Connecting the Dots:
Enduring Challenges In the Nation's Information Sharing Environment

A Monograph

By

COL John C. Valledor

United States Army

School of Advanced Military Studies

United States Army Command and General Staff College

Fort Leavenworth, Kansas

AY 09-10

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	12-05-2010	AOASF Monograph, August 2009-May 2010

4. TITLE AND SUBTITLE
Connecting the Dots: Enduring Challenges in the Nation's Information Sharing Environment

5. FUNDING NUMBERS

6. AUTHOR(S)
COL John C. Valledor (U.S. Army)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Advanced Military Studies Program
250 Gibbon Avenue
Fort Leavenworth, KS 66027-2134

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
1 Reynolds Avenue
Fort Leavenworth, KS 66027

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
CGSC

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***

This study asks, what are the enduring challenges that continue to hinder stakeholders in the information sharing environment from effectively sharing terror-related information to prevent future catastrophes.

Four enduring tensions stymie relevant stakeholders from effectively sharing terrorism-related information. First, fine-tuning of the nation's information sharing environment lost momentum in a transition year where policymakers where distracted by bitter partisan politics and competing domestic policy agenda items. Second, sub-optimization of the information sharing environment contributed to a failure to address emerging threats, especially an increasing number of self-radicalized, "lone wolf" conspirators. Third, the current information sharing environment remains over saturated frustrating efforts by stakeholders in the information sharing environment from effectively retrieving relevant, actionable information on looming terror plots. Finally, ad hoc agreements between federal agencies, specifically Defense and the Justice, are unclear, lack effective standards and are too informal to mandate action.

Applying the U.S. Army's design doctrine, this study explores the nature of the information sharing environment, defined as both a complex adaptive supra-system and wicked problem. It then compares understanding of the homeland security system against two terror-related attacks from 2009, the Fort Hood rampage and the Christmas Day attack respectively.

15. SUBJECT TERMS
Information Sharing Environment, Christmas Day Attack, Fort Hood Rampage, U.S. Army Design Doctrine, National Information Sharing Strategy, Homeland Security

15. NUMBER OF PAGES
74

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	Unclassified

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

COL John C. Valledor

Title of Monograph: Connecting the Dots: Enduring Challenges in the Nation's Information Sharing Environment

Approved by:

_____ Gerald S. Gorman, Ph.D.	Monograph Director
_____ Peter J. Schifferle, Ph.D.	Monograph Reader
_____ Stefan J. Banach, COL, IN	Director, School of Advanced Military Studies
_____ Robert F. Baumann, Ph.D.	Director, Graduate Degree Programs

ABSTRACT

CONNECTING THE DOTS: ENDURING CHALLENGES IN THE NATION'S INFORMATION SHARING ENVIRONMENT, by COL John C. Valledor, U.S. Army, 73 pages.

Since the horrific attacks of September 11, 2001, the nation has seen the largest expansion and reorganization of government since the National Security Act of 1947, transforming the nation's homeland security system around, amongst other things, an information sharing environment. Nearly a decade later this study asks, what are the enduring challenges that continue to hinder stakeholders in the information sharing environment from effectively sharing terror-related information to prevent future catastrophes.

This study posits that four enduring tensions continue to stymie relevant stakeholders from effectively sharing terrorism-related information. First, much needed fine-tuning of the nation's information sharing environment lost momentum in a transition year where policymakers where distracted by bitter partisan politics and competing domestic policy agenda items. Second, sub-optimization of the information sharing environment contributed to a failure to address emerging threats, especially those involving an increasing number of self-radicalized, "lone wolf" conspirators. Third, the current information sharing environment remains over saturated with too many incompatible information systems, frustrating efforts by stakeholders in the information sharing environment from effectively retrieving relevant, actionable information on looming terror plots. Finally, ad hoc agreements between federal agencies, specifically Defense and the Justice, are unclear, lack effective standards and are too informal to mandate action.

Applying the U.S. Army's emerging design doctrine, this study explores the nature of the information sharing environment, defined here as both a complex adaptive supra-system and wicked problem. The study applies design's cognitive environmental, problem and solution frames as the lens for gleaning greater understanding of the true nature of the ill-structured problem. It then compares understanding of the homeland security system against two terror-related attacks from 2009, the Fort Hood rampage and the Christmas Day attack respectively. The resulting bi-partisan investigations and Congressional hearings since provide invaluable insights into existing failures in the system that should serve as a guide to the nation's policy makers to tackle the nation's exigent challenge—protecting America from further terrorist attacks.

The Fort Hood rampage and Christmas Day attack should serve as a clarion call to the nation's policy makers compelling them to complete the transformation of the nation's homeland security system and eliminate the newly exposed gaps as their top priority. Congress must update and amend existing homeland security statutes and mandate the development of more formal relationships between the nation's Departments and agencies, especially between Defense and Justice. Consistent with its oversight function, Congress should ensure that formal relationships between the information sharing environment stakeholders are in fact leading to increased thwarting of known and emerging terror plots and support the Program Manager for the Information Sharing Environment in streamlining proliferation of government-wide database systems.

TABLE OF CONTENTS

INTRODUCTION AND OVERVIEW

> The U.S. Government had sufficient information to have uncovered this plot and potentially disrupt the Christmas Day attack. But our intelligence community failed to connect those dots, which would have placed the suspect on the no-fly list.
>
> —President Barack Obama, January 5, 2010[1]

At 12:33 p.m. Central Standard Time, the Obama's are enjoying a workout at the Kaneohe Bay U.S. Marine Corps Base near the President's childhood home in Kailua, Hawaii, their first holiday vacation of his volatile first year in office.[2] Back in the continental United States, Americans are still digging out from an unusually harsh series of back-to-back winter storms that left North America blanketed in deep snow pack. Unlike past years, the Department of Homeland Security does not elevate the, now familiar, national terror alert level. The National Homeland Security Advisory Level stands at "Yellow-Elevated."[3] Officially, there are no lights 'blinking red' in the nation's information sharing system, no alerts or warnings of looming terror attacks during the 2009-2010 holiday season.

---

[1]President Barrack Obama, Address, "Remarks Following a Meeting on Improving Homeland Security," *U.S. Government Printing Office*, (January 5, 2010). http://www.gpoaccess.gov/presdocs/2010/DCPD-201000005.pdf (accessed January 10, 2010).

[2]Phillip, Elliot, "Quiet Christmas Day for Obama's in Hawaii," *The Seattle Times*, December 25, 2009. http://seattletimes.nwsource.com/html/nationworld/2010598353_obamaday26.html (accessed January 9, 2009).

[3]Alaska Division of Homeland Security and Emergency Management, *Situation Report 09-358*, (December 24, 2009). http://fc.ak-prepared.com/dailysitrep/I011FBFA4.0/DHS&EM%20Daily.%20SITREP%2009-358.pdf (accessed March 15, 2010).

Meanwhile, in the frigid December skies over Canada, Flight 253, a Northwest Airlines Airbus A330, on its last hour of a nine-hour-long transatlantic flight that originated in Holland, commences its final descent from a cruising altitude of 36,000 feet. On board are 279 passengers, eight flight attendants and three pilots.[4] The plane's captain announces over the intercom that they are initiating their final approach into Michigan's Detroit Metropolitan Airport. This procedure occurs thousands of times a day in the skies overhead, its purpose being to alert the flight crew to prepare the cabin and passengers for landing in the remaining twenty-minutes of flight. Suddenly and without warning, the fire indicator light in the cockpit's instrument panel illuminates. The captain reaches for his onboard intercom handset to verify the cabin's status with his cabin crew. His eyes widen and jaw drops as he turns and stares at his co-pilot in pure disbelief. The sounds emanating from his handset revealing a scene of utter panic as passengers and crewmembers are loudly screaming, *"Oh my God, the plane's on fire!"* Fifteen seconds later, the plane's port side windows, just above the twinjet's mid-wing fuel tanks flash and erupt in a bright yellow and orange, blazing ball of fire, instantly breaching the fuel tanks and severing the plane's wings from the fuselage. The Airbus A330's high-tech, composite carbon-fiber fuselage splinters and ruptures into two separate pieces.[5] Losing its fight with gravity, the nose end immediately drops to earth. The plane's midsection, still travelling in excess of 280 knots from the thrust of its two Rolls-Royce Trent engines, continues forward into a frightening barrel roll, spilling its

[4]"PHOTOS Passengers help foil Christmas Day attack on Detroit-bound plane; terrorist charged," *Naplesnews.com*, (December 26, 2009), 1-5. http://www.naplesnews.com/news/2009/dec/26/terrorist-attempt-passengers-help-foil-christmas-d/ (accessed March 4, 2010).

[5]Find out more about the Airbus A300-series jets at http://www.airbus.com/en/aircraftfamilies /a330a340/a330-300/specifications/ (accessed January 10, 2010).

contents into the thin, sub-zero skies—a scene eerily similar to the 1996 Trans World Airlines Flight 800 catastrophe. The blast effects were amplified by the sudden depressurization of the plane's cabin nearly three miles above the earth. Canadian citizens below, going about their jubilant Christmas Day rituals, have no idea that they are about to be showered, like the 1988 Lockerbie, Scotland catastrophe, by thousands of pieces of falling debris, consisting of a destroyed airliner, bits of burning luggage and lifeless bodies horribly ripped apart.

Hours later, the Al Jazeera television network broadcasts a taped recording from shadowy members of the offshoot extremist group, al Qaeda in the Arabian Peninsula, claiming credit for perpetrating the Christmas Day attack in the skies over North America, justifying their deadly act to "avenge U.S. attacks on fellow militants in Yemen."[6]

This horrific scenario, appalling as it sounds, thankfully did not fully occur, at least not the elements describing the plane's disintegration over U.S. and Canadian airspace. However, most of the facts and details associated with its depiction are real, as this December 25, 2009, failed attack on the nation's air transportation sector nearly succeeded. This particularly disturbing terrorist attack, occurring at a unique moment in history, President Obama's first year in office, serves as a reminder that al Qaeda and its offshoot affiliates remain ideologically committed on perpetuating their self-declared global *jihād* well into the second decade of the twenty-first-century. To be repeated in the future by more spectacular attacks of equal or greater audacity, this recent attack is consistent with Osama Bin Laden's February 23, 1998 *fatwā,* an Islamic term meaning

[6]"Al Qaeda Claims Christmas Day US Flight Bomb Plot," *BBC News*, (December 28, 2009), http://news.bbc.co.uk/2/hi/middle_east/8433151.stm (accessed March 4, 2010).

"legal opinion."[7] This fatwa avowed Bin Laden's intention to destroy the United States and its allies around the globe by declaring, "We—with Allah's help—call on every Muslim who believes in Allah and wishes to be rewarded to comply with Allah's order to kill Americans and plunder their money whenever and wherever they find it."[8]

Sadly, close to a trillion dollars exhausted in America's treasure as well as the nation's largest post Cold War era consolidation of government could not prevent this terror-related attack, along with six others, from occurring in 2009. The layered defense framework consisting of the federal Air Marshal Service, the nation's expanded terror watch listing system, intrusive and high-tech passenger screening procedures both at home and abroad, and most telling, the nation's vastly reorganized intelligence and information sharing enterprises could not prevent this attack. All of the purportedly integrated layers of homeland protection toppled like a line of dominoes. In the end, as the nation learned on September 11, 2001, from the tragedy of the heroic passengers in United Flight 93, it took the low cost yet incredibly heroic actions of a young Dutch citizen named Jasper Schuringa, the apparent final line of defense, to foil this attack. He had the courage and wherewithal to overcome the panic-driven paralysis of fellow passengers onboard his ill-fated airliner and promptly acted to prevent a would-be suicide bomber from successfully detonating his concealed weapon of mass destruction.[9] In the first decade of the twenty-first-century, branded at the very beginning by the horrific

---

[7]Annemarie Schimmel, *Islam: An Introduction*, (Albany, NY: State University of New York Press, 1992), 63.

[8]Walter Laqueur, ed., *Voices of Terror: Manifestos, Writings, and Manuals of Al Qaeda, Hamas, and other Terrorists from Around the World and Throughout the Ages*, (New York, NY: Reed Press, 2004), 412.

[9]Sarah Netter, "Jasper Schuringa Yanked Flaming Syringe out of Abdulmutallab's Pants," *ABC News, Good Morning America*, (December 28, 2009). http://abcnews.go.com/GMA/northwest-flight-253-hero-yanked-flaming-syringe-abdulmutallab-pants/story?id=9432099 (accessed March 6, 2010).

events of September 11, 2001, and now its tail end by this foiled terrorist attack, Americans are again asking, how could this event have happened?

To their credit, Congress and the executive branch have done a great deal to improve the safety and security of Americans following the surprise attacks of September 11, 2001. In response to these traumatizing attacks, America fought back, holding al Qaeda and its violent extremist allies accountable wherever they plot, train and fight, as well as ushered in sweeping changes to the way the nation protects the homeland. Coming to grips with the notion of strategic surprise by terrorism as a new form of global warfare, the nation initiated a sobering bipartisan review—*the National Commission on Terrorist Attacks Upon the United States,* known as the 9/11 Commission. The 9/11 Commission's report revealed numerous failures that collectively contributed to this tragedy and subsequently proposed forty-one separate recommendations to prevent them from happening again. Among the many failures and missed opportunities cited, the report highlighted the problem of "watchlisting [sic]," "information sharing" or of "connecting the dots." The report concluded, "The biggest impediment to all source analysis—to a greater likelihood of connecting the dots—is the human or systematic resistance to sharing information."[10] Aggressively acting on the collective findings and recommendations of, not only, the 9/11 Commission, but the subsequent Weapons of Mass Destruction Commission and the Markle Foundation Task Force, a national

[10]The 9/11 Commission Report, *Final Report of the National Commission on Terrorist Attacks Upon the United States.* (Washington, D.C.: U.S. Government Printing Office, 2004), 417. http://www.9-11commission.gov/report/911Report.pdf (accessed August 29, 2009). Hereafter cited as *9/11 Commission Report*.

information sharing environment was formally established and incrementally refined.[11] Further, the impact of the 9/11 Commission's findings and recommendations on Congress and the Oval Office, coupled with a genuine fear of re-attack, catalyzed the largest consolidation of federal agencies and reorganization of the intelligence community since the National Security Act of 1947.[12] Nevertheless, nearly a decade later, the transformation of the information sharing environment remains a work in progress.

The nation's political leaders are often quick to point out that since the trauma of September 11, 2001, the nation has not suffered repeated attacks on its home soil, especially spectacular attacks that are the hallmarks of al Qaeda's global terror franchise. However, in light of a series of alarming terror-related events in 2009, conspicuously an executive branch transition year, there is growing concern that the nation's homeland security enterprise may have in fact failed to anticipate threat groups that continually innovate. It appears as if violent extremist organizations are increasingly turning to the tactic of using "homegrown" attacks from within the nation's borders by lone, "radicalized" American citizens. In the wake of these worrisome terror-related incidents and nearly a decade's worth of incremental improvements to the information sharing system, this study asks, what are the enduring challenges that continue to hinder

[11]Zoe Baird, and Jim Barksdale, "Nation at Risk: Policy Makers Need Better Information to Protect the Country," *The Markle Foundation Task Force on National Security in the Information Age*, (March 10, 2009), 4. http://www.markle.org/downloadable_assets/20090304_mtf_report.pdf (accessed January 14, 2010).

[12]National Security Act of 1947, P. L. No. 235-80, 61 Stat. 495 (codified as amended at 50 U.S.C. §§401 *et seq.* (2000 and Supp. IV 2004). http://intelligence.senate. gov/nsaact1947.pdf (accessed December 12, 2009).

stakeholders in the information sharing environment from effectively sharing terror-related information to prevent future catastrophes?

The lack of information sharing between federal, state, local authorities and the private sector, especially about individuals with ties to terror groups, was the cornerstone of the 9/11 Commission's findings. It was apparent to the 9/11 Commission's panel members that interconnected data bits of information regarding the looming 9/11 conspiracy resided within disparate government agency databases as well as private sector data sources. The fundamental problem was not a lack of information, rather that no primary agency or decision maker had enough integrated information about fledgling terror-related conspiracies to form a mosaic-like aggregate threat picture and act to prevent them. This failure was highlighted in the now infamous July 2001 "Phoenix Memo" in which Federal Bureau of Investigation agents sent a memorandum to their headquarters trying, but failing to draw attention to "potential Islamic terrorists attending pilot training in the United States."[13] Thereafter, the nation branded this problem as "connecting the dots." Facing what amounted to the nation's first strategic shock of the twenty-first-century, Congress quickly intervened by enacting new and far-reaching legislation enabling the United States government, with new powers, to break down long standing administrative barriers or "walls" between federal foreign intelligence and domestic law enforcement agencies.[14] Equally, Congress followed the lead of the former Bush Administration and supported the need for establishing an information sharing

[13]George Tenet with Bill Harlow, *At the Center of the Storm, My Years at the CIA*, (New York: Harper Collins Publishers, 2007), 192.

