion, institutional evolution, and intelligence prioritization, it is important to examine common problems within those areas and what, if anything, can be done to mitigate them and chart a new path forward that incorporates alternative approaches to those already tested over the last decade. As with many large undertakings, the key challenges in the domestic intelligence field appear to be organizational, with continuing struggles to channel the considerable manpower and resources invested in the homeland security arena over the last decade toward more efficient and effective ends. The solution likely lies not in breaking up the puzzle and beginning completely anew, but rather in tweaking pieces of the puzzle here and there in order to come to a more comprehensible and logical arrangement of parts.

This final chapter will briefly examine the prospects for consolidation and specialization within the U.S. domestic intelligence system. Key within this debate is the idea that U.S. domestic security is not best served by a top-down, conventionally hierarchical intelligence structure. Instead, leaders need to consider the benefits of adopting the tactics of the most capable asymmetric adversaries arrayed against the United States. This includes an organizational ability to drive responsibility and execution down to the lowest levels, which breeds greater adaptability in the face of frequent changes to the threat landscape. In addition, some notable voices have expressed concern over an artificially rigid divide between domestic and foreign intelligence which, despite the landmark reforms enacted shortly after the 9/11 attacks, continues to influence the way important intelligence agencies interact with each other in Washington. Finally, the introduction of so many new DHS subcomponents with indigenous intelligence capabilities of their own necessitates a brief discussion of whether the IC should be formally expanded to provide a better seat at the table for domestically-focused intelligence agencies.

A. CONSOLIDATION

One common criticism of the current domestic intelligence architecture that surfaces from various analyses is that the system in place now remains too disjointed, fractured, and bureaucratically dispersed to achieve the optimal level of responsiveness to a dynamic and rapidly changing domestic threat environment. Gregory Treverton of RAND has brought to light the observations of several high-level practitioners and domestic security experts who feel this way and others have chimed in on this subject as well. And while some have pointed out the fact of this disjointedness within the domestic intelligence system, others have proposed alternative means of approaching the issue of domestic intelligence in an effort to address the problem of disjointedness. For example, Luis Garicano and Richard Posner have proposed consolidation within the IC on a grand scale: "One possibility that deserves serious consideration would be a consolidation of most existing agencies into four primary agencies: a foreign intelligence agency, a military intelligence agency, a domestic intelligence agency, and a technical data collection agency (satellite mapping, electronic interception, etc.)."[62]

While the merits of Garicano and Posner's proposal across the entire IC are open to debate, the main thrust of their argument for a simplified intelligence structure resonates particularly strongly when applied to DHS's I&A and the multitude of DHS intelligence elements it must coordinate. On the one hand, there are benefits to having distinct intelligence elements within such disparate DHS agencies as CBP, ICE, USCIS, TSA, the Coast Guard, and the Secret Service. One could argue that each of these agencies performs a critical domestic security function encompassing thousands of routine and high-interest interactions every day. On the other hand, the existence of six separate intelligence elements within the DHS Intelligence umbrella alone suggests the potential for information overload, challenges with inter-agency coordination, and uncertain accountability, which the preceding chapters have discussed in detail.

To remedy some of these recurring problems, it might be wise to take a Garicano and Posner approach to the organization of DHS Intelligence. Rather than continuing

[62] Garicano and Posner, "What Our Spies Can Learn From Toyota."

with the multiplicity of intelligence elements within the various components that has come to dominate the current organizational arrangement, planners could seriously consider the possibility of refining DHS' intelligence functions down to a set of core focus areas. For example, CBP, ICE, and USCIS, while not sharing identical missions by any stretch of the imagination, do arguably cover common territory in the conduct of their daily duties. Rather than have three distinct intelligence elements working for each of these agencies in different office space and with different marching orders from their agency bosses, an alternative would be to consolidate their intelligence functions within an Illicit Flows Intelligence Directorate within DHS, encompassing the areas of counternarcotics, customs enforcement, and immigration.

Similarly, TSA and the Coast Guard, which are responsible for distinct components of the transportation landscape, do nonetheless share an important focus on securing vital components of the nation's infrastructure system. Planners could feasibly consolidate the intelligence elements of TSA and the Coast Guard within an Infrastructure Intelligence Directorate that would be responsible for incorporating DHS' varied infrastructure intelligence functions. A Counterterrorism Intelligence Directorate could be charged with maintaining a critical linkage with NCTC and the CIA and FBI's respective counterterrorism capabilities, along the lines of the FBI's new Joint Regional Intelligence Group (JRIG) concept, which would share collocation in major urban fusion centers with the DNI's Domestic Intelligence Representatives. Finally, a Cyber Intelligence Directorate within DHS would help to focus the department's efforts in a realm in which it has made clear it would like to be a key player, but for which its capabilities are still in a maturing phase and lack the robustness of its Defense Department counterparts at the National Security Agency.

B. SPECIALIZATION

While consolidation within DHS in particular could go a long way toward focusing the department's efforts on a key set of critical mission areas, a drive toward more specialization within DHS and the IC as a whole with respect to domestic intelligence operations could have the effect of enhancing accountability and empowering

those analysts at the lower, and consequently more responsive, levels of the domestic intelligence system. Under Secretary Wagner highlighted a promising concept in this regard in the congressional testimony she gave in May 2010:

> One of the main improvements, I think, that is being made in the intelligence community is the idea of these pursuit groups, where we are charging people to take hold of a specific piece of information and follow it all the way through, to pull that string to find everything else, and to institutionalize that approach so that we don't have compartmentalization, you know, like, "I am assuming that this guy here did something on this so I am not going to check to make sure it got done."[63]

A pursuit group approach implemented more consistently across the domestic intelligence system has the potential to cut across all three of the primary problem areas discussed in this paper. Such an approach could help improve intelligence fusion by charging a specific person or group of people with correlating data in a manner that would force them to interface with other agencies. It could partially sidestep the growing pains associated with institutional evolution by driving ultimate responsibility for a mission or focus area to a smaller, more responsive group of specialists in a given area. And it could potentially improve intelligence prioritization by creating small groups or individuals who are well-versed in what it takes to distinguish background noise from crucially relevant intelligence that is vital to the isolation of a threat to domestic security.

Henry Crumpton takes this concept of the pursuit group approach a step further by proposing the possibility of establishing a "domestic *security intelligence* corps" and a "special agent-case officer (SACO)" position, as a way of specializing the unique skills required for domestic intelligence gathering, analysis, and dissemination.[64] This idea also has merit in that it gets to the heart of a historically-based challenge within the FBI in particular concerning an institutionally ingrained unwillingness within that organization to acknowledge intelligence professionals as on par with their special agent peers. By professionalizing the homeland security intelligence analyst as a distinct career choice for an aspiring young person entering the domestic intelligence field today, there

---

[63] *DHS Intelligence Enterprise*, 21.

[64] Crumpton, "Intelligence and Homeland Defense," 210.

exists the potential to breed a whole cadre of future experts in a field that is perhaps still defined more by the tricky civil liberties questions it poses than any hard and fast truths about how best to tackle the thorny issues of domestic protection. What is clear is that the status quo method of making domestic intelligence analysis a collateral duty for some (as in many fusion centers) or a position of low regard for others (as in the FBI) is a temporary band-aid that will not serve the nation's domestic security interests well in the future.

C. THE FOREIGN-DOMESTIC INTELLIGENCE DIVIDE

One of the primary issues contributing to a perception of the domestic intelligence system as being fairly disjointed and fractured at the macro level is the persistence of a divide between foreign and domestic intelligence that often hinders better coordination. Just as consolidation and specialization could potentially address the handful of shortcomings detailed in this paper, so too could bridging the divide between foreign and domestic intelligence help to create a more seamless domestic intelligence system.

Art Hulnick captures the dilemma well in his discussion of the drawbacks of having a Cold War-era legacy of divided foreign and domestic intelligence operations persist into a new era in which groups like Al Qaeda do not abide by the same rules of engagement as the Soviets did. As one of his proposed areas of intelligence reform going forward, Hulnick has suggested doing away with this "artificial" divide:

> The fifth area of reform would end the artificial barriers between foreign and domestic intelligence in collection and analysis. This relic of the Cold War era had resulted from fears that intelligence agencies might become secret police agencies, as had happened in Nazi Germany, the military dictatorship of wartime Japan, and the Communist state of the Soviet Union. Terrorism, espionage, and global crime do not respect such boundaries. To establish an efficient intelligence system that actually shares information and works together, the rules and laws that maintain the split between foreign and domestic operations and research must be changed.[65]

[65] Arthur S. Hulnick, "Intelligence Reform 2008: Where to from Here?" *International Journal of Intelligence and CounterIntelligence* 21 (2008): 630.