[14]Jeremy Shapiro, "Managing Homeland Security, Developing a Threat-Based Strategy," *Brookings Institution*, (February 28, 2007), 7. http://www.brookings.edu/papers/ 2007/0228terrorism_ shapiro_Opp08.aspx (accessed October 30, 2009).

environment, linking federal government databases with those of state, local and tribal authorities, with the goal of improving what the 2010 Quadrennial Homeland Security Review now labels the "shared awareness of risks and threats."[15] Today, the sharing of terrorism-related information occurs within the independent sharing environments of five designated, federal communities of interest: "the Intelligence Community; Law Enforcement; Defense; Homeland Security; and Foreign Affairs."[16]

Conversely, some prominent "watchdog" organizations became increasingly nervous by the same sweeping legislation that led to the breakdown of longstanding interagency walls, specially the passage of the controversial October 2001, USA Patriot Act.[17] Fearing abuse of the government's new powers, especially warrantless surveillance of private citizens under the banner of preemptive security, the American Civil Liberties Union (ACLU) and the Center for Democracy and Technology (CDT) have consistently challenged this statute on the grounds that it violates the fundamental civil liberties and freedoms of citizens in both the public and cyber domains. Indicative of their much publicized signature concerns the ACLU in 2003 published an analysis of the USA Patriot Act in which they charged, "Limits on police spying approved by federal courts

---

[15]U.S. Department of Homeland Security, *Quadrennial Homeland Security Review (QHSR) Report: A Strategic Framework for a Secure Homeland*, (Washington, D.C.: February 2010), 65. http://www.dhs.gov/xlibrary/ assets/qhsr_report.pdf (accessed March 11, 2010). Hereafter cited as QHSR 2010.

[16]The White House, *National Strategy for Information Sharing(NSIS): Successes and Challenges in Improving Terrorism-Related Information Sharing*, (Washington, D.C.: October 31, 2007), 10. Hereafter, this study will refer to this reference as the NSIS and the members of these communities of interest by their short titles e.g., Intelligence Community, Justice, Defense, Homeland Security and State and refer to subordinate agencies by their acronyms e.g., TSA, FBI.

[17]"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001," P. L. No. 107-56, 115 Stat. 272, October 26, 2001. http://frwebgate. access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_ laws&docid=f:publ056. 107.pdf (accessed December 2, 2009).

will be swept aside, freeing state and local police to spy on political and religious activity, thus violating citizens' First Amendment rights (sec. 312)."[18]

This study posits that in 2009, momentum was lost transforming the nation's information sharing environment. Arguably, the primary focus of Washington lawmakers and the White House in particular, has been the formation of a newly elected administration and governance under President Obama's signature agenda, amidst both an ideologically polarized electorate and an unending stream of global national security challenges.

In the first year of the Obama administration, focused efforts by policy makers mostly proceeded on three separate fronts. First, was averting further economic disaster in the wake of a deep and prolonged global recession. Second, was managing a fragile peace and responsible drawdown strategy from the war in Iraq, while simultaneously setting a new strategy for a protracted and increasingly problematic parallel war in Afghanistan. Third, was the passage of an ambitious and highly divisive trillion dollars-plus, national-level entitlement program—universal healthcare for Americans. Furthermore, during 2009, these three broad fronts diverted the attention of policymakers and the public from addressing the nation's underlying vulnerabilities to terrorist attack. The nation may have exposed a vulnerable flank that al Qaeda and its offshoot affiliates simply exploited. Conversely, in the Defense domain, the nation's military remained on a long-drawn-out war footing making steady progress pursuing and eroding al Qaeda networks across the globe. In the Operation *Enduring Freedom* theater of operations one

[18]Timothy J. Edgar, "How "Patriot Act 2" Would Further Erode the Basic Checks on Government Power That Keep America Safe and Free," *American Civil Liberties Union (ACLU)*, (March 20, 2003), 4. http://www.cdt.org/ security/patriot2 /030320aclu.pdf (accessed March 25, 2010).

measure of progress against al Qaeda-inspired militants is seen by the increasingly effective campaign of using unmanned U.S. Predator strikes against the Haqqani network. This militant group being one of several Afghani Taliban groups operating in safe havens along Pakistan's volatile northwest tribal frontier.[19] However, efforts to deny al Qaeda militants and their affiliate's safe havens from which to plot future attacks on the homeland from failed or failing states have defied common wisdom. Instead of diminishing the prospects of follow-on attacks, they seem to be inspiring an ever-increasing stream of reprisal attacks against the homeland. As a result, the nation appears more vulnerable than in the past. No matter how successful efforts to erode al Qaeda networks appear, it is becoming increasingly apparent that the nation simply cannot bomb a growing list of enemies into submission.

Some question if the nation's efforts to pursue and erode al Qaeda networks across the globe have resulted in the nation gaining the breathing room needed to improve its collective security framework. In his book, *Protecting the American Homeland, One Year On*, Michael O'Hanlon suggested that the nation "squandered precious time brought about by the disruption of al Qaeda in Operation Enduring Freedom that should have been used to prepare ourselves against the next strike."[20] Similarly, eight years later and despite President Obama's increased military efforts in Afghanistan, it appears as if both he and Congress may have simply lost valuable time

[19]"The Resurgence of al-Qaeda, the Bombs that Stopped the Happy Talk," *The Economist*, (January 30th-February 5th, 2010), 69-71.

[20]Michael E. O'Hanlon, with Peter R. Orszag, Ivo H. Daalder, I. M. Destler, David L. Gunter, James M. Lindsay, Robert E. Litan, and James B. Steinberg, *Protecting the American Homeland, One Year On*, (Washington, D.C.: Brookings Institution Press, 2002), x-xi.

entrenched and distracted by toxic partisan politics battles, interfering with the nation's exigent challenge—protecting America from further terrorist attacks.

In President Obama's first year in office, the nation experienced seven domestic terror-related events, two of them resulting in the deaths of Americans. In June 2009, an attack against a Little Rock, Arkansas recruiting station by a self-radicalized Muslim convert, Abdulhakim Muhammad, resulted in the killing of an active duty Army soldier and wounding of another.[21] This particular event became the harbinger of worse things to come. In early November, an alleged self-radicalized, U.S. Army psychiatrist, cut down clusters of soldiers at a Fort Hood, Texas Soldier Readiness Center, killing thirteen and wounding forty-three others.[22] Then, as was introduced earlier, on December 25, 2009, a courageous traveler foiled a Nigerian student, travelling with a U.S. approved multiple-entry visa, as he attempted to detonate an improvised explosives device sewn into his underwear. As in the notorious "Shoe Bomber" plot, al Qaeda's aim was to bring down a Detroit-bound transatlantic airliner with all onboard.[23]

Moreover, in each instance, the post-mortem analyses of the available information leading up to these separate terror plots exposed serious chinks in the armor of the supposedly integrated homeland security efforts. These three particular events, although separated by time and scope, share a common worrisome thread—data bits of

---

[21]Steve Barnes, and James Dao, "Gunman Kills Soldier Outside Recruiting Station," *New York Times*, (June 2, 2009), 1. http://www.nytimes.com/2009/06/02/us/02recruit.html (accessed January 10, 2010).

[22]U.S. Department of Defense, Independent Review Related to Fort Hood, *Protecting the Force: Lessons Learned from Fort Hood*, (Washington, D.C.: January 13, 2010), 1. http://www.defense.gov /pubs/pdfs/DOD-ProtectingTheForce-Web_Security_HR_13Jan10.pdf (accessed January 15, 2010). Hereafter cited as the DOD Independent Review.

[23]Elizabeth Williamson, "Obama Connects al Qaeda to Jet Plot," *Wall Street Journal*, (January 2, 2010), 1-2. http://online.wsj.com/article/SB126242308343313439.html?mod=rss_Today%27s_Most _Popular (accessed January 3, 2010).

information revealing indications and warnings of these emerging terror plots were present within the nation's information sharing environment. However, as the nation witnessed earlier in the decade, for myriad reasons the very agencies generously funded and charged with collecting, analyzing and disseminating the fused, "federally integrated" meaning of these data bits, inexplicably failed to "connect the dots." As before, local first preventers and responders, along with the nation's top officials, had to face an increasingly alarmed and infuriated public.

Of these three events, the Fort Hood rampage became such a lightning rod topic that the resulting public furor compelled the executive branch and Congress to initiate a series of investigations. In the days following the Fort Hood rampage public and media coverage of the carnage "marked the first time in seven weeks that a subject other than health care, the economy or Afghanistan registered as the No. 1 story in the news."[24] The re-exposure of the nation's homeland security enterprise failures, by subsequent bipartisan investigations and Congressional hearings, will again shed light on the state of effectiveness and cooperation by the relevant stakeholders in the information sharing environment. Not surprisingly, the systematic failure of federal agencies to share budding terror-related conspiracies is not new. Therefore, this study explores the following supporting questions to support its thesis, what happened to the sweeping changes put in place in the wake of the 9/11 attacks? What can the nation learn from these recent attacks to close the apparent gaps in the United States government's highly funded security apparatus? In a climate fraught with hyper-partisan politics, are course corrections in the much-needed evolution of the nation's information sharing

[24]Mark Jurkowitz, "The Army Base Massacre Dominates the Week," *Pew Research Center's Project for Excellence in Journalism (PEJ)*, (November 2-8, 2009), 1. http://www.journalism.org/index_report/pej_news_coverage_index_november_28_2009 (accessed January 12, 2010).

environment even doable? The answers are unclear; this study examines the nature of this ill-structured problem.

This study posits that pervasive and deep-rooted obstacles to information sharing still stand in the way of progress. Specifically, four enduring tensions continue to stymie the relevant stakeholders in the information sharing environment from effectively sharing terrorism-related information to prevent future terrorist catastrophes.

First, much needed fine-tuning of the nation's information sharing environment simply lost momentum during a political transition year where policymakers were utterly distracted by raw and bitter partisan politics and a competing domestic policy agenda. Beltway politics has evolved into a polarizing contact sport with an endless chorus of outrageous blowhard pundits and media elites stoking flames of discontent amongst polarized factions within the electorate. This brand of politics increasingly blurs the links between terrorism and national information sharing efforts. Too often, politicians use the fear of terrorist attacks as a political football, sensing a distracted executive branch; the opposition party viewed partisan attacks on the President's handling of botched terror-related conspiracies in 2009 as fair game. Such was the case when Maine's Republican Senator Susan Collins, a member of the Senate Committee on Homeland Security and Government Affairs, employed this tactic in her January 2010 weekly Republican National Committee radio address. Specifically citing the Christmas Day attack plot, she levied the charge that, "The Obama administration appears to have a blind spot when it comes to the War on Terrorism."[25] Her polarizing charge alluding to the notion that the Obama administration, focused mostly on setting its political footprint in a risk-riddled

[25]Susan Collins, Senator (R-ME), "Transcript: GOP Weekly Radio Address," RNC Blog, entry posted January 30, 2010. http://rncnyc2004.blogspot.com/2010/01/senator-susan-collins-weekly-republican.html (accessed January 30, 2010).

transition year, was overwhelmingly distracted. Most distressing, the 9/11 Commission made a particularly crucial recommendation specifically addressing the challenges associated with executive branch transitions of power.[26]

Second, sub-optimization of the information sharing environment, in its current state, contributed to the failure to address emerging threats, especially those involving an increasing number of radicalized, "lone wolf" conspirators. The recently published Independent Review related to the Fort Hood shooting revealed that Defense "force protection policies were not optimized for countering internal threats."[27]

Third, an information sharing environment saturated with countless incompatible information systems and databases, continues to frustrate efforts by stakeholders in the communities of interest from efficiently harvesting relevant, actionable information on developing threats. When it comes to measuring frustration within the law enforcement and intelligence communities Congress often gets an earful. In Congressional testimony before the House of Representatives Subcommittee of Intelligence, Information Sharing, and Terrorism Risk Assessment, one State Fusion Center official stated, "The next step would be to consolidate some of these sources [existing systems] into a coherent streamline manner so that analysts wouldn't have to check 10 websites to gather information."[28] In similar testimony, Russell M. Porter, Director of the State of Iowa Intelligence Fusion Center, Iowa Department of Public Safety, expressed his frustration

[26]*9/11 Commission Report*, 422.

[27]DOD Independent Review, 3.

[28]U.S. House of Representatives, Hearing before the Subcommittee on Intelligence Information Sharing, and Terrorism Risk Assessment, Committee on Homeland Security, *A Report Card on Homeland Security Information Sharing*, H. Rpt. 110-141, September 24, 2008, 26. http://homeland.house.gov /hearings/index.asp?ID=169 (accessed January 11, 2010). Hereafter cited as *A Report Card on Homeland Security*.

with not having a "single place to go for information," and having to "change 30 passwords every quarter."[29]

Fourth and finally, ad hoc agreements between federal agencies, specifically Defense and Justice, are unclear, lack effective standards and are too informal to mandate action.[30] Confusion still lingers in a dense, multi-layered system where jurisdictional issues between federal, state and local authorities still prevent integrated intervention efforts.[31]

Given the recently released U.S. Army's design doctrine, the following section in this study will apply its approach as the methodology for addressing the research question.

METHODOLOGY

> It [design team] needs to ask, "Why has this situation developed?" and "what does it mean?" or more simply, "what's the real story here?"
>
> —Stefan Banach, "The Art of Design, a Design Methodology"[32]

The goal of this study is to answer the question, "What are the enduring challenges that continue to hinder stakeholders in the information sharing environment from effectively sharing terror-related information to prevent future catastrophes?" This

[29]Ibid.

[30]DOD Independent Review, Finding Number 2.11, 19.

[31]*A Report Card on Homeland Security Information Sharing,* 41.

[32]Stefan Banach, and Alex Ryan, "The Art of Design, A Design Methodology," *Military Review* (April 30, 2009), 109. http://usacac.army.mil/CAC2/MilitaryReview/ Archives/English/MilitaryReview _20090430_art016.pdf (accessed January 12, 2010).

study applies the U.S. Army's emerging "design approach" to glean greater understanding of this ill-structured problem, challenge its existing paradigm, presumptions and wide-ranging set of strategies applied by the United States government to resolve its observed tendency of having multiple points of failure.

Why opt for a design approach? The U.S. Army has recently embarked on an institution-wide effort to improve cognitive understanding of conflict in the twenty-first-century—the application of "design" in doctrine. The Army learned from its initial experiences in Operation *Iraqi Freedom* that although the longstanding Military Decision Making Process has served the institution well, it might not be complete in enabling holistic understanding of complex or ill-structured problem sets. This is especially so when addressing the full spectrum of threats the nation faces. The Army faced an interesting conundrum, the Military Decision Making Process was a proven methodology to solve problems right, but was not necessarily solving the right problems. Therefore, the objective of design is to "create a systematic and shared understanding of complex operational problems to enable a broad approach to its resolution."[33] With respect to the myriad of challenges associated with the nation's information sharing environment, truly understanding the associated dynamics, tensions and underlying issues make it worth testing under the Army's design approach. The information sharing environment's multi-layered system of seemingly complimentary jurisdictional authorities readily identifies it as a complex adaptive system; system being the operative term used throughout this

[33]U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-5-500, *Commander's Appreciation and Campaign Design* (CACD), (Fort Monroe, VA: Headquarters, TRADOC, 28 January 2008), 4-5. Hereafter cited as TRADOC PAM 525-5-500.

study.[34] These individually complex, multi-level, flexibly coordinated supra- and substructures are connected by U.S. law and national policy to function as an integrated whole in what an exponent of systems theory, Ervin Laszlo, labels "social system holarchies."[35] In 2008, highlighting the depth of scale in this problem, Sheriff Baca, from the Los Angeles County Sherriff's Department, acknowledged before Congressional testimony that there are "over 19,000 law enforcement agencies that need to be federated into Joint Regional Intelligence Centers."[36]

Equally, defining the difficult challenges associated with correcting this system where there is widespread disagreement on ways of solving the problem, defining desired end states, and achieving them further categorizes the information sharing environment as a "wicked problem."[37] The term "wicked problems" has been adopted by U.S. Army design doctrine. This term was originally coined by planning theorists Horst Rittel and Melvin Webber.[38] This study applies the Army's design approach as the lens for examining the nation's information sharing environment—both a complex adaptive system and a wicked problem. As such, the information sharing environment problem set

[34]Ludwig von Bertalanffy, *General System Theory: Foundations, Development, Applications*, Revised Edition, (New York, NY: George Braziller Inc., 1993), 252. The author defines a system as, "a series of elements standing in interrelation among themselves and with the environment."

[35]Ervin Laszlo, *The Systems View of the World: a Holistic Vision for our Time*, (Cresskill, NJ: Hampton Press Inc., 1996), 51.

[36]*A Report Card on Homeland Security Information Sharing*, 44-45.

[37]TRADOC PAM 525-5-500, 9.

[38]Horst W.J. Rittel and Melvin M. Webber, "Dilemmas in the General Theory of Planning," *Policy Sciences 4*, (1973), 161. http://www.metu.edu.tr/~baykan/arch467/Rittel+Webber+Dilemmas.pdf (accessed March 15, 2010).

will be explored using design concept's three cognitive frames of reference: the operational environment, the problem, and the solution, or design concept.[39]

The operational environment frame will be examined utilizing a set of drawings (see Appendix B, Illustrations) in this study, applying a "three-phase process of formulating the mess: searching, mapping and telling the story."[40] The searching phase uses a drawing as a tool, of a snapshot in time, of the current observed system, describing the "structural, functional and behavioral" aspects as well as the associated obstructions and system dynamics. The subsequent system-mapping phase, traces the lines of interactions between the system's stakeholders and their emergent themes. The telling the story phase, involves packaging the emergent messages that are associated with the mess to create shared understanding of the current reality including "what is at stake, influence and of interests to the relevant stakeholders."[41] Properly applied, the operational environment frame bounds the study's inquiry into the "observed and desired systems with the associated risks and tensions that can lead to achieving an undesired system."[42] The tensions between the observed, desired and undesired systems reveal the system's "logic of transformation and system of opposition" that in turn, reveal areas of intervention as well as tensions worthy of exploiting.

The problem frame is a refinement of the environmental frame that enables identification of specific areas of intervention that, in design theory, should reveal

---

[39]Banach, 109.

[40]Jamshid Gharajedaghi, *Systems Thinking, Managing Chaos and Complexity: a Platform for Designing Business Architecture*, (Burlington, MA: Elsevier Inc., 2006), 132-135.