Hulnick's point is an important one that deserves further consideration by domestic security planners. By multiple accounts, the U.S. counterterrorism effort abroad has been very successful in isolating and neutralizing the threat to the homeland emanating from violent extremist organizations abroad, particularly their top leadership. Concerns over civil liberties here in the United States notwithstanding, domestic intelligence operations should be joined at the hip with counterterrorism operations overseas. Agencies like NCTC have gone a long way toward achieving this, but more at the strategic level than the operational. There needs to be more integration between domestic and foreign operations. Crumpton echoes this point, saying, "Another challenge for intelligence in homeland defense is to bridge the gap between domestic and foreign operations. Existing links need to be reinforced and new links forged."[66]

D. ACTING LIKE THE ADVERSARY IN ORDER TO DEFEAT IT

Perhaps most unsettling to domestic experts and average citizens alike in the post-9/11 environment has been a realization that the adversaries of the United States today are more commonly the small, networked, agile, asymmetrically-inclined foes like Al Qaeda and Anonymous who represent a far less predictable threat than the Soviets did more than 20 years ago. As a result, it is incumbent upon the U.S. domestic intelligence system to realize that the most effective way to confront such a distinct type of adversary is not to rely on the Cold War model that fit the IC's needs so well during that time period, but to transition to a smaller, more networked, more agile intelligence approach that challenges the adversaries on their terms.

The creation of state fusion centers that provide a space to concentrate intelligence and law enforcement representatives from federal, state, local, and tribal entities has been a solid step in the direction of creating a more networked, agile line of defense. But to a significant degree, many of the more robust intelligence collection and analysis capabilities still reside with the Washington-based agencies that make up the IC. DHS Intelligence illustrates the hybrid nature of the current arrangement. A full-fledged member of the IC, DHS possesses a seat at the national-level intelligence table equal to

[66] Crumpton, "Intelligence and Homeland Defense," 211.

that of its peers at the FBI and CIA. As previously discussed, it also possesses the intelligence capabilities of six distinct components—CBP, ICE, USCIS, TSA, the Coast Guard, and the Secret Service—which are all organized in the sort of top-down hierarchical structure that is common among Washington agencies.

The real disconnect is that while much responsibility has been driven down to the lowest levels through the creation of state fusion centers, much of the heavy lifting in terms of collection and analysis continues to be done at the national level, thereby fostering a certain level of dependence of state and local authorities on the cooperation and competence of national-level authorities. As Crumpton suggests, a possible remedy for this dependency relationship between local and national authorities would be to allow more locally-oriented intelligence and law enforcement officials to have the autonomy to build greater networks among themselves: "The United States should encourage intelligence and law enforcement leaders in the field to build interdependent networks among themselves and to act decisively, rather than harness them to a distant, centralized, layered system of operational planning."[67] This could at least partially address the current status quo within U.S. domestic intelligence in which the FBI does not share classified collection plans with state and local authorities, leaving those authorities to have to sometimes guess what it is important to collect against.

The pitfalls associated with a "distant, centralized, layered system of operational planning" have been noted numerous times in this paper—whether it be the failure of DHS to work in a timely manner with the states to identify SINs or the occasional distribution by DHS Intelligence of information not particularly well-suited to local customers' needs. What is needed in the future is to take the capabilities being brought to bear now and rearrange them in a way that will further empower analysts and law enforcement personnel at the lowest levels. The conventional top-down approach will simply not stand the test of time as adversaries become smaller, more agile, and less apt to think like the big bureaucracies aligned against them in the domestic intelligence arena.

[67] Ibid., 212–13.