[41]Ibid., 140.

[42]U.S. Army Field Manual-Interim (FMI) 5-2, *Design (Draft)*, (Washington, D.C.: Headquarters, Department of the Army, 20 February 2009), 20-23. Hereafter cited as FMI 5-2.

potential levers for nudging the system from the observed to the desired state. The focus of analysis in this frame centers on defined tensions and the recommended actions needed to achieve the system's "logic of transformation."[43] The differences between the observed and desired system states helps define the true problem at play. The problem frame's drawing and associated narrative should expose opportunities for application of appropriate strategies that are relevant to the system's stakeholders and their associated interrelationships.

The solution frame enables understanding of why the desired system differs from the observed system. Ideally, the design concept applies a broad array of applicable strategies to organize the efforts of the system's actors toward achieving the desired state.[44] This study explores existing, real world "solutions" that have been applied to date in the form of national-level statutory and regulatory policy, added system infrastructure, as well as increased resourcing to achieve the desired system.

Better understanding of the information sharing environment's stakeholders and their interrelationships is gleaned by referencing the personal views and insights of key 'system insiders,' former Federal Department leaders: George Tenet, former Director of Central Intelligence as well Tom Ridge and Michael Chertoff, both former Department of Homeland Security Secretaries. Their recently published memoirs provide colorful perspectives of the tensions that exist between the nation's federal departments, Congress and the executive branch, all executing the provisions of published national strategies to deter, prevent and defeat terrorism and further attacks against the homeland.

Finally, this study integrates two recent terror-related incidents—the Fort Hood

[43]Ibid., 23-24.

[44]Ibid., 25.

rampage and the Christmas Day attack and their associated investigations, findings and recommendations as relevant case studies supporting this study's thesis. These case studies are timely and relevant examples of real-time incidents revealing fissures present in the information sharing environment. Further, both case studies provide valuable insights into the efficacy of the mitigation strategies applied in the form of policy, resources and continued evolution of the nation's overarching security apparatus. The Fort Hood rampage reflects how the nation's information environment, a binary system, uses 'bottom-up' or internal intelligence inputs to feed the fusion cycle in the system. Conversely, the Christmas Day terror plot illustrates the relative effectiveness of the nation's 'top-down' or external intelligence fusion process. The design drawing will depict how the system receives and fuses intelligence information from internal and external sources and compares them to what actually happened in the two case studies.

Much of the terror-related information and intelligence shared and resident in the nation's information sharing environment is classified secret or higher by the owning agencies to protect sources and methods; however, no classified information was used in supporting the study's thesis, research methodology or conclusions. In fact, all of the material cited in support of the study's thesis is commonly available in the unclassified public information domain.

The study acknowledges that perfect, government-wide information sharing is not a panacea for total homeland security. When it comes to attacks against the homeland, the nation's enemies simply have to get it right once, while the hard working, unsung heroes of the sixteen separate agencies that make up the Intelligence Community are expected to be correct about pending attacks, 100 percent of the time. As the world

witnessed on the December 30, 2009 attack against CIA operatives in Afghanistan, highly courageous Intelligence Community members continue to put their lives on the line to protect the nation.[45]

THE ENVIRONMENTAL FRAME

> One FBI official told me, 'if you need to know it, we're going to tell you, but we can tell you right now, you'll never need to know it.'
>
> —BGen (Ret.) Matthew Broderick, Director DHS Operations Center[46]

Where does one begin to map out a complex adaptive supra-system, its observed dynamics and underlying tensions that, if leveraged appropriately, have the potential to alter its course from observed to desired state? This study begins its investigation of this ill-structured problem using a 'center-out' approach, dissection fashion, to explore the dynamics and opportunities at play. With that as a starting reference point, the depiction of the environmental frame focuses on answering six supporting questions. The questions are as follows:

- What is the underlying framework of this system?
- Who are the relevant stakeholders in this complex adaptive system?

[45]Lisa Curtis, with Matt Mayer, Jena Baker McNeill, and Charles Stimson, "Christmas Day Terror Plot Highlights Need to Sharpen Intelligence System," Web Memo No., 2751, *The Heritage Foundation*, (January 8, 2010), 2. http://www.heritage.org/Research/NationalSecurity /wm2751.cfm (accessed March 4, 2010).

[46]Tom Ridge with Larry Bloom, *The Test of Our Times: America Under Siege and How We Can Be Safe Again*, (New York: Thomas Dunne Books, 2009), 162. Former DHS Secretary, Tom Ridge, illustrates a frustrating culture of competition amongst national level Departments. In the memoir's Chapter labeled, "*Matthew Broderick's Day Off*," he recounts a discussion between the former DHS Operations Center Director and a top official recalling that the FBI was "almost never forthcoming" regarding information sharing and collaboration amongst domestic agencies.

- What is the medium for exchanging information between the relevant stakeholders?
- What statutory, regulatory or policy-driven authorities govern the behavior and functions of the system's relevant stakeholders?
- What extra environmental factors shape the behavior of the relevant actors and define its overall system tendency?
- What is the potential of leveraging the system's existing dynamics, tensions and momentum to redirect its trajectory toward the desired state?

Figure 1 (Appendix B) is the design analysis drawing depicting the information sharing environment as it is—a complex adaptive supra-system. Their departmental or agency seal serve as nodal visual reference points represent the system's relevant actors and stakeholders. In the drawing, the lines and arrows connecting these nodes express the observed relationships and reflect its function within the five communities of interest. Finally, the drawing's canvas overlays the multiple layers of government at play, from foreign partners, federal, state, local, tribal as well the private sector using pastel shading as the background palette. Generally, terror-related information continually enters this binary system from two directions. Top-down, or external terror-related information and intelligence enters the system from abroad via the nation's vast network of foreign intelligence partners. One notable partner being the International Criminal Police Organization (INTERPOL), depicted on the top right corner of the drawing. The United States has been an INTERPOL partner since 1923 and along with 187 other member

countries assists its Fusion Task Force in sharing information and investigating global terrorism-related cases.[47]

Bottom-up, or internal sharing of domestic terror-related information and intelligence, depicted in the lower left corner of the drawing, enters the system as observed and reported suspicious activity reports (SAR) or serious incident reports (SIR) by the greater public, private sector entities, media organizations or the local law enforcement community.[48] Information entering this binary system is not an either/or proposition, on any given day, the system dynamically churns and fuses information from foreign as well domestic sources simultaneously, again revealing the complexity and difficult challenges associated with the nation's homeland security and intelligence communities.

Forming a pentagon, the center of the drawing depicts the five communities of interest in the information sharing environment. At the core of this environment is the National Counterterrorism Center, currently led by its Director, Michael E. Leiter and established by President Bush on August 27, 2004 under Executive Order 13354. The National Counterterrorism Center became the "primary organization" charged with analyzing and integrating all intelligence pertaining to terrorism. Addressing the greater public's fear of an unbounded 'big brother' state, President Bush subsequently issued Executive Order 13356 to improve information sharing activities in ways that "protect the

[47]International Criminal Police Organization (INTERPOL), *Terrorism Fact Sheet: Fusion Task Force*, COM/FS/2010-02/PST-01, February 2010. http://www.interpol.int /Public/ICPO/FactSheets /PST01.pdf (accessed March 30, 2010).

[48]Office of the Director of National Intelligence (ODNI), Interagency Threat Assessment and Coordination Group (ITACG), *"Intelligence Guide for First Responders,"* (2009), 78. http://www.ise.gov/ docs /ITACG_Guide.pdf. (accessed November 29, 2009). Hereafter cited as ITACG, Intelligence Guide to First Responders. This guide defines SAR as, the reporting of suspicious activity to an appropriate government agency, defined as behavior that may be indicative of intelligence gathering or preoperational planning related to terrorism, criminal espionage, or other illicit intention.

freedom, information privacy, and other legal rights of Americans." Congress, exercising its powers, formally codified into law elements of the President's two executive orders by defining its statutory charter and placing the National Counterterrorism Center under the newly established Office of the Director of National Intelligence in the Intelligence Reform and Terrorism Prevention Act of 2004.[49]

Located in McLean, Virginia with a staff of approximately 600 analysts, the National Counterterrorism Center prepares strategic assessments, daily briefings and situation reports from multiple sources about potential terrorist acts. The National Counterterrorism Center supports the nation's watch listing system by maintaining a system of databases, The Terrorists Identities Datamart Environment (TIDE) that contains the identities of well over 500,000 potential terrorists.[50] The customers of their 'federally integrated' reports include the President, Congress and the members of the communities of interest.[51] Congressional passage of the Intelligence Reform and Terrorism Prevention Act of 2004 also mandated the creation of the information sharing environment led by a Program Manager from within the Office of the Director of National Intelligence, hereafter the program manager for the information sharing environment cited as the PM-ISE. Specifically, the Intelligence Reform and Terrorism Prevention Act mandates that the PM-ISE shall, "Assist, monitor, and assess the implementation of the ISE by Federal departments and agencies to ensure adequate

[49]NSIS, 1-12.

[50]Congressional Research Service (CRS) Report for Congress, *The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns*, Order Code R41022, (Washington, D.C.: January 15, 2010), 6. http://www.fas.org/sgp/crs/intel/R41022.pdf. (accessed January 26, 2010).

[51]Ibid., 2.

progress, technological consistency and policy compliance; and regularly report the findings to Congress."[52]

This law also mandated a supporting Information Sharing Council as an adjunct advisory panel to assist the President and the PM-ISE in the development of policy, procedures, guidelines and most importantly, federal information sharing standards for all departments and agencies participating within this newly-established information sharing environment. President Obama elevated the function of the Information Sharing Council by integrating it under the Executive Office of the President within the Interagency Policy Committee.[53] In July 2009, President Obama appointed Mike Resnick as his Senior Director for Information Sharing Policy to oversee the integration of information sharing and access policy within the Interagency Policy Committee, defining information sharing "a top priority of the Obama administration."[54]

How does the National Counterterrorism Center fuse terrorism-related information? Located at the core of the nation's homeland security apparatus, it receives intelligence and terror-related information from the stakeholders among the five communities of interest, Intelligence, Defense, Homeland Security, Justice and State. Vetting of intelligence in the system is managed through the

---

[52]*Intelligence Reform and Terrorism Prevention Act of 2004*. Public Law 108-458, 118 Stat. 3638, 108th Cong., (December 17, 2004), §1016(a) (iii), 32. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ458.108.pdf (accessed November 29, 2009).

[53]For more information on the core functions of the PM-ISE visit their web portal at: http://www.ise.gov/pages/background.aspx. (accessed September 30, 2009).

[54]John O. Brennan, Memorandum to Cabinet Principals, *"Strengthening Information Sharing and Access,"* (Washington, D.C.: Office of the Assistant to the President for Homeland Security and Counterterrorism, July 2, 2009). http://www.fas.org/sgp/obama/brennan070209.pdf (accessed December 12, 2009).

Office of the Director of National Intelligence as the primary agency within an Intelligence Community consisting of the nation's sixteen separate civil and military intelligence gathering agencies and organizations.

The National Counterterrorism Center aggregates information using a six-step cycle to produce federally integrated information products. The six-step intelligence and information fusion cycle is as follows: 1) planning and requirements development; 2) information gathering, collection and recognition of indications and warnings; 3) processing and collation of information; 4) intelligence analysis and production; 5) intelligence/information dissemination; and 6) reevaluation.[55] Merging all-source inputs from federal as well as state, local and tribal agencies involves a fusion cycle that creates a holistic picture of the threats and vulnerabilities that confront the greater communities of interest.[56] Some intelligence analysts have informally described the process of intelligence fusion as piecing together a puzzle from a stack of individual parts without having the benefit of the picture on the puzzle's box cover to see the whole picture. In addition to managing the Terrorist Identities Datamart Environment as one of many terror-related information and intelligence databases, the National Counterterrorism Center disseminates fused products to information sharing environment stakeholders in the communities of interest as well as all state, local and tribal agencies in the nation's states and territories.

---

[55]U.S. Department of Justice, *Baseline Capabilities for State and Major Urban Area Fusion Centers, a Supplement to Fusion Center Guidelines*, Washington, D.C.: September 2008, 9. http://it.ojp.gov/documents/baselinecapabilitiesa.pdf (accessed December 2, 2009).

[56]Information Sharing Environment (ISE), *Progress and Plans, Annual Report to Congress*, (Washington, D.C.: PM-ISE, June 30, 2009), 20-21. http://www.ise.gov/docs/reports/ISE_2009-Annual-Report_ FINAL_2009-06-30.pdf. (accessed November 30, 2009).

State, local and tribal agencies, in turn, disseminate fused products across a disparate array of database systems and portals in the three classified and public information domains to the nation's expansive list of first preventers and responders. Interestingly, in a 2006 nationwide survey conducted by the Justice Department Research and Statistics Association, it was discovered that across the nation there exists as many as 266 information sharing systems in place or under development. Of these 266 systems, 105 resided statewide, 102 were operational, thirty-four were in the planning phase and twenty-five were under development.[57]

Continually working the design system investigation outwards, at the state and regional level of government, criminal and terror-related intelligence is received from the National Counterterrorism Center and fused with similar information coming up from state, local and tribal law enforcement agencies across a nationwide network of seventy-two state and regional fusion centers.[58] Analysts from across the interagency are detailed to staff these fusion centers under separate, independently drafted, interagency memorandums of understanding. The concept of fusion centers evolved from the Department of Justice 2003 National Criminal Intelligence Plan, performing their core functions and responsibilities in accordance with the Department's Bureau of Justice

[57]Lisa Walbolt Wagner, Justice Research and Statistics Association, *Information Sharing Systems: a Survey of Law Enforcement*, (Washington, D.C.: July 31, 2006), 6. http://www.jrsa.org/pubs/reports/improving-crime-data/Info_Sharing_Systems.pdf. (accessed February 4, 2010).

[58]Current information on status of state and regional fusion centers can be found in the DHS web portal located at: http://www.dhs.gov/files/programs/gc_1156877184684.shtm. (accessed December 11, 2009).

Assistance 2006 Fusion Center Guidelines.[59] Illustrative of post 9/11 improved interagency or "Whole of Government" efforts, the fusion center guidelines procedures is a product collaboratively staffed and published by both Justice and Homeland Security.

Information Sharing Networks and Database Systems

What information systems or mediums do the stakeholders in the information sharing environment use to share information and intelligence across multiple agencies and the three codified classifications domains? Information within the information sharing environment resides in three separate national security classification domains, at the high end is top secret/sensitive compartmented information (TS/SCI) information; in-between is secret/collateral information; and in the low end is controlled unclassified information (CUI)/sensitive but unclassified (SBU) information.[60] All of the stakeholders in the information sharing environment that have government-approved top secret-level security clearances may post and retrieve top secret, terror-related intelligence within a tight network of closed systems known as the Joint Worldwide Intelligence Communications Systems (JWICS). However, several hurdles lay before law enforcement agencies seeking to retrieve top secret-level intelligence. Hurdles include a lack of funding for sourcing and maintaining JWICS systems, availability of proper information storage infrastructure—sensitive compartmented information facilities, or

[59]U.S. Department of Justice, Fusion Center Guidelines, *Developing and Sharing Information in a New Era*, Washington, D.C.: July 2006, 10-13. http://www.it.ojp.gov/documents/fusion_center _guidelines.pdf. (accessed November 12, 2009).

[60]Information Sharing Environment (ISE), *Enterprise Architecture Framework version 2.0*, (Washington, D.C.: PM-ISE, September 2008), 19. http://www.ise.gov/docs/eaf/ISE-EAF_v2.0_ 20081021.pdf (accessed September 15, 2009). Hereafter cited as ISE-EAF v. 2.0.

having enough assigned personnel on staff with vetted security clearances trained to handle and protect sensitive intelligence. Equally challenging is a government-wide backlog of security clearance investigations. Proper background checks and investigations can take months to complete for each separate individual requesting approved access to classified and sensitive information.[61] One policy mandated work-around solution is a procedure known as a "tearline," where highly sensitive aspects of information are removed by the owning agency to "protect intelligence sources and methods."[62] This procedure can lead to lowering of the classification level for use by a wider network of analysts and end-users across the information sharing communities of interest. However, this very procedure was identified by the 9/11 Commission as fostering "stovepipes" and a "need to know" versus a "need to share" culture within the greater Intelligence Community—an enduring source of tension resident in the observed system.[63]

Collectively, Homeland Security, Justice and Defense have twenty major information-sharing networks to support their collective homeland security missions. Systems such as the Homeland Secure Data Network (HSDN) facilitate rapid electronic information exchange, including with state, local and tribal agencies. Of these twenty networks, four operate in the top secret/secret classification domain and ten operate in the

[61]*Report Card on Homeland Security Information Sharing*, 12-13.

[62]J.M. McConnell, Intelligence Community Policy Memorandum Number 2007-500-1, *"Subject: Unevaluated Domestic Threat Tearline Reports,"* Office of the Director of National Intelligence (ODNI), (Washington, D.C.: November 19, 2007). http://www.dni.gov/electronic_reading_room/ICPM%202007-500-1,%20Unevaluated%20Domestic%20Threat%20Tearline%20Reports.pdf (accessed December 2, 2009).

[63]Mark A. Sauter and James Jay Carafano, *Homeland Security: a Complete Guide to Understanding, Preventing, and Surviving Terrorism*, (New York: McGraw-Hill, 2005), 18.

sensitive but unclassified domain.[64] The National Counterterrorism Center (NCTC) manages NCTC Online-secret (NOL-S) as the primary information sharing database for posting and retrieving intelligence products from across three separate interagency databases including, Justice's FBInet, Homeland Security's HSDN and the Defense Joint Intelligence Support System (JDISS).[65] Only one network is unclassified. Nine of these networks share information only within a single department; the remaining eight facilitate information sharing among federal, state, local and tribal government agencies. Justice and Defense exchange law enforcement information between FBI and the Naval Criminal Investigative Command on Law Enforcement Information Exchange (LInX). Homeland Security and Justice also host four web-based applications that collect, warehouse, and disseminate homeland security-related information. These applications include Homeland Security Information Network (HSIN), the department's main information technology system for sharing terrorism and related information, and Justice Law Enforcement Online (LEO).[66] All four-system applications are considered to be sensitive but unclassified and are available for use by relevant federal, state, local and tribal government agencies. Finally, in crisis management, the FBI manages ORION to

[64]U.S. Government Accountability Office (GAO), *Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to be Better Coordinated with Key State and Local Information-Sharing Initiatives*,GAO-07-455 (Washington, D.C.: April 2007), 2. http://www.gao.gov/highlights /d07455high.pdf (accessed August 29, 2009).

[65]*ITACG Intelligence Guide for First Responders*, 39.

[66]Ibid., 37.

enhance situational awareness, standardize crisis and event management processes between FBI command posts.[67]

Controlled access of information shared between agencies in the unclassified domain can still occur by employing procedural, software and hardware firewalls including the use of personally identifiable information mediums (e.g., Common Access Card). Still, more fool proof measures are needed in the twenty-first-century, what Secretary Chertoff labeled as "the three Ds,—*description, device and digit*." Description refers to information known to an individual (e.g., a social security card), device referring to an identity or document (e.g., a cell phone or portable electronic device tied to an individual) and digit referring to biometric information (e.g., one's fingerprints, or individual-unique retinal images).[68]

Defense geographic Combatant Commanders manage several independent information sharing portals in the unclassified domain for the posting and retrieval of for official use only-level information with external partners, including the interagency, in their areas of responsibility in the controlled unclassified information/sensitive but unclassified classification domain. These portals and database systems include non-Secure Internet Protocol Router Network (NIPRnet), Collaborative Information Environment (CIE), managed by U.S. Northern Command in the execution of Homeland Defense and Civil Support activities and Asia Pacific Area Network (APAN), managed separately by U.S. Pacific Command. U.S. Pacific Command is responsible for

[67]U.S. Department of Justice, *Robert S. Mueller, III: Congressional Testimony before the Senate Committee on the Judiciary*, Washington, D.C.: Press Room, Federal Bureau of Investigation, January 20, 2010, 2. http://www.fbi.gov/cpngress/congress10/mueller 012010.htm (accessed March 6, 2010)

[68]Michael Chertoff and Lee H. Hamilton. *Homeland Security, Assessing the First Five Years*. Philadelphia, PA: University of Pennsylvania Press, 2009, 119.

Homeland Defense and Civil Support activities in the Hawaiian Islands. Combined Enterprise Regional Information Exchange System (CENTRIXS) is yet another Defense database system managed by the remaining geographic combatant commands to enable multiple secret-level coalition partners to share information. (e.g., CENTRIXS-I utilized by the Multi-National Forces Iraq participating nations).[69] As such, the nation's information sharing environment, through Defense, has yet another redundant source of harvesting global information and intelligence beyond INTERPOL's existing law enforcement architecture.

How are information sharing standards and protocols defined? Consistent with Intelligence Reform and Terrorism Prevention Act of 2004 statutory provisions, the PM-ISE establishes common information exchange standards, processes and business practices using the National Information Exchange Model and Universal Core. The National Information Exchange Model, a partnership effort between Justice and Homeland Security, has as its core goal to develop, disseminate and support enterprise-wide information exchange standards and processes. In spirit, this partnership enables jurisdictions to effectively share critical information in emergencies, as well as support the day-to-day operations of agencies throughout the nation. Universal Core is an interagency implementation profile that provides the framework for sharing the most commonly used data concepts of *"who, what when, and where,"* the starting point for all data integration amongst databases. Universal Core is a collaborative effort between the

[69]U.S. Department of Defense, *Information Sharing Implementation Plan*. Washington, D.C.: Office of the Assistant Secretary of Defense for Network and Information Integration, April 2009, 16-18. http://cio-nii.defense.gov/docs/DoD%20ISIP%20-%20APR%202009 _approved.pdf (accessed November 30, 2009).

National Information Exchange Model governance board, the intelligence community, Homeland Security, Justice and Defense.[70]

A critical node in the multi-agency data exchange enterprise is the FBI's Terrorist Screening Center. Established in 2003 by Presidential directive, Homeland Security Presidential Directive-6 (HSPD-6)—*Directive on Integration and Use of Screening Information to Protect Against Terrorism*, required the creation of a national Terrorist Screening Center. The new organization previously known as the Terrorist Threat Integration Center, under this directive it specified that the Terrorist Screening Center will, "Develop, integrate, and maintain thorough, accurate, and current information [watch lists] about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information)."[71]

Why was there a need for a national-level Terrorist Screening Center? Prior to 2003, the nation relied on numerous federal agencies to screen individuals and maintained separate watch lists. Consolidating all terror watch lists under the Terrorist Screening Center's consolidated terrorist watch list, or the Terrorist Screening Database, it has evolved into the federal government's master repository for all known or appropriately suspected international and domestic terrorist records used for watch list-related screening.[72]

---

[70]ISE-EAF version 2.0, 85-86.

[71]President, Homeland Security Presidential Directive-6 (HSPD-6), "Directive on Integration and Use of Screening Information to Protect Against Terrorism", *U.S. Government Printing Office*, (September 16, 2003), 1-2. http://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf (accessed January 16, 2010).

[72]ISE-EAF version 2.0, E-4-E-5.

Not to be confused with the mission of Justice's Terrorist Screening Center, the Homeland Security Customs and Border Protection agency oversees the National Targeting Center. Established on October 21, 2001, this organization consists of more than sixty employees whose mission is to sift and filter through information in other government databases, looking for terrorists and weapons bound for the United States. The National Targeting Center uses software known as the Automated Targeting System to filter a comprehensive listing of names with known connections to other terror-related databases. The Automated Targeting System "processes information, picking up on anomalies and "red flags" and provides a basis for targeters[sic] to determine what cargo or passengers are "high risk," whether they require scrutiny at the port of entry or overseas, or whether they can come to our shores at all.[73] As discussed later, this critical node played a key role in managing information during the Christmas Day attack.

At the bottom of the nation's information sharing environment are private sector entities and the public at large. They observe their environment and, in bottom-up fashion, report suspicious behavior, activities or incidents to local law enforcement authorities, the nation's first preventers, as serious activity or incident reports. Conversely, when the effects of criminal activity, terror-related attacks, manmade or natural disasters inflict great physical and psychological suffering on the public or result in catastrophic disruptions to the nation's critical infrastructure and key resources, the nation relies on Homeland Security's National Response Framework to catalyze the first

[73]U.S. Customs and Border Protection, *National Targeting Center Keeps Terrorism at Bay*, (Washington, D.C.: March 2005). http://www.cbp.gov/xp/CustomsToday/2005/March/ntc.xml (accessed March 2, 2010).

responder system.[74] It is worth noting that of the nation's critical infrastructure and key resources across the seventeen Critical Infrastructure and Key Resource sectors identified in the 2003 Homeland Security Presidential Directive-7 (HSPD-7)—*Critical Infrastructure Identification, Prioritization and Protection,* the vast majority are owned or operated by the private sector.[75] This fact necessitates information sharing efforts between government and the private sector. The nation's efforts to manage consequence management in the homeland are not limited to just terrorist attacks. To address consequence management of both natural disasters and weapons of mass destruction and effects, the design analysis drawing reflects the relationships between the relevant consequence management stakeholders in the system.

U. S. Northern Command, the primary Defense organization responsible for Homeland Defense and Civil Support, conducts military operations within its assigned area of responsibility utilizing forces to deter, detect, or defeat an incursion into sovereign territory, and its land, air and maritime approaches. It is highlighted in the lower left quadrant of the design drawing. Its standing Joint Task Force Civil Support, (JTF-CS) plans and integrates Defense support to the designated primary agency for chemical, biological, radiological, nuclear or high-yield explosives (CBRNE) consequence management.[76] JTF-CS and the FEMA region-associated regional Defense Coordination Officers represent Defense in its role of supporting the designated primary

---

[74]U.S. Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency,* (Washington, D.C.: January 2009), 11. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf. (accessed September 15, 2009).

[75]Read more on HSPD-7, *Critical Infrastructure Identification, Prioritization and Protection*, at http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1 (accessed January 20, 2010).

[76]Joint Publication 3-27 (JP 3-27), *Homeland Defense,* (Washington, D.C.: Chairman of the Joint Chiefs of Staff, 12 July 2007), II-4 to II-7. Hereafter cited as JP 3-27.

federal agencies consistent with the National Response Framework.[77] While National Guard Bureau does not exercise operational authority, it provides coordination and communication between the states, Defense, and other federal agencies. This role is crucial when the states conduct domestic operations in support of state governors in a Title 32 U.S. Code status.[78]

The National Guard's role in managing forces in all fifty-four states and territories is reflected in the design drawing by the individual state Standing Joint Force Headquarters. Each state has a joint force headquarters, which integrates Army and Air National Guard resources. The Joint Force Headquarters provide a focal point to interoperate jointly with combatant commands and any federal joint task forces that may perform Homeland Defense or Civil Support within a state's boundaries.[79] To better capitalize on improved information sharing and the synergy gleaned from established long-term mission partner relationships, some state Joint Force Headquarters offices are co-located near state or Regional Fusion Centers. Defense maintains its relationships with the foreign partner community across the globe through geographic combatant commanders executing duties and responsibilities consistent with the Unified Command Plan in their respective areas of responsibility.[80]

The Federal Emergency Management Agency reflects Homeland Security's role consistent with the National Response Framework. It includes the Federal Coordination

---

[77]Kendall D. Gott and Michael G. Brooks, ed., *The U.S. Army and the Interagency Process: Historical Perspectives*, Fort Leavenworth, KS: Combat Studies Institute Press, 2008, 19.

[78]JP 3-27, II-14.

[79]JP 3-27, II-15.

[80]Find out more about the Department of Defense Unified Command Plan (UCP) at: http://www.defense.gov/home/features/2009/0109_unifiedcommand/ (accessed March 30, 2010).

Officer, depicted just below Homeland Security's seal. In times of national disasters, the Federal Coordinating Officer is typically located at the designated Disaster Field Office with the U.S. Coast Guard and interagency-wide Emergency Support Functions among multiple agencies supporting first responders. In cases involving screening against potential terrorists in the aviation transportation sector, Homeland Security's Transportation Security Administration, also established in the aftermath of the 9/11 attacks is depicted in a supporting role to first preventers.[81]

Located in the drawing's upper left quadrant is Congress, a critical node in the supra-system, performing its role in appropriations, legislation and oversight. Further, Congress directs the Government Accountability Office often called "the Congressional watchdog," in its role as an auditing instrument to inform members of Congress on matters related to statutory provisions and pending legislation.[82]

At the top of the supra-system are the President, his Cabinet top officials and the National Security Council. In the arena of homeland security, the counterpart to the National Security Council is the Homeland Security Council.[83] The design analysis drawing does not imply that the Department principals do not engage the President in forums other than homeland security. They do. This drawing simply depicts a snap shot in time of the nodal relationships between the relevant stakeholders, including key Cabinet and Departmental leaders in the context of terror-related information sharing activities.

---

[81]Gott, 28.

[82]Find out more about the U.S. Government Accountability Office (GAO) at: http://www.gao.gov/about/index.html (accessed December 2, 2009).

[83]President, Executive Order 13228 (EO 13228), "Establishing the Office of Homeland Security and Homeland Security Council," *Federation of American Scientists* (October 8, 2001). http://www.fas.org /irp/offdocs /eo/eo-13228.htm (accessed January 11, 2010).

Other relevant actors that shape the information sharing environment include both domestic and global media organizations.[84] As the nation witnessed in the twin disasters of September 11, 2001 and Hurricane Katrina in 2005, too often they perform the crucial, albeit informal, function as being the system's source for framing a common operating picture for decision makers, first responders and the public at large. As mentioned earlier, many private "watchdog" organizations perform an informal function of reporting actual or perceived abuses of United States government information gathering activities and litigate in behalf of citizens. They too are a relevant actor in this supra-system. The American Civil Liberties Union and Center for Democracy and Technology and their relationship with the nation's judicial system represent the ever-vigilant private sector organizations whose self-declared charter is to protect the privacy and civil liberties of Americans against actual or perceived abuses by the information sharing environment's stakeholders across all levels of government. In 2007, the Center for Democracy and Technology published an analysis of the privacy guidelines promulgated by the Information Sharing Environment and warned that both CIA and Defense were operating "outside their assigned mission areas; reiterating that they should not collect or analyze domestic intelligence."[85]

Having examined the interrelationships of the information sharing environment's stakeholders across multiple layers of government, its governing authorities and wide array of mediums for sharing information across the three classification domains, it is

[84]White Paper, "GIS Supporting the Homeland Security Mission," *Environmental Systems Research Institute (ESRI)*, (Redlands, CA: May 2007), 4. http://www.esri.com/library /whitepapers/pdfs/gis-supporting-hls.pdf (accessed March 15, 2010).

[85]Jim Dempsey, "CDT Analysis of Privacy Guidelines for the Information Sharing Environment for Terrorism Information," *Center for Democracy and Technology (CDT)*, (February 2, 2007), 10. http://www.cdt.org/security/20070205iseanalysis.pdf (accessed March 3, 2010).

appropriate to examine the role that existing tensions play in shaping the overall tendency of the system. Figure 3 (Appendix B) depicts the environmental frame expressing its observed, desired and undesired system tendencies as well as the positive and negative tensions that define what FMI 5-2, *Design*, labeled both the 'system of transformation' and the 'system of opposition' respectively.[86]

The Observed System

For all the nation has invested in national security this past decade, it remains prone to terrorist attack and emerging national security threats. The supra-system has not adequately improved the nation's ability to know what it knows about emerging threats. As stated by the President in the wake of the Christmas Day attack—the nation still cannot connect the dots. Additionally, civil liberties remain at risk because government-wide polices to safeguard them have not kept up with the pace of change in the nation's expanded intelligence gathering authorities.[87]

The system is susceptible to failure at multiple entry points. Being a binary system with an information and intelligence fusion cycle fed from both internal and external nodal entry points, data becomes susceptible to degradation before ever reaching the core of the supra-system—the National Counterterrorism Center. The result is increased data as well as "noise" requiring longer analysis and potential delays in

[86]Note: with the subsequent release of FM 5-0, *The Operations Process*, the terms "system of transformation" and "system of opposition" were deemed too confusing for the force and have been rescinded and replaced by "system tendencies and potentials."

[87]Zoe Baird and Jim Barksdale, "Nation at Risk: Policy Makers Need Better Information to Protect the Country." *The Markle Foundation Task Force on National Security in the Information Age*, (March 10, 2009), 1. http://www.markle.org/downloadable _assets/20090304_mtf_report.pdf (accessed January 14, 2010).

disseminating federally integrated to the end user in support of real time operations. This challenge was exemplified during the Christmas Day attack when either State or Homeland Security officials misspelled the suspected terrorist name, causing delays in cross-agency watch list screening procedures.[88]

The system contains blind spots between agencies. Blind spots or gaps are created when agencies make distinctions between domestic and foreign threats.[89] Further, in a throwback to the Cold War era, the nation placed a premium on security of information that resulted in a culture that rigidly controlled access to information, requiring individuals to demonstrate a "need to know" before information could be seen.[90] Old habits die hard and although some progress has been made since the findings of the 9/11 Commission, some members in Intelligence and Justice still find it difficult to share across agencies. In a survey of Homeland Security and law enforcement officials conducted in 2009 by the Homeland Security Affairs Journal one respondent complained that when a local law enforcement official discovered a resident's name on a terrorism watch list he queried the FBI to find out why and was told, "I can't tell you."[91]

One repetitive complaint by end users of federally aggregated information is that it does not support real-time operations. In a 2006 internal Homeland Security Inspector

---

[88]The White House, *Summary of the White House Review of the December 25, 2009 Attempted Terrorist Attack*, (Washington, D.C.: January 8, 2010), 6. http://www.whitehouse.gov/sites/default/files/summary_of_wh_review _12-25-09.pdf (accessed January 8, 2010).

[89]Zoe Baird and Michael A. Vatis, "Creating a Trusted Network for Homeland Security, Second Report of the Markle Foundation Task Force," *The Markle Foundation Task Force on National Security in the Information Age*, (December 3, 2003), 6. http://www.markle.org/ downloadable_assets/nstf_report2_full_report.pdf (accessed August 29, 2009).

[90]Ibid.

[91]Hamilton Bean, "Exploring the Relationship between Homeland Security Information Sharing & Local Emergency Preparedness," *Homeland Security Affairs*, Volume V, No. 2 (May 2009), 9. http://www.hsaj.org/pages/volume5/issue2/pdfs/5.2.5.pdf (accessed December 12, 2009).

General's investigation, security officials were asked to rate the quality of information disseminated to end users via reports and portal postings. The answers were not surprising. State and local users stated that Homeland Security's HSIN network "did not provide them with timely and relevant information needed to support their counter-terrorism mission." Further, similar respondents complained that the HSIN-Secret portal "did not contain useful products."[92] End users rated the information they received as not actionable.