E. SHOULD THE IC BE EXPANDED?

Finally, a possible remedy to the difficulties of coordinating the varied intelligence capabilities within DHS would be to grant individual IC membership status to CBP, ICE, USCIS, TSA, and the Secret Service (with the Coast Guard already serving as a formal member of the IC). While this could potentially bestow upon these components greater legitimacy and networking opportunities in the eyes of formidable peers like NSA, the FBI, and the CIA, the downside risk is that DHS' component agencies would be pulled even further from local entities, with which there exists an uneven and still nascent relationship in the first place. The risks of expanding the IC and granting formal status to those five components outweigh the benefits. The problems of coordination within DHS are an internal matter that can and should be rectified by the Under Secretary for I&A, and a possible realignment along the lines of what has been proposed earlier in this chapter would go a long way toward solving issues of interagency intelligence coordination within DHS.

F. CONCLUSION

A little more than a decade after the 9/11 attacks, it comes as no surprise that DHS and the IC still need more time to fully mature and develop the domestic intelligence system. The broad areas of challenge discussed in this thesis—intelligence fusion, institutional evolution, and intelligence prioritization—to a large degree present understandable obstacles that senior leaders and planners simply need more time to grapple with. The system is by its very nature a vast collection of competing agencies and interests, so fusion would predictably present new challenges. The relatively recent arrival of new entities like DHS, NCTC, and DNI clearly need more time to solidify their bureaucratic foundations. And the system as a whole needs to learn how to get all of the disparate parts to work together in order to avoid duplicative effort and focus on what is truly critical in securing the homeland.

But acknowledging all of this is not to lose sight of a central reality: these three areas need to be addressed with a serious level of urgency within the domestic intelligence community. The terrorist threat will remain persistent, as it has since the

9/11 attacks, and the looming threat of fiscal tightening will add a new dimension to the already difficult task before homeland security specialists. The increasingly urgent focus within the public sector of searching for greater efficiencies in every bureaucratic nook and cranny will not simply pass by the domestic intelligence sphere, somehow leaving it unscathed. Just as the Defense Department and federal entitlement programs will need to scale back in order to address significant long-term debt problems, so too will DHS and the IC as a whole. Just as in a private enterprise, domestic intelligence leaders will need to prove themselves expert at getting the most out of their budgets, and in many cases this will require fresh and creative thinking, which this final chapter has hopefully just begun to touch upon.

It is clear that many within the domestic intelligence arena have worked tirelessly to make the system more responsive and seamless. It is also clear that the incentives to generate even more responsiveness and seamlessness will not go away anytime soon, as asymmetric threats to the homeland proliferate. While the American public often displays a short-term memory over these kinds of issues, senior policy makers cannot afford to do the same. Whether we admit or not, Al Qaeda is evolving, Anonymous is evolving, and a whole host of other actors, both known and unknown, are evolving in ways yet to be seen. The task of getting America's domestic intelligence capabilities up to speed has just begun, and there is more work to be done.

What the federal government must do going forward is to train specialists in the domestic intelligence field—specialists in cyber threats, infrastructure, the flow of goods and people, and counterterrorism—and then breed a culture of cross-collaboration that will allow them to succeed individually and as a community. But the DHS model of attempting to create a big tent where everyone becomes a generalist in all matters of concern to the homeland is not working. We need our own super-empowered individuals to counter the super-empowered individuals arrayed against us, to borrow a Thomas Friedman term. By being smarter with its resources and taking greater care in how it delegates responsibilities across the domestic intelligence bureaucracy, Washington can help DHS and others focus more effectively on only those tasks for which they are best suited, allowing those agencies with the greatest competence in their respective fields to take the lead. Such a concerted effort will help make for a safer homeland.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Allen, Charles. "Terrorism in the Twenty-First Century: Implications for Homeland Security." Remarks to the Washington Institute for Near East Policy, May 6, 2008, http://www.washingtoninstitute.org/policy-analysis/view/terrorism-in-the-twenty-first-century-implications-for-homeland-security.

Blair, Dennis C. "Strengthening Our Front Line of Defense." *Washington Post Op-Ed*, December 18, 2009, http://articles.washingtonpost.com/2009-12-18/news/36806239_1_intelligence-reform-intelligence-agencies-national-intelligence.