Related to the previous issue of a "need to know" paradigm, trust, or the lack thereof, was another widespread finding in internal investigations from the 9/11 Commission to repeated Homeland Security's Office of the Inspector General (OIG) investigations. Again, members of the greater law enforcement community do not trust the HSIN database to share sensitive case information. Many respondents expressed concern that by posting sensitive cases on the network they "are leaked or compromised," "divulging personal or private information with users who do not have a need to know."[93]

Lastly, the system suffers from a lack of clear jurisdictional policies. In a supra-system composed of multi-level (state, local and tribal) subsystems across 3,086 counties nation-wide disparities in jurisdictional authorities exist. In many cases, state laws differ from those of the federal government, preventing what would be expected to be common practice of exchanging information across multiple levels of government. In Congressional testimony before the Committee on Homeland Security, John McKay,

[92]U.S. Department of Homeland Security, Office of the Inspector General. *Homeland Security Information Network Could Support Information Sharing More Effectively*. OIG-06-38, Washington, D.C.: June 2006, 22-24. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_06-38_Jun06.pdf (accessed January 15, 2010). Hereafter cited as OIG-06-38.

[93]Ibid.

Professor from Practice, the Seattle School of Law, declared that "from a national perspective, making State and local law enforcement records available to Federal agencies is a required critical component of 21st Century public safety." In one particular case "information that might have prevented an attack was found, after the fact, in the files of a municipal police department."[94]

The design approach revealed positive tensions that have the potential to nudge the current or observed system towards the desired state. These tensions included the very real fear of re-attack. This fear across key branches of government was the impetus behind most of the proactive actions by Congress and the President in the wake of the 9/11 attacks. Further, law enforcement officials repeatedly testified that the increased level of federal, state, and local law enforcement partnerships, exemplified in FBI's Joint Terrorism Task Forces and state and regional Fusion Centers has improved a sense of trust among the greater law enforcement community.[95] Increased partnerships led to collaborative training and increased technical assistance, two factors receiving favorable support from the greater law enforcement community.

The proliferation of information technology in government and the private sector has resulted in a work force that is better informed in the use of these systems, reducing the amount of time needed to assimilate new systems. Still, a Homeland Security internal audit found that the Department fielded new information systems without properly training the staff on how to effectively use them.[96]

---

[94]*A Report Card on Homeland Security Information Sharing,* 34.

[95]Ibid., 13.

[96]OIG-06-38, 9.

Increased funding by Congress, evident in the expansion of nation-wide state and regional Fusion Centers and proliferation of more information systems down to state, local and tribal government levels has been cited in Congressional testimony as a very positive tension. However, under the current constraints of the nation's economy, anxiety abounds on the willingness of Congress to finish a work in progress.[97]

Clearly, a major challenge that the nation faces with regard to improved information sharing is balancing the need to leverage evolving and ever-improved information technology with matching internal training programs so government employees can assimilate them more effectively.

THE PROBLEM FRAME

So, what is the problem here? The design framework outlined in the Army's Field Manual 5-0, *The Operations Process*, suggests drafting a "concise problem statement" that considers how "tensions and competition effect the operational environment by identifying how to transform the current conditions to the desired end state."[98] In addition to considering the associated effects of tensions and competition, the statement "accounts for time and space relationships inherent in the problem frame."

Using design's doctrinal suggestion for the framework of a problem statement, the problem that emerges is one where the Information Sharing Environment suffers from the collective effects of dissimilar factors including, rigid organizational cultures, unclear federal, state and local policies and a saturation of non-compliant information system

[97]Ibid, 24.

[98]FM 5-0, 3-11.

architecture. These factors collectively prevent the stakeholders from the communities of interest from effectively gathering, evaluating, fusing and disseminating actionable threat information. As such, the nation's top officials, first preventers and responders remain unable to make timely and effective decisions during real-time operations. Further, given the dynamic pace of innovation and adaptation by the nation's enemies, the Information Sharing Environment must adapt and change faster than the nation's enemy's change. Finally, changes in the information sharing regime must not compromise the Constitutional rights, civil liberties and privacy of American citizens.

The biggest challenge the nation faces in finding a solution to this problem involves striking a balance between three opposing forces. How do policy makers protect citizen's rights and civil liberties while simultaneously employing secure and functional information sharing database systems that are value added during real-time operations? The subsequent case studies will expose United States government efforts to find this delicate balance against two real world events involving both traditional foreign and 'home grown' threats. In the case of the Fort Hood rampage, the nation's lower tier subsystems including local law enforcement agencies and a regional FBI Joint Terrorism Task Force received suspicious activity reports (SAR), but where eventually surprised by the outcome. In the case of the Christmas Day terror plot, the nation's foreign partner supra-system received ample warnings and indicators of a pending attack, but in the end, it too was equally surprised by the outcome.

THE SOLUTION FRAME

With the ill-structured problem defined using the Army's design approach, what strategies have policymakers implemented in the face of the tensions and risks associated with the nation's information sharing environment? This next section of the study lays out the gamut of existing and evolving national-level strategies and solutions put forth as the "solution" or "design concept." Again, these collective solutions are then compared against two recent terror-related incidents, the Fort Hood Shooting rampage and the Christmas Day attack to gauge their effectiveness.

Figure 5 (Appendix B) depicts the solutions applied to this problem as national-level lines of effort including new executive branch policy and strategy, Congressional legislation, consolidation of government and new infrastructure.[99] Highlighted previously in the study, in the wake of the trauma of September 11, 2001, President Bush and Congress exercised great initiative in adapting the very fabric of government to address the challenges posed by terrorism as a new form of global warfare. In the policy arena, the most notable instrument implemented regarding information sharing was the 2007 "National Strategy for Information Sharing." This national-level policy document was nested with and complimented sister strategies including "The National Strategy for Homeland Security," "The National Security Strategy" and "The National Strategy for Combating Terrorism." Articulating in one source the policy objectives of the nation in the field of information sharing, it was quickly followed by similarly aligned and nested Department level information sharing strategies from the members of the community of

[99]Note: Section 6-66 of U.S. Army Field Manual 3-0, *Operations*, defines a line of effort as, linking multiple tasks and missions using the logic of purpose—cause and effect—to focus efforts toward establishing operational and strategic conditions.

interest including Defense, Justice, Homeland Security, and the Intelligence Community. State, however, did not issue its own complimentary information sharing strategy.

Interestingly, many of President Bush's national-level strategies, including the "National Strategy for Information Sharing," were promptly removed from President Obama's (*www.whitehouse.gov)* web portal. Curiously, the fact that former Bush Administration policy cannot be found in the current White House web portal lends credibility to what some have labeled as President Obama's "un-Bush" mandate.[100] This apparent overt political act to eradicate existing policy writ large may not be helpful in charting a new direction for the nation to follow in the arena of information sharing. At the very least, the administration should publish new strategies to better inform the federal bureaucracy. Well over a year into President Obama's term in office, his policy team has yet to publish a new policy document to replace that of the former administration. Policy appears to be in a state of suspended animation, affording opportunities to the nation's adversaries. Even more telling, the office responsible by law for managing the nation's information sharing environment, the Program Manager for Information Sharing (PM-ISE), maintains a very informative web portal, (*www.ise.gov*), with an embedded tab labeled "archives." This tab opens a separate page with a comprehensive listing of documents chronicling the evolution of policy in national-level information sharing efforts. Today, if you follow that page's hyperlink, all of the archives conspicuously stop in 2008, giving the impression that efforts to improve the nation's information sharing environment made no progress during the transition of

[100]Eliot Cohen, "What's Different About the Obama Foreign Policy?" *Wall Street Journal*, August 2, 2009, 2. http://online.wsj.com/article/SB10001424052970203946904574300402608475582.html (accessed December 12, 2009).

administrations in 2009. No Obama Administration policy documents regarding information sharing are currently posted.

The second and most notable impact in transforming government operations in the face of new threats was the largest consolidation of government since 1947. Highlighted earlier in the study, in the days and months following the 9/11 attacks, efforts to transform government were highlighted by the creation of the Department of Homeland Security that consolidated twenty-two separate departments and agencies into one. Homeland Security changes included the creation of the National Targeting Center, the National Counterterrorism Center and the Transportation Security Administration. Justice changes included the growth and proliferation of state and regional Fusion Centers. In the Defense arena the most notable changes included creation of U.S. Northern Command with an assigned standing Joint Task Force to address and mitigate the impact of high-consequence weapons of mass destruction—Joint Task Force Civil Support.[101]

Not to be outdone by the executive branch, Congress passed significant legislation previously outlined, including the USA Patriot Act, the Implementing Recommendations of the 9/11 Commission Act, the Homeland Security Act, and the Intelligence Reform and Terrorism Prevention Act. All have been incrementally amended. By far the biggest impact made by Congress has been appropriations, a major catalyst of change. According to the Office of Management and Office, in the arena of Homeland Security alone, well over $406 billion U.S. tax payer dollars have been budgeted to the

[101]Congressional Research Service (CRS) Report for Congress, *Homeland Security: Roles and Missions for United States Northern Command*. Order Code RL34342, Washington, D.C.: January 28, 2008), 3. http://www.fas.org/sgp/crs/ homesec/RL34342. pdf (accessed September 9, 2009).

Department of Homeland Security since its creation 2002, this figure jumps to a trillion-dollars-plus when you combine the efforts of the other Federal Departments.[102]

Given the transformation of the United States government overarching security apparatus in the wake of the 9/11 attacks outlined in this study with improved laws, executive branch policy, new federal organizations and generous funding, are there still gaps in the system? The following two case studies provide a sobering look at the state of the nation's generously funded information sharing environment. Each highlights how the existing framework explored in this study actually responds to recent, real-world events.

CASE STUDY: FORT HOOD RAMPAGE

> We face threats from homegrown terrorists—those who live in the communities they intend to attack, and who are self-radicalizing, self-training, and self-executing.
>
> —Robert S. Mueller, III, FBI Director, Congressional Testimony[103]

On November 5, 2009, dozens of U.S. Army soldiers from numerous units across the Army's largest Post, Fort Hood, Texas, were conducting pre- and post-deployment Soldier Readiness Processing activities at the Soldier Readiness Center. They were completely unaware of the catastrophe that was about to befall them. At 1:34 p.m. Central Standard Time, the alleged perpetrator, U.S. Army Major Nidal Malik Hassan, a 39-year-old medical doctor, entered the Soldier Readiness Center in uniform, took a seat

[102]See Office of Management and Budget, Table 5-2, Budget Authority by agency: 1976-2015, at: http://www.whitehouse.gov/omb/budget/Historicals/. (accessed March 10, 2010).

[103]Robert S. Mueller, III, *Congressional Testimony*,1.

at a nearby empty table and without warning, stood up yelling, *"Allahu Akbar!"*—Arabic for "God is great!"[104] He then began his brutal rampage, randomly shooting and cutting down clustered soldiers and civilians around him. According to eyewitnesses, he purposefully targeted fellow soldiers in uniform.

An American-born Muslim of Palestinian descent, Major Hassan used two privately owned handguns, a Fabrique Nationale-57, a 5.7-millimeter semi-automatic pistol and a Smith and Wesson caliber .357 Magnum revolver, firing more than 100 rounds in a span of ten-minutes.[105] First responders, including Fort Hood Post Police officer, Sergeant Kimberly Munley, was on-scene within three minutes of the initial 911 calls, encountering Major Hassan and resulting in a rapid exchange of gunfire between the two. In the crossfire, Sergeant Munley wounded Major Hassan as she too was struck twice on her leg and once on the wrist. Fellow Fort Hood Post Police officer, Sergeant Mark Todd, seeing his partner fall from her encounter with Major Hassan yelled *"Police, drop your weapons!"* as Major Hassan attempted to reload his semi-automatic pistol. As before, the two quickly exchanged gunfire, however, this time Major Hassan fell. Sergeant Todd subsequently removed Major Hassan's weapons and restrained him before the perpetrator succumbed to unconsciousness from his wounds.[106] The encounter between Major Hassan and the two police officers lasted a mere forty-five seconds. Shot

---

[104]"Fort Hood Shootings: the meaning of 'Allahu Akbar,'" *The Telegraph*, (November 6, 2009), 2. http://www.telegraph.co.uk/news/worldnews/northamerica/usa/6516570/Fort-Hood-shootings-the-meaning-of-Allahu-Akbar.html (accessed January 16, 2010).

[105]Larra Jakes, and Devlin Barret, "AP Sources: Rampage Gun Purchased Legally," *Seattle Times*, (November 6, 2009), 1. http://seattletimes.nwsource.com/html/politics/ 2010219175_ apusforthoodshootinggun.html (accessed March 10, 2010).

[106]James C. McKinley Jr., "Second Officer Gives Account of Shooting at Fort Hood," *New York Times*, (November 12, 2009), 2. http://www.nytimes.com/2009/11/13/us/13hood.html?pagewanted= 1&_r=3&hp (accessed March 8, 2010).

four times, Major Hassan was paralyzed in his encounter with Officers' Munley and Todd.[107] This traumatizing and brazen attack resulted in thirty people wounded, and thirteen killed—twelve soldiers and one civilian, eleven dying at the scene of the crime, including a pregnant soldier and two others who died from their wounds at local area hospitals.

A joint criminal investigation involving multiple law enforcement jurisdictions, including the FBI, the Army's Criminal Investigation Command and the Texas Rangers Division is ongoing. Under the military jurisdiction of the U.S. Army and the Uniform Code of Military Justice, Major Hassan, the alleged, lone gunman, was charged with thirteen counts of premeditated murder and thirty-two counts of attempted murder. Additional charges are pending, including an additional charge of murder for the killing of an unborn child in military court-martial proceedings, these charges making him eligible for the death sentence.[108] Formally redefining this mass casualty attack, a "terror plot" increases the possibility that Major Hassan will be indicted in the federal criminal court system.[109]

What did the nation's information sharing system know about Major Hassan prior to his rampage? It appears as if the trail of 'dots' began a year prior to this horrific attack. In 2008, an FBI Joint Terrorism Task Force was conducting an unrelated investigating against a radical Muslim cleric, Anwar al-Awlaki, known for his

---

[107]Robert D. McFadden, "Army Doctor Held in Fort Hood Rampage," *New York Times*, (November 6, 2009). http://www.nytimes.com/2009/11/06/us/06forthood.html?_r=1&pagewanted=2 (accessed March 8, 2010).

[108]Aaron Cooper with Tedd Rowlands, Barbarra Starr, and Brian Todd, "Fort Hood Suspect Charged with Murder," *CNN*, (November 12, 2009), 2. http://www.cnn.com/2009/CRIME /11/12/ fort.hood.investigation/index.html (accessed March 6, 2010).

[109]Ibid.

inflammatory anti-American teachings. This Imam had murky associations with known Islamists, including two of the September 11, 2001 hijackers. In the course of the FBI surveillance of Awlaki, that included phone and e-mail communications, the FBI intercepted communications with Major Hassan.[110] These communications included eighteen e-mails between the two over a six-month period, from December 2008 to June 2009.[111] The personal communications between these two men is considered the mechanism behind Major Hassan's 'radicalization' and selective targeting of America's military. What was his motive? In testimony before Congress, the Honorable Juan Carlos Zarate opined,

> For homegrown or self-radicalized individuals or cells, military bases and symbols provide the most visible and legitimate targets that help them justify their actions – orally and theologically – by tying their attacks directly to the perceived attacks on Muslims by the U.S. military.[112]

According to anonymous officials with access to the transcripts of the e-mails, one of the e-mails describes an exchange in which Major Hassan wrote, "I can't wait to join you" in the afterlife.[113] The context of the e-mail exchanges between these two men are highly suggestive of Major Hassan's intent to carry out a follow on suicide attack.

---

[110]Drew Griffin with Elaine Quijano, Carroll Cratty and Brian Todd, "Profiler: Fort Hood Suspect a Loner," *CNN*, (November 12, 2009). http://www.cnn.com/2009/CRIME/11/11/texas.fort.hood. investigation/index.html (accessed March 6, 2010).

[111]Brian Ross and Rhonda Schwartz, "Major Hassan's email: 'I Can't Wait to Join You' in Afterlife," *ABC News*, (November 19, 2009). http://abcnews.go.com/Blotter/major-hasans-mail-wait-join-afterlife/story?id=9130339 (accessed January 12, 2010).

[112]Senate and Homeland Security and Governmental Affairs Committee, Statement by Juan Carlos Zarate, "The Fort Hood Attack: A Preliminary Assessment," *Center for Strategic and International Studies (CSIS)*, November 19, 2009, 4. http://hsgac.senate.gov/public/ index.cfm? FuseAction=Hearings.Hearing& Hearing_ID=70b4e9b6-d2af-4290-b9fd-7a466a0a86b6 (accessed December 12, 2009).

[113]Ross, 1.

The FBI Joint Terrorism Task Force, staffed with embedded Defense liaison personnel shared their surprising revelation with the Army's Criminal Investigative Services for follow-up action. However, after an internal joint investigation between Defense and the FBI, it was determined that Major Hassan's connections to this radical cleric were benign and follow-on action was dropped in part, "because the content of the communications was explainable by his research and nothing else was found." At the time, Major Hassan, a psychiatrist, was conducting his medical residency at the Washington, D.C., Walter Reed Army Medical Center, where he often counseled soldiers undergoing psychological treatment for their combat experiences in Iraq and Afghanistan. Major Hassan's research on Islam and its radical underpinnings in the two wars provided a suitable cover for his odd internet activities. As such, investigators decided, "that Major Hassan was not involved in terrorist activities or terrorist planning."[114] Another 'dot' in the trail leading to this massacre alluded to possible 'walls' or "stovepipes" between members of the information sharing system. There were numerous media reports stating that members of the Criminal Investigative Services working with the FBI's Joint Terrorism Task Force were not sharing information on Major Hassan's possible connections to a radical cleric because, "the task force's ground rules prevented that information from being transmitted outside the task force."[115]

Yet another 'dot' in this plot involved another possible motive for this attack. Major Hassan's extremist leanings and possible motivation behind it are traceable to presentations he made to fellow medical staff members while previously assigned to the

[114]David Johnston and Scott Shane, "U.S. Knew of Suspect's Tie with Radical Cleric," *New York Times*, (November 10, 2009). http://www.nytimes.com/2009/11/10/us/10inquire.html?_r=1 (accessed March 5, 2010).