Cardillo, Robert. "Intelligence Community Reform: A Cultural Evolution." *Studies in Intelligence* 54 (2010): 1–7.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report to the President of the United States*, March 31, 2005, http://www.gpo.gov/fdsys/pkg/GPO-WMD/pdf/GPO-WMD.pdf.

"Concern over DHS Move to Create Giant Information Databank." Homeland Security News Wire, December 8, 2011, http://www.homelandsecuritynewswire.com/dr20111208-concern-over-dhs-move-to-create-giant-information-databank.

Crumpton, Henry A. "Intelligence and Homeland Defense." In *Transforming U.S. Intelligence*, edited by Jennifer E. Sims and Burton Gerber, 198–219. Washington, DC: Georgetown University Press, 2005.

Dilanian, Ken. "U.S. Counter-Terrorism Agents Still Hamstrung by Data-Sharing Failures." *Los Angeles Times*, October 4, 2010, http://articles.latimes.com/2010/oct/04/nation/la-naw-terrorism-data-100510.

A DHS Intelligence Enterprise: Still Just a Vision or Reality? Hearing Before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security, 111th Cong. (May 12, 2010) (statements of Caryn Wagner, Under Secretary of Homeland Security for Intelligence and Analysis, and Jane Harman, Chair of the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security).

Dombey, Daniel. "U.S. Intelligence: Tribal Warfare." *Financial Times*, March 12, 2010, http://www.ft.com/intl/cms/s/0/0a252d6e-2c6e-11df-be45-00144feabdc0.html#axzz2MoM0XvR7.

Garicano, Luis, and Richard A Posner. "What Our Spies Can Learn From Toyota." *Wall Street Journal Op-Ed*, January 12, 2010, http://online.wsj.com/article/SB10001424052748704586504574654261998633746.html.

Hulnick, Arthur S. "Intelligence Reform 2008: Where to from Here?" *International Journal of Intelligence and CounterIntelligence* 21 (2008): 621–34.

National Security Preparedness Group. *Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations*. Washington, DC: Bipartisan Policy Center, September 2011.

Perrow, Charles. "The Disaster after 9/11: The Department of Homeland Security and the Intelligence Reorganization." *Homeland Security Affairs* II (2006): 1–32.

The Role of DHS in the IC: A Report by the Aspen Institute. Hearing Before the Subcommittee on Terrorism, HUMINT, Analysis, and Counterintelligence of the Permanent Select Committee on Intelligence, 112th Cong. (January 18, 2012) (statements of Rep. Sue Myrick, Chairwoman of the Subcommittee on Terrorism, HUMINT, Analysis, and Counterintelligence of the House Permanent Select Committee on Intelligence, and Rep. Mike Thompson, the subcommittee's Ranking Member).

Transportation Security Information Sharing: Stakeholders Generally Satisfied but TSA Could Improve Analysis, Awareness, and Accountability, GAO-12-44, November 2011, http://www.gao.gov/assets/590/586430.pdf.

Treverton, Gregory F. *Reorganizing U.S. Domestic Intelligence: Assessing the Options*. Santa Monica: RAND, 2008.

U.S. Department of Homeland Security, Office of the Inspector General. *DHS' Efforts To Coordinate and Enhance Its Support and Information Sharing With Fusion Centers*, OIG-12-10, November 2011, http://www.oig.dhs.gov/assets/Mgmt/OIG_12-10_Nov11.pdf.

U.S. Government Accountability Office. *Information Sharing: DHS Could Better Define How It Plans to Meet Its State and Local Mission and Improve Performance Accountability*, GAO-11-223, December 2010, http://www.gao.gov/assets/320/314114.pdf.

U.S. Library of Congress. Congressional Research Service, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, by Todd Masse. CRS Report RL33616.Washington, DC: Office of Congressional Information and Publishing, August 18, 2006.

U.S. Senate. *Federal Support for and Involvement in State and Local Fusion Centers*. Majority and Minority Staff Report for the Permanent Subcommittee on Investigations of the Committee on Homeland Security and Governmental Affairs, October 3, 2012, http://cdn.govexec.com/media/gbc/docs/pdfs_edit/100312cc1.pdf.

Zegart, Amy B. *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. Princeton: Princeton University Press, 2007.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California