[115]Griffin, 2.

Walter Reed Army Medical Center. In one August 2007 presentation, he raised the concern of fellow medical practitioners when he expressed a radical view that "justified suicide bombing and stated that *'Shari'a* law took precedence over the US Constitution.''[116] Given he was pending deployment to Afghanistan on November 28, 2009, some believe this pending deployment conflicted with his twisted views of Muslims serving in the U.S. military. In fact, in 2006, according to a sworn statement from his adviser, "Major Hassan met with an academic adviser to see whether he would qualify for conscientious objector status, saying he opposed the war in Iraq on religious grounds."[117] No doubt, Major Hassan's supervisors should have intervened based on the conspicuous activities highlighted here. The notion of intervention by Major Hassan's leaders was highlighted in the Defense findings. However, they are unrelated to this study's thesis. Adding to the notion that Major Hassan had terrorist leanings, retired Army General Barry McCaffrey opined, "it's starting to appear as if this was a domestic terrorist attack on fellow soldiers by a major [sic] in the Army who we educated for six years while he was giving off these vibes of disloyalty to his own force."[118] Linking the trail of 'dots' to the study's design analysis, clearly several system positive and negative tensions were at play. The fact that Defense and Justice members shared suspicious information while working in a Joint Terrorism Task Force represents a 'positive tension' of increased state, local and tribal partnerships. Conversely, deep-rooted organizational

[116]Bryan Bender, "Fort Hood Suspect was an Army Dilemma," *The Boston Globe*, (February 22, 2010), 3. http://www.boston.com/news/nation/washington/articles/2010/02/22/ft_hood_ suspect_was_ army_dilemma/ (accessed March 6, 2010).

[117]Ibid., 2.

[118]General (Ret.) Barry McCaffrey, Interview with CNN Anchor, Anderson Cooper, "Investigating Fort Hood Massacre," CNN, *Anderson Cooper 360 Degrees*, November 6, 2009, 11. http://transcripts.cnn.com/ TRANSCRIPTS/0911/06/acd.01.html (accessed March 6, 2010).

culture coupled with unclear jurisdictional authorities acted as powerful and opposing 'negative tension.'

Independent Review: Findings and Recommendations

Regarding "information sharing" in this mass casualty event, the independent review panel highlighted "gaps" when it came to sharing information with the right people. Referencing providing information to relevant entities the report cited, "The time has passed when bureaucratic concerns by specific entities over protecting "their" information can be allowed to prevent relevant threat information and indicators from reaching those who need it—Commanders."[119]

Earlier in the case study it was alluded that there might have been discrepancies regarding the sharing of information between Defense and the FBI's Joint terrorism Task Forces. In the report's section labeled "Going Forward" the report cited,

> [DOD will] act immediately with the Federal Bureau of Investigation to enhance operations with Joint Terrorism Task Forces. To protect the force, our leaders need immediate access to information pertaining to Service members, indicating contacts, connections, or relationships with organizations promoting violence. One additional step may be to increase Service participation on the Joint Terrorism Task Forces.[120]

The report addressed the challenges discovered by Defense Criminal Investigative Services regarding the ability to "search for" and "analyze" information outside their databases. This particular limitation restricts analysis and investigations outside each of the Services. This gap can reduce law enforcement capability to "prevent, detect or

[119]DOD Independent Review, 3.

[120]Ibid.

investigate criminal activity." The proposed Defense recommendation includes leveraging the existing and highly effective Naval Criminal Investigative Service's "Law Enforcement Information Exchange" (LInX) as a model.[121] Similarly, in finding 2.11, the panel uncovered that Defense guidance regarding information sharing agreements, (e.g., Memoranda of Agreements), between Defense and federal, state and local law enforcement do not mandate action and lack clear standards. The associated recommendation requires the military Departments and Defense agencies to develop formal information sharing agreements "with allied and partner agencies; Federal, State and local law enforcement; and criminal investigative agencies."[122]

Regarding "internal threats" like those posed by "lone wolf" perpetrators, the panel discovered that "DOD force protection programs and policies are not focused on internal threats." In recommendation 3.2, the panel analyzed existing programs, especially a model deemed "successful" by Naval Criminal Investigative Services and their "Threat Management Unit" and recommended that Defense "develop policies and procedures to integrate the currently disparate efforts to defend DOD resources and people from internal threats."[123]

Earlier in the study's design approach, the environmental frame system's analysis drawing identified Suspicious Activity Reporting (SAR) or Serious Incident Reports (SIR) as the "bottom-up" input mechanism into the binary system by the public, private sector organizations, the media and local law enforcement. In panel finding 3.5, they discovered that Defense does not have "access to a force protection threat reporting

[121]Ibid., 19.

[122]Ibid., 20.

[123]Ibid.

system for suspicious incident activity reports." The Assistant Secretary of Defense for Homeland Defense recommends adopting the FBI "eGuardian" secure web-based system for sharing SAR and SIR threat indications and warnings between Defense and federal, state and local law enforcement agencies. As such, this recommendation supports adopting the FBI eGuardian system as well as the appointment of a "single Executive Agent to implement, manage and oversee this force protection threat reporting system."[124]

This case study highlights several points brought out in the study's design analysis. Clearly, Defense and Justice are critical stakeholders in the information sharing environment. The two Departments share a node in the system, FBI's Joint Terrorism Task Forces, and they share information system and databases across the three classifications domains. On the surface, these linkages should have led to a more in-depth inquiry into Major Hassan's suspicious activities. However, there appears to be enduring issues with 'stove piping" of information and with ineffective ad hoc agreement mechanisms. Further, it is apparent that when it comes to harvesting, analyzing and disseminating law enforcement information, there appears to be some lingering jurisdictional confusion as to which system to use. Finally, the system in this mass casualty event was not helpful in informing first preventers and responders in managing real time operations, a clear failure of step five in the system's intelligence fusion cycle. Fort Hood Police officers had no idea who they were running up against and had no clue that a potential "lone wolf" terrorist resided in their Army Post. Interestingly, the radical

[124]Ibid., 30.

cleric linked in this event surfaced again fifty-one days later as he too was reportedly associated with the Christmas Day "underwear bomber."[125]

CASE STUDY: CHRISTMAS DAY ATTACK

> In Schiphol, his name did not appear on any terrorist screening watchlist. And so nothing pinged to keep him off of the plane. While in the air, Customs in Detroit has access to the entire TIDE database, and as we now all know that's the large mega-database; it has 500,000-plus names in it. And they knew he had a ping there, and so they were ready, when he landed in Detroit, to question him about that—that ping against the TIDE database.
>
> —Janet Napolitano, DHS Secretary[126]

On December 16, 2009, a 23-year-old Muslim Nigerian national, Umar Farouk Abdulmutallab obtained a round-trip ticket from Lagos, Nigeria to Detroit, Michigan. Without raising suspicion, he purchased his ticket using $2,831 in cash at the Accra International Airport in Gana, Nigeria.[127] On Christmas Eve, Abdulmuttalab began his twenty-seven-hour, 7,000-mile trip to blow up a transatlantic airliner over the United

[125]Jeanne Meserve and Pam Benson, "Official: Apparent Contact between Abdulmuttalab and Radical Cleric," *CNN*, (December 31, 2009), 1-2. http://www.cnn.com/2009/POLITICS/12/31 /abdulmutallab.terror.radical.cleric/index.html (accessed January 12, 2010).

[126]The White House, *Briefing by Homeland Security Secretary Napolitano, Assistant to the President for Counterterrorism and Homeland Security Brennan, and Press Secretary Gibbs, 1/7/10*, Office of the Press Secretary, (Washington, D.C.: January 7, 2010). http://www.whitehouse.gov/the-press-office/briefing-homeland-security-secretary-napolitano-assistant-president-counterterroris (accessed January 25, 2010).

[127]"Key Dates Surrounding the Christmas Day Attack," *ABC News*, (December 2009), 2. http://abcnews.go.com/Business/wirestory?id=9506563&page=2 (accessed March 6, 2010).

States and "ruin a holiday."[128] He was traveling with a Nigerian passport and a 2008, two-year, multi-entry U.S. visa obtained in London.

Arriving in Amsterdam, Holland, on Christmas Eve, he subsequently boarded Delta Airlines Flight 253, an Airbus A330 twinjet airliner operated by Northwest Airlines. He successfully passed airline-screening procedures in both Murtala Muhammad Airport in Lagos, Nigeria and Schiphol Airport in Amsterdam. The tight screening procedures at Schiphol Airport included a procedure known as "spot profiling," that involves assessing a passenger's body reactions including facial expressions, behaviors and physical gestures to reveal if that person is lying in response to a series of security related questions.[129] He passed this check with no problems. Again, the fact that he was travelling overseas with only a shoulder bag as carry-on luggage and no cold weather clothing did not raise any 'red flags' with security screeners at both the Nigerian and Holland gates. Most disappointing, this airport had seventeen full body scanners on site, but none were used to screen passengers on this particular flight. Amsterdam's Schiphol Airport officials purchased the highly controversial millimeter-wave, full-body scanner systems two years prior but were not in use on December 25, 2010, due to European Union concerns over "privacy and human rights."[130] Unable to detect hidden bomb components sewn into his underwear, he also passed both "pat down" and "metal detectors" with ease.

---

[128]"The Underwear Bomber: Detroit Plane Plot," *The Discovery Channel*, (originally aired on March 11, 2010). Hereafter cited as Discovery Channel documentary.

[129]Discovery Channel Documentary.

[130]Allegra Stratton, "Full-body Scanners Ordered for Airports says, Gordon Brown," *The Guardian*, (January 10, 2010). http://www.guardian.co.uk/world/2010/jan/03/gordon-brown-airport-body-scanners (accessed March 2, 2010).

At 11:00 p.m. on Christmas Eve, he boarded Flight 253 with a seat assignment of 19A, a window seat directly above the twinjet's wing fuel tanks. This particular seat assignment ideally located where it would facilitate breaching the airliner's hull in the event of a bomb detonation; windows being the weakest points in an otherwise extremely rigid carbon-fiber fuselage. Fellow passengers reportedly remember seeing nothing out of the ordinary from Abdulmutallab during the long flight, except that forty-minutes before the airliner began its final approach into Detroit he went into the plane's lavatory for about twenty-minutes. Airline security investigators believed that Abdulmuttalab used this lavatory visit to assemble his bomb components and execute final pre-detonation checks.[131] He returned to his seat without drawing further undue attention and completely covered himself with a blanket.[132]

As Flight 253 initiated its final twenty-minute approach into Detroit Metropolitan Airport, witnesses reported hearing "popping noises" similar to the sound made by "fire crackers." Fellow passengers then reported seeing smoke and fire rising from Abdulmutallab's window seat, with flames climbing the surrounding wall of the fuselage filing the cabin with acrid smoke. This scene prompted a fellow passenger, a Dutch filmmaker named Jasper Schuringa seated one row back in seat 20J, to dash across and over the seats, pouncing on the would-be suicide bomber who appeared to be igniting a concealed bomb in his underwear—erupting into flames on his groin and lap.[133] Suffering burns to his own hands, Schuringa pulled a burning syringe from

[131]Discovery Channel Documentary.

[132]U.S. District Court, Eastern District of Michigan, Criminal Complaint Affidavit, "U.S. v. Umar Farouk Abdulmutallab," *New York Times*, (December 26, 2009), 2. http://graphics8.nytimes.com/packages/pdf/national/20091226ComplaintAffidavit.pdf (accessed March 6, 2010).

[133]Ibid., 3-4.

Abdulmutallab's lap. He then forcibly placed his opponent in a headlock and with the help of fellow passengers and crewmembers dragged the severely burned terrorist towards the forward first class section of the plane where they doused Abdulmutallab with blankets and fire extinguishers, ripping his clothes off to search for more concealed explosives devices. Passengers restrained Abdulmutallab until the plane landed where U.S. Customs and Border Protection agents apprehended him.[134] There were no federal Air Marshals travelling on this flight.

On January 6, 2010, Abdulmutallab received a formal six-count criminal indictment from a U.S. District Court. Charges included: attempted use of a weapon of mass destruction; attempted murder within the special aircraft jurisdiction of the United States; willful attempt to destroy an aircraft; willfully placing a firearm or destructive device on an airplane; use of a firearm or destructive device; and possession of a firearm or destructive device in furtherance of a crime.[135] FBI forensic analysis of the improvised explosives device concealed and sewn into Abdulmutallab's underwear and associated, partially melted medical syringe, revealed that it consisted of bomb components including approximately eighty-grams of a powdered form of Pentearythritol, known as the high explosive PETN, and another high explosive liquid material, Triacetone Triperoxide, also known as TATP.[136] Once convicted of these charges in criminal court, Abdulmutallab, faces the prospect of spending the remainder of his life behind bars.

---

[134]Sarah Netter, "Jasper Schuringa Yanked Flaming Syringe out of Abdulmutallab's Pants," *ABC News, Good Morning America*, (December 28, 2009). http://abcnews.go.com/GMA/northwest-flight-253-hero-yanked-flaming-syringe-abdulmutallab-pants/story?id=9432099 (accessed March 6, 2010).

[135]Mueller, 3.

[136]Ibid.

This foiled terror attack reveals a telling pattern by al Qaeda. Not only do they prefer to plot and carry out high profile attacks, they continue to target the air transportation sector and have a proclivity for retrying previously failed terror attempts. Airline disasters have a unique affect on people's psyche, one that al Qaeda seems to favor. This repeated attempt being eerily similar to Richard Reid's, the "Shoe Bomber," December 2001 plot to bring down another transatlantic flight, American Airlines Flight 63, by concealing both PETN and TATP explosives in his shoes.[137] Interestingly, this same "shoe bomber" plot led to more comprehensive airline pre-boarding screening procedures across the global air transportation industry, including full body scanners which would have detected Abdulmuttalab's concealed bomb, the very procedures that failed to raise suspicions and detect the hidden bomb on December 25, 2009. Further, four months earlier, al Qaeda tipped its hand on the future use of PETN and TACP when another al Qaeda-trained suicide bomber detonated while attempting to assassinate Saudi officials in Yedda, Saudi Arabia.[138] Many consider the particular attack a "trial run" for the one later planned over North America.

What did the supra-system contain about this 23-year-old Nigerian national? By all accounts, there was enough intelligence in the information sharing environment on Abdulmutallab before he boarded this fateful flight. The U.S. Embassy in London issued his two-year visa on June 16, 2008 and subsequently entered its details into the Advance Passenger Information System (APIS).[139] Homeland Security's Customs and Border

---

[137]"Judge Denies Bail to Accused Shoe Bomber," *CNN*, (December 21, 2001). http://archives.cnn.com/2001/US/12/28/inv.reid/ (accessed January 22, 2010).

[138]Discovery Channel Documentary.

[139]Tettersall, 2.

Protection agency uses this database to screen and monitor international travelers and to expedite customs clearing procedures. For air travel, Customs and Border Protection requires airlines to submit passenger manifests to its APIS system. In February 2008, APIS submissions were mandated to be transmitted in advance of passenger check-in.[140] In May 2009, Britain denied Abdulmutallab his visa application to attend a non-government approved institution, alerting the greater European security community of his suspicious inclinations. Having been denied entry into Great Britain, he opted to attend a school in Sana'a, Yemen from August through December 2009 to study Arabic.

His visit to Yemen probably establishes the most critical 'dot' in the information sharing system. On November 18, 2009, his father, Alhaji Umar Mutallab, the Chairman of a large Nigerian bank, approached authorities expressing concern over his son's illicit activities in Yemen—Yemen fast becoming the world's terror capital. He reported his son's possible collusion with and potential "radicalization" by Islamic extremists to U.S. Embassy intelligence officials in Abuja, Nigeria.[141] This credible admission and warning prompted the embassy in Abuja to send a "VISAS VIPER" cable with the information from Abdulmutallab's father to all U.S. diplomatic missions and State in Washington and the National Counterterrorism Center for review. The National Counterterrorism Center entered Abdulmutallab's name into the Terrorist Identities Datamart Environment (TIDE) database.[142] Curiously, as the epigraph in the beginning of this case study revealed, Custom's and Border Protection officials were alerted of Abdulmuttalab's name in the

[140]For more information on APIS, see the Transportation Security Administration (TSA) web page at: http://www.checktsa.com/apis.stm/apis (accessed February 12, 2010).

[141]"Key Dates Surrounding the Christmas Day Attack,"2.

[142]Discovery Channel Documentary.

TIDE database while the airliner was already in flight to Detroit. According to established procedures, Customs and Border Protection's National Targeting Center, located in Reston, Virginia, screen the TIDE database only after receiving the airline's flight passenger manifest. Again, screening occurs when the airliner is already in flight to the United States.[143] This procedural 'dot' in the system did not result in an emergency directive to the doomed airliner to return to Amsterdam, too late for this measure to have prevented the successful execution of this plot. This established procedure, a component of Homeland Security's The Enforcement Communications System (TECS) within the wider Terrorist Screening Database (TSDB) is a flaw in the system that is one of many currently under review.[144] Yet another 'dot' resided within the Intelligence Community that should have triggered sirens to sound for terror watchlist screeners. In September 2009, the National Security Administration had intercepted conversations between al Qaeda extremists in Yemen that referenced a plot to use a "Nigerian" for an upcoming attack in the United States. This information resided in the highest classified domains of the Intelligence Community and was made available to the National Counterterrorism Center.[145] The intelligence received regarding intercepted communications between al Qaeda-affiliated groups referenced three telltale words, "Umar," "Farouk," and

[143]Ibid.

[144]Senate Committee on Homeland Security Governmental Affairs, "Testimony by Mr. Timothy J. Healy, Director, FBI Terrorist Screening Center," *Federal Bureau of Investigation*, (Washington, D.C.: March 10, 2010), 1-6. http://www.fbi.gov/congress/congress10/healy031010.htm (accessed March 13, 2010).

[145]Mark Mazzetti and Eric Lipton, "Spy Agencies Failed to Collate Clues on Terror," *New York Times*, (December 31, 2009). http://www.nytimes.com/2009/12/31/us/31terror.html?pagewanted=all (accessed March 5, 2010).

"Nigerian."[146] The system was dealing with a Sunni threat. Having the future suicide bomber's first name, Islamic sect and nationality, the Intelligence Community should have "connected these dots" and placed Umar Farouk Abdulmuttalab on the most restrictive terror watchlist of all—the "No-Fly" list.[147]

Further, in the post-mortem investigation, press reports revealed an embarrassing error in the spelling of Abdulmutallab's name by either State or National Counterterrorism Center officials that may have contributed to a delay in connecting Abdulmutallab's to the correct watch list. The President's preliminary inquiry labeled this glitch as, "a series of human errors occurred—delayed dissemination of a finished intelligence report and what appears to be incomplete/faulty database searches on Abdulmutallab's name and identifying information."[148]

United States Government Corrective Actions

Once the dust settled on what the system knew about this terror plot, President Obama stood before the nation and accepted full responsibility for the "systematic" failures to "connect the dots" by the intelligence and counterterrorism communities. The President's mea culpa, however, should not absolve the stakeholders in the nation's information sharing environment from working more effectively with each other. No

[146]Schimmel, 19-20. Oddly the name "Umar," is a Sunni throwback to "Umar Ibn al-Khattab (CE 634-644), who succeeded Abu Bakr, the Prophet Muhammad's confidant and successor. The fact that intelligence referred to a Sunni perpetrator should have alerted terrorist analysts of the potential threat.

[147]Discovery Channel Documentary.

[148]The White House, *Summary of the White House Review of the December 25, 2009 Attempted Terrorist Attack*, (Washington, D.C.: January 8, 2010), 6. http://www.whitehouse.gov/sites/default/files/summary_of_wh_review _12-25-09.pdf (accessed January 8, 2010). Hereafter cited as summary of White House Review of December 25, 2009 Terrorist Attack.

doubt, progress has been made since the traumatic events of September 11, 2001, but there is still some room for improvement. Collaboration between Justice and Homeland Security has, in fact, vastly improved over the last five years, exemplified by a steady stream of co-authored and published policy documents highlighted earlier in this study. However, the same cannot be said regarding the status of collaboration between State and Homeland Security, especially in the area of visa security matters. On December 25, 2009, Abdulmutallab's visa was not even revoked on the day he attempted to down an airliner over North America. This awkward oversight in the glare of the media spotlight prompted the President to direct the following corrective action of State, "Review visa issuance and revocation criteria and processes, with special emphasis on counterterrorism concerns; determine how technology enhancements can facilitate and strengthen visa-related business processes."[149] The relationship between State and Homeland Security, being rather poor, contributed to the lack of information sharing between the Nigerian consular office, run by State, and Homeland Security.[150]

Finally, of the nine key findings released in the President's unclassified preliminary inquiry and review, the following two highlight pervasive obstacles to effective information sharing in the nation's information sharing environment:

- NCTC and CIA personnel who are responsible for watchlisting did not search all available databases to uncover additional derogatory

[149]The White House, *Memorandum for the Heads of Executive Departments and Agencies, Subject: Attempted Terrorist Attack on December 25, 2009: Intelligence, Screening and Watchlisting System Corrective Actions,* (Washington, D.C.: January 7, 2010). http://www.whitehouse.gov/ sites/default/files/potus_directive_corrective_actions_1-7-10.pdf (accessed January 7, 2010).

[150]Jena Baker McNeill, "Six Questions for Detroit Terror Plot Hearings," WebMemo No. 2749, *The Heritage Foundation*, (January 8, 2010), 2. http://www.heritage.org/Research/ HomelandSecurity /wm2749.cfmn (accessed January 22, 2010).

information that could have been correlated with Mr. Abdulmutallab to the Intelligence Community.

- Information technology within the CT [counterterrorism community] did not sufficiently enable the correlation of data that would have enabled analysts to highlight the relevant threat information.[151]

Does al Qaeda deserve credit here for choreographing a near-perfect terror plot? After all, it appears as if too many 'dots' were aligned in their favor. First, the perpetrator, a military-aged Muslim male, known to have recently traveled to Yemen, a known al Qaeda safe haven, travels to the U.S. on one of the most iconic dates in the Judeo-Christian calendar. Second, he purchases international tickets with cash. Third, this same individual, denied entry into Great Britain previously, has the circumstances behind the event recorded within the European intelligence community and is brought to the attention of U.S. intelligence officials by his father's candid personal warning. This particular alarm should have been deafening to the U.S.-European intelligence communities. Fourth, the perpetrator's first name and nationality were resident within the nation's highest classified database domains of the Intelligence Community one month prior to the attempted attack. Fifth, he boarded two back-to-back international flights with only carry-on luggage and no winter clothing, even though he was travelling to a cold weather region in December. Most of North America lay blanketed in deep snow from an unusually harsh series of mid-December winter storms. Sixth, Schiphol Airport's full body scanners, all seventeen systems, were not in use that day. Seventh, in accordance to established TSA procedures, the watchlisting system activates cross-domain passenger manifest screening only after the airliner departed. Finally, the perpetrator was travelling in a U.S.-bound transatlantic airliner without Federal Air

[151]"Summary of White House Review of the December 25, 2009 Terrorist Attack," 5.

Marshals. Had TSA officials connected the dots sooner on this suspected international traveler they could have directed that an Air Marshal travel on the same flight.

The alignment of these 'dots' makes this case study a new "classic example" of systemic failures in a United States government-owned enterprise. Domestic and international security officials will study this plot for years to come. The nation was lucky in that this al Qaeda-inspired perpetrator was extremely incompetent and a visiting foreign national had the guts to act when others cowered in fear. Next time, and al Qaeda's track record indicates that there will be a next time, America may not be so lucky.

Clearly, the two case studies outlined here reveal that despite massive government efforts to improve the nation's overarching homeland security apparatus gaps remain. It remains to be seen what lessons the Republic learns from these recent terror-related attacks and how quickly they are implemented before the next attack.

CONCLUSIONS AND RECOMMENDATIONS

> Just as today's threats to our national security and strategic interests are evolving and interdependent, so too must our efforts to ensure the security of our homeland reflect these same characteristics. As we develop new capabilities and technologies, our adversaries will seek to evade them, as was shown by the attempted terrorist attack on Flight 253 on December 25, 2009.
>
> —Janet Napolitano, DHS Secretary[152]

Today, the nation remains vulnerable to attack. In 2009, the nation was once again profoundly surprised by terrorism as a global form of twenty-first-century warfare despite nearly a decade's worth of massive government-wide reorganization and resourcing efforts, efforts specifically designed to shore up an enormous homeland security structure and its underlying information sharing supra-system. The two terror-related events outlined in this study, separated by a mere fifty-one days, tested the very framework and logic behind the nation's complex information sharing environment.

As before, the nation's brave first responders, represented in the Fort Hood rampage by police officers Munley and Todd, had no idea when they responded to a flood of local 911 calls that they would be risking their very lives arriving on a scene of sheer carnage and terror. They were utterly surprised despite the fact that a regional FBI Joint Terrorism Task Force and the Army's Criminal Investigation Command shared suspicious activity reporting that a U.S. Army commissioned officer residing at their Post had radical leanings and was in active contact with an Islamic extremist. Similarly, on Christmas Day, 289 passengers, including a young gutsy Dutch citizen, had no idea that

[152]U.S. Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland,"* (Washington, D.C.: February 2010), iii. http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf (accessed March 11, 2010).

they were travelling on a suicide mission despite nearly two months worth of intelligence and information indicating otherwise. These two specific attacks, alarming as they were, revealed the current state of affairs in the nation's information sharing system.

The system essentially defined in this study as binary in nature by applying the Army's design approach, is structured to spring into action on one end by pulling intelligence and information into it from a vast network of internal domestic sources and on the other by external foreign partner sources. The two case studies explored here illustrate that the system pulled credible information and intelligence from both ends, yet failed to push it to the first preventers on both ends, negating the principle of "sharing." This notion lends credence to the complaint by Homeland Security officials in a recent audit that, "[Information Sharing] means information going to the JTTF [Joint Terrorism task Force] and very little coming back."[153]

This study outlined that four enduring challenges to information sharing continue to burden stakeholders in the nation's information sharing environment. One challenge being political distraction. 2009 was a historic year by many accounts. The nation elected its first-ever afro-American President who assumed the reins of government under an ambitious domestic political agenda and an unending stream of global national security and socioeconomic challenges. In a domestic political environment marked by divisive partisan politics, ongoing efforts to improve the existing information sharing environment simply lost momentum, crowded out of the public spotlight by policy agenda items of higher priority. This problem was emblematic in the very entity charged with managing and refining the nation's information sharing environment—the Program

[153]Bean, 9.

Manager for Information Sharing Environment (PM-ISE) web site. Its web site (*www.ise.gov*) has become a national information sharing policy time capsule, the last posting conspicuously stopping in July 16, 2008, indicating very little progress in the evolution of information sharing policy during President Obama's first year in office. It remains to be seen if the Obama administration will re-publish its version of a National Information Sharing Strategy as a means of rectifying existing failures, especially in the wake of the much-publicized terror-related events of 2009.

Second, the Fort Hood rampage exposed a chink in Defense efforts to address threats from within the nation's borders. Largely focused on fighting two prolonged wars across the globe, Defense admittedly lost its attention on addressing internal threats including "lone wolf" conspirators that are in the words of the FBI Director "increasingly self-radicalized, self-trained and self-executing."[154] The Defense, Justice and Homeland Security communities must take a hard look at the findings of a series of independent and bipartisan reviews related to the Fort Hood rampage and retool internal, Departmental force protection policies and procedures to thwart future attacks of this nature.

Third, the information sharing community has too many independent database systems; one Department of Justice funded study found 266, which are not user-friendly to the very end-user consumers of information and intelligence.[155] This problem is compounded by the proliferation of information database systems across the community of interest operating across three national classification domains. End users face a backlog of background security checks to gain access to classified terminals, an organizationally-driven culture to over-classify data, and a pervasive sense that highly

[154]Mueller, 2.

[155]Wagner, 4.

classified information and intelligence is of higher quality than that made available by public means. The PM-ISE mandated by law to establish and develop the very environment by which the greater community of interest continues to face a myriad of challenges. The nation may benefit by exploring partnerships with private sector, information management enterprises, like Google, that have demonstrated proficiency in managing immense volumes of data.[156] This problem area is one that Congress can shape with focused and renewed oversight.

Finally, the information sharing environment must tackle the issue of trust. Trust defined here as end users of information and intelligence feeling comfortable in sharing sensitive investigative data and case files across multiple jurisdictions. This problem, revealed by the Fort Hood attack investigative panel as being caused by ill-defined business practices within ad hoc agreements between multi-jurisdictional entities within the FBI's Joint Terrorism Task Forces. Identified as a problem in the Defense investigation of the Fort Hood rampage, procedural agreements between Justice and Defense must close existing loopholes to exchanges of information affecting public safety and security. Additionally, military commanders must be included in the information sharing enterprise, specially involving derogatory information about members within their commands so they can exercise their authority to intervene before the onset of the next disaster.

This study applied the Army's 'design' approach as a tool for gaining a greater appreciation of the nature of the nation's information sharing environment—an ill-structured and wicked problem. Having tested the approach, one finding and one

[156]Norman J. Ornstein, "Congress Must Re-examine Its Role on Security Matters," *American Enterprise Institute (AEI)*, (January 13, 2010), 1-2. http://www.aei.org /article/101522 (accessed February 22, 2010).

recommendation to future design practitioners and researchers are worth highlighting here.

First, the environmental frame component of design methodology proved to be most helpful. Going through the effort of mapping the information sharing environment from multiple references resulted on the surface in developing a rather complicated system drawing. However, stepping back and visualizing this mapping of a supra-system enabled it to be essentially defined as binary in nature. Once it became apparent in the environmental frame that the system's logic depends on information being "pulled-in" from two ends, internal and external, and is supposed to "push-out" fused products to end users through a framework of multi-agency stakeholders. The problem that emerged was that the Fort Hood rampage and the Christmas Day attack represented failures on both output ends of the defined system. Further, identifying the associated system tensions, both positive and negative, added the needed context for understanding its tendencies—observed, desired and undesired. Again, mapping out the system's trajectory provided insight into the efficacy of existing strategies applied by the United States government to steer it from observed to desired end states.

Second, design doctrine clearly advises convening a 'design team' to better define the ill-structured problem present. This study did not employ a team; as such, its findings and recommendations are subject to personal bias and lack of expertise in subject matters outside a single person's personal body of knowledge. Ideally, if one were to form a design team to address this study's subject matter, that team would be relatively small, (preferably less than ten members), with representation by individuals from across the information sharing environment community of interest. Adding representatives from the

ACLU or CDT to this team, representing a contrarian view, would also ensure that the group does not succumb to the influence of groupthink and that the privacy and civil liberties of the most valuable stakeholder in the system—American citizens—be taken into account.

Al Qaeda, leading a global terror franchise, will continue to generate strategic surprises and security challenges well into the first half of the twenty-first-century, requiring an agile, adaptive and dependable information sharing environment to thwart them at every turn. Al Qaeda and its offshoot affiliates are not a "threat"—they are an active enemy engaged in active hostilities against the United States. They continue to be at war with the United States and its allies, whether or not we choose to be at war with them. Al Qaeda constantly back up their threats with actions, including attempts—fortunately unsuccessful on December 25, 2009—to attack the U.S. homeland. To be sure, they continue their maniacal quest to acquire any form of weapons of mass destruction and they will not hesitate to use them.[157] Next time, failure of America's Homeland Security community to effectively pull, analyze, fuse and push credible indications and warnings of imminent attacks involving al Qaeda's acquisition and use of weapons of mass destruction will be catastrophic indeed.

[157]Thomas Donnelly and Frederick W. Kagan, *Ground Truth: The Future of U.S. Land Power*, Washington, D.C.: American Enterprise Institute Press, 2008, 15.

APPENDIX A
ABBREVIATIONS AND ACRONYMS

ACLU	American Civil Liberties Union
APAN	Asia Pacific Area Network
APIS	Advance Passenger Information System
CAC	Common Access Card
CACD	Commander's Appreciation and Campaign Design
CBRNE	Chemical, Biological, Radiological, Nuclear or High-yield Explosives
CDT	Center for Democracy and Technology
CENTRIXS	Combined Enterprise Regional Information Exchange System
CIA	Central Intelligence Agency
COI	Communities of Interest
CRS	Congressional Research Service
CT	Counterterrorism
CUI	Controlled Unclassified Information, information handling caveat
DCI	Director of Central Intelligence
DCO	Defense Coordinating Officer
DHS	U.S. Department of Homeland Security
DNI	Director of National Intelligence
DOD	U.S. Department of Defense
DOJ	U.S. Department of Justice
DOS	U.S. Department of State
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FOUO	For Official Use Only, information handling caveat
FPS Portal	Federal Protective Services Portal
GAO	U.S. General Accounting/ Government Accountability Office
HSA	Homeland Security Act (Public Law 107-296, November 25, 2002)
HSC	Homeland Security Council
HSDN	Homeland Secure Data Network
HSIN-I	Homeland Security Information Network-Intelligence (DHS)
HSPD	Homeland Security Presidential Directive
INTELINK-U	Intelligence Community Intranet, Unclassified
INTERPOL	International Criminal Police Organization
IRTPA	Intelligence Reform and Terrorism Prevention Act (Public Law 108-458, December 17, 2004)
ISC	Information Sharing Council
ITACG	Interagency Threat Assessment and Coordination Group
JDISS	Joint Deployable Intelligence Support System
JFHQ-State	Joint Force Headquarters in every State (NGB)
JFO	Joint Field Office
JTF-CS	Joint Task Force-Civil Support (DOD)
JTTF	Joint Terrorism Task Force (FBI)
JWICS	Joint Worldwide Intelligence Communications System
LEA	Law Enforcement Agency
LEO	Law Enforcement Online (FBI)
LES	Law Enforcement Sensitive, information handling caveat

LInX	Law Enforcement Information Exchange (FBI)
MNCE	Multi-National Collaboration Environment
NCTC	National Counterterrorism Center
N-DEX	National Data Exchange (FBI)
NGB	National Guard Bureau
NIEM	National Information Exchange Model
NIPRNet	Non-Secure Internet Protocol Router Network
NIS	National Intelligence Strategy
NOL-S	National Counterterrorism Center Online-Secret (NCTC)
NOC	National Operations Center (DHS)
NSC	National Security Council
NSIS	National Strategy for Information Sharing (ODNI)
NSPD	National Security Presidential Directive
NTC	National Targeting Center
ODNI	Office of the Director of National Intelligence
OIF	Operation Iraqi Freedom
PETN	Pentearythritol (high explosives)
PIN	Personal Identifiable Number
P. L.	Public Law
PM-ISE	Program Manager-Information Sharing Environment
POTUS	President of the United States
QHSR	Quadrennial Homeland Security Review (DHS)
RFA	Request for Assistance
RISSnet	Regional Information Sharing Systems Secure Intranet
SAR/ SIR	Suspicious Activity Reporting/ Suspicious Incident Reports
SBU	Sensitive But Unclassified, information handling caveat
SIPERNet	Secret Internet Protocol Router Network
TATP	Triacetone Triperoxide (high explosives)
TECS	The Enforcement Communications System (DHS)
TIDE	Terrorist Identities Datamart Environment
TRIPwire	Technical Resources for Incident Prevention (DHS)
TS	Top Secret, information handling caveat
TSC	Terrorist Screening Center (FBI)
TS/ SCI	Top Secret/ Sensitive Compartmented Information, information handling caveat
TSA	Transportation Security Administration
TSDB	Terrorist Screening Database
TTIC	Terrorist Threat Integration Center
UCore	Universal Core
U.S.	United States
U.S.C.	United States Code
USCG	United States Coast Guard (DHS/ DOD)
WMD/ E	Weapons of Mass Destruction/ Effects

APPENDIX B
ILLUSTRATIONS

Figure 1, System Stakeholder Relationships

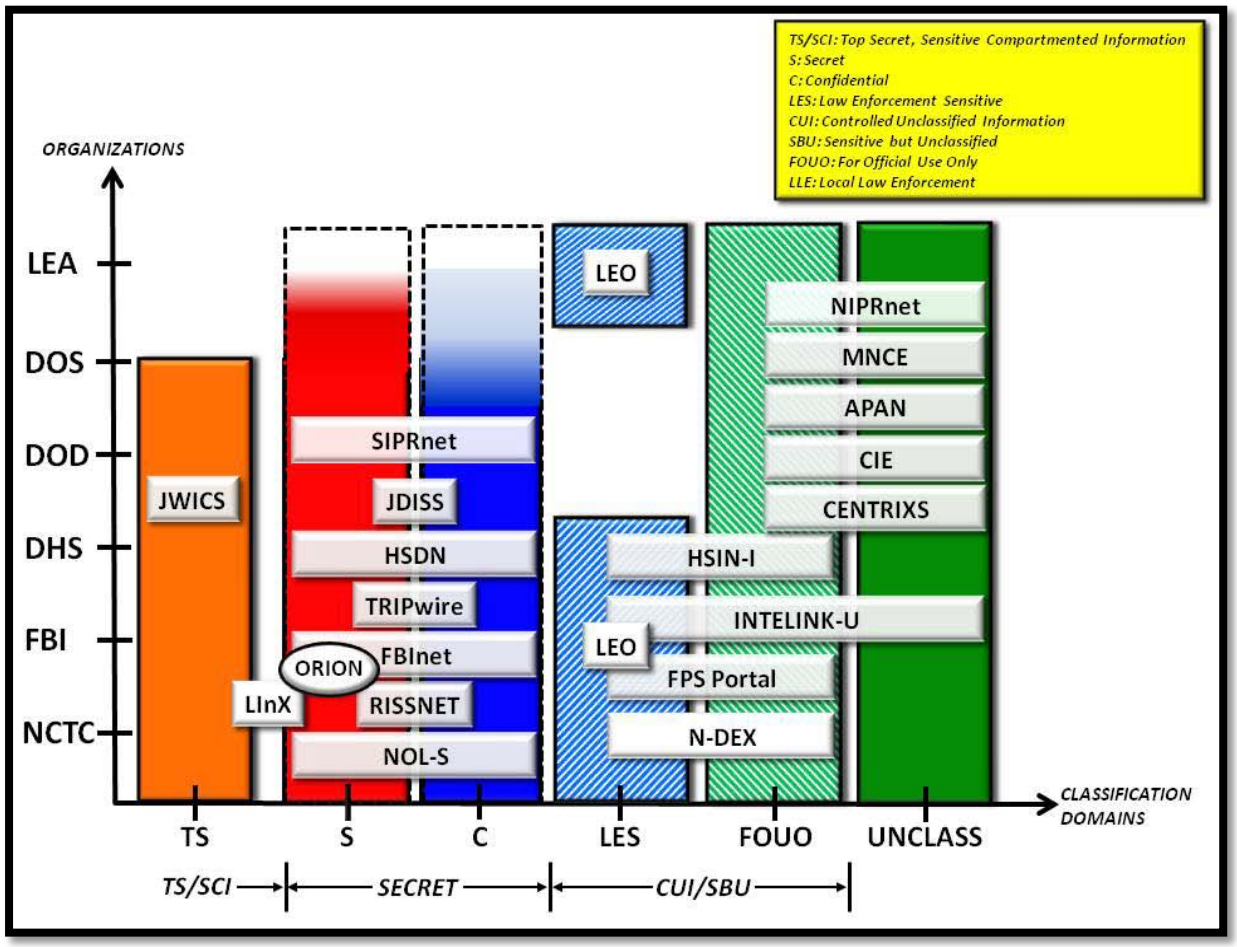

Figure 2, Stakeholder Database Systems

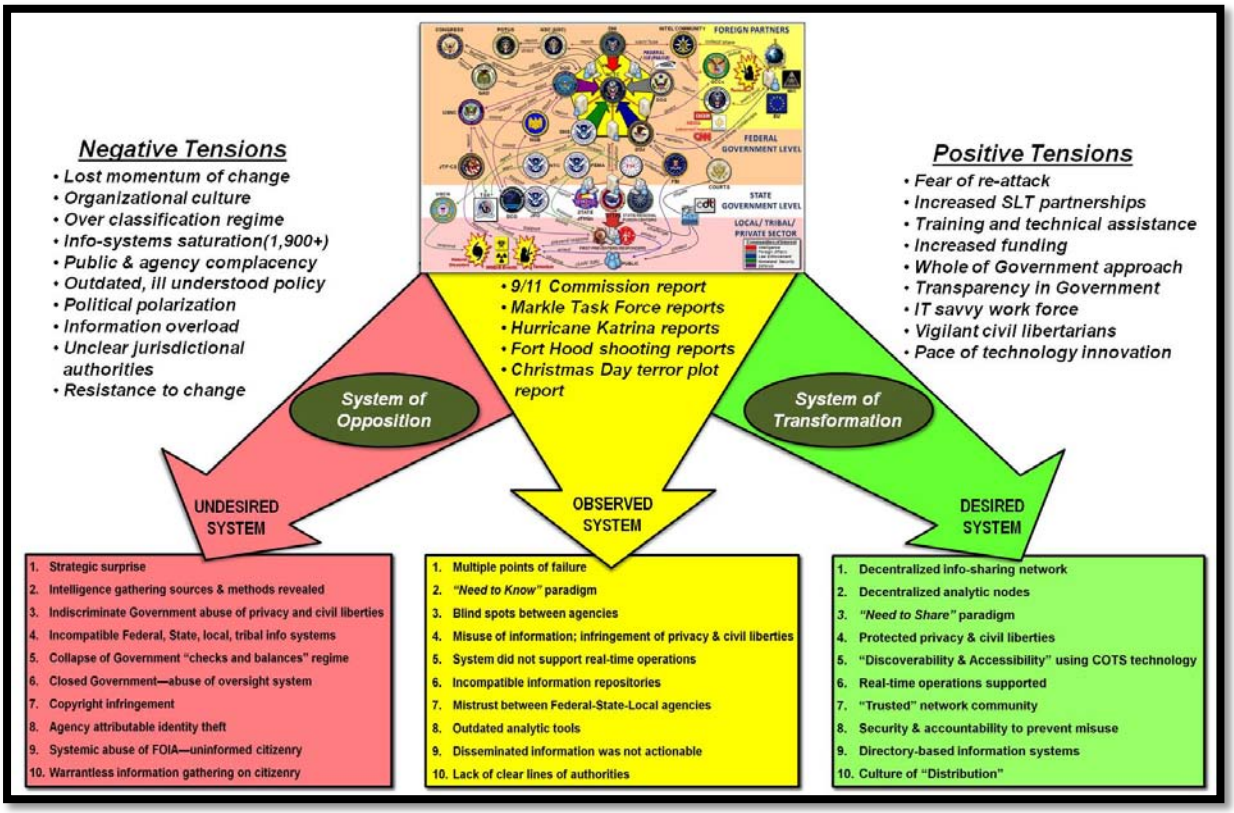

Figure 3, The Environmental Frame

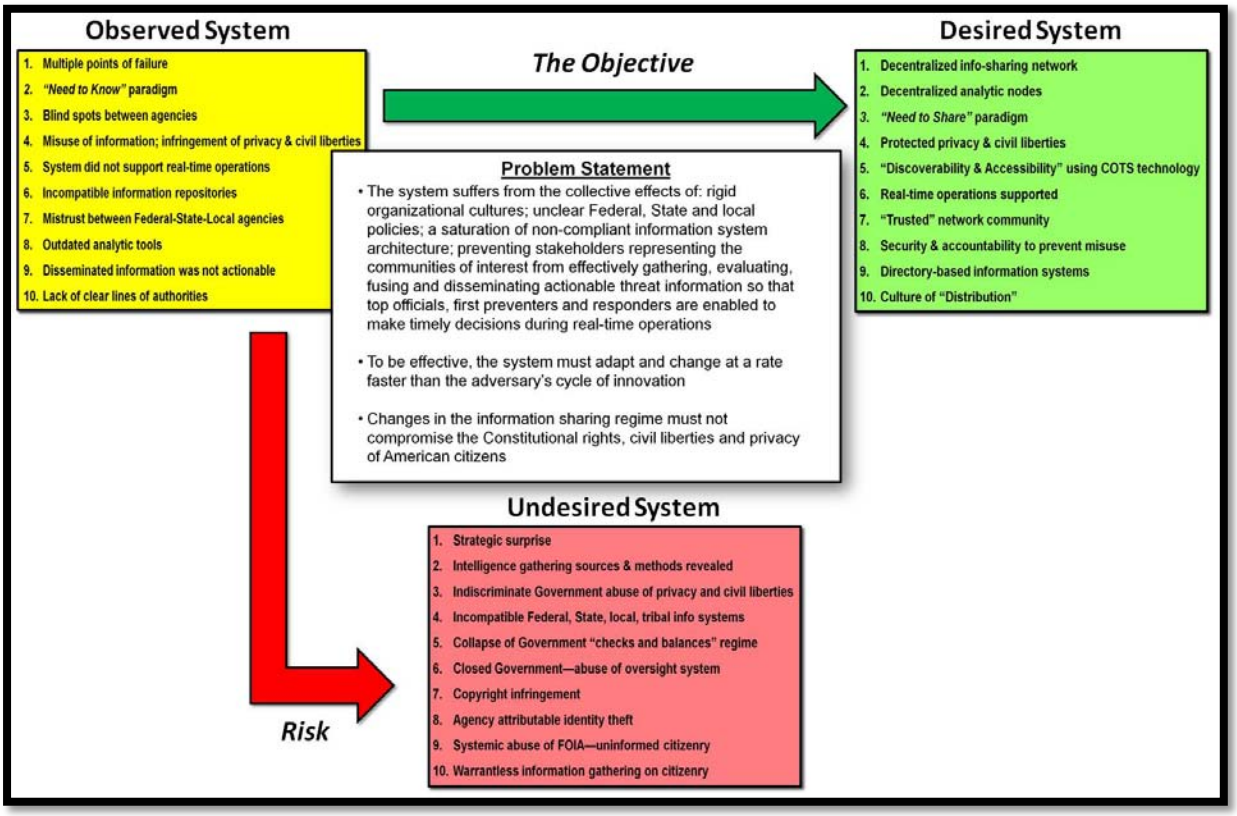

Figure 4, The Problem Frame

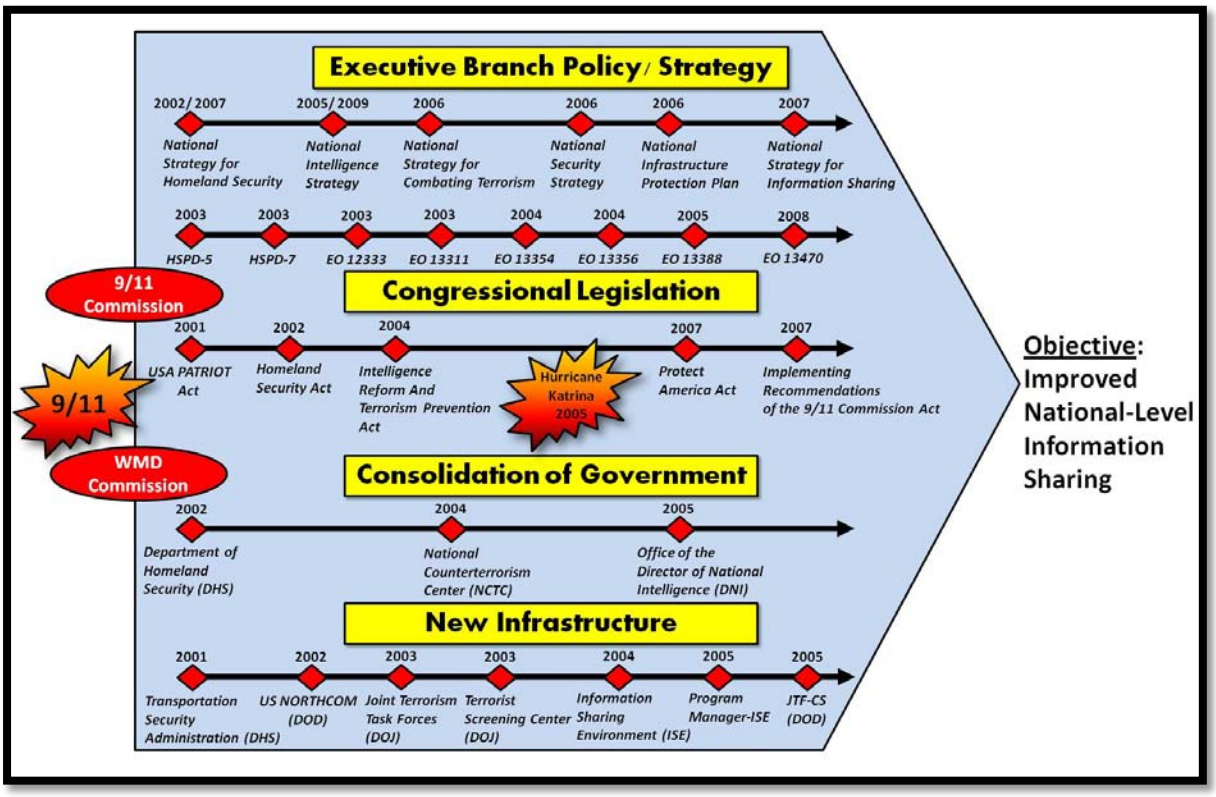

Figure 5, Solution Frame (National Lines of Effort)

BIBLIOGRAPHY

Published Sources:

Bertalanffy, Ludwig von. *General System Theory: Foundations, Development, Applications.* Revised Edition, New York, NY: George Braziller Inc., 1993.

Chertoff, Michael and Lee H. Hamilton. *Homeland Security, Assessing the First Five Years*. Philadelphia, PA: University of Pennsylvania Press, 2009.

Donnelly, Thomas, and Frederick W. Kagan. G*round Truth: The Future of U.S. Land Power.* Washington, D.C.: American Enterprise Institute Press, 2008.

Gharajedaghi, Jamshid. *Systems Thinking, Managing Chaos and Complexity: a Platform for Designing Business Architecture.* Burlington, MA: Elsevier Inc., 2006.

Gott, Kendall D., and Michael G. Brooks, ed. *The U.S. Army and the Interagency Process: Historical Perspectives.* Fort Leavenworth, KS: Combat Studies Institute Press, 2008.

Laqueur, Walter, ed. *Voices of Terror: Manifestos, Writings, and Manuals of Al Qaeda, Hamas, and other Terrorists from Around the World and Throughout the Ages.* New York, NY: Reed Press, 2004.

Lazlo, Ervin. *The Systems View of the World, a Holistic Vision for our Time*. Cresskill, NJ: Hampton Press, Inc., 1996.

O'Hanlon, Michael, E., with Peter R. Orszag, Ivo H. Daalder, I. M. Destler, David L. Gunter, James M. Lindsay, Robert E. Litan, and James B. Steinberg. *Protecting the American Homeland, One Year On.* Washington, D.C.: Brookings Institution Press, 2002.

Ridge, Tom with Larry Bloom. *The Test of Our Times: America Under Siege and How We Can Be Safe Again.* New York: Thomas Dunne Books, 2009.

Schimmel, Annemarie. *Islam: An Introduction.* Albany, NY: State University of New York Press, 1992.

Sauter, Mark, A., and James, Jay, Carafano. *Homeland Security: a Complete Guide to Understanding, Preventing, and Surviving Terrorism*. New York: McGraw-Hill, 2005.

Tenet, George with Bill Harlow. *At the Center of the Storm, My Years at the CIA.* New York: Harper Collins Publishers, 2007.

"The Resurgence of al-Qaeda, the Bombs that Stopped the Happy Talk." *The Economist*, (January 30th-February 5th, 2010).

Articles Published Online:

"Al Qaeda Claims Christmas Day US Flight Bomb Plot." *BBC News*, (December 28, 2009). http://news.bbc.co.uk /2/hi/middle_east/8433151.stm (accessed March 4, 2010).

Banach, Stefan J., and Alex Ryan. "The Art of Design, A Design Methodology." *Military Review* (April 30, 2009). http://usacac.army.mil/CAC2/ MilitaryReview/Archives /English /MilitaryReview_20090430_art016.pdf (accessed January 12, 2010).

Barnes, Steve, and James Dao. "Gunman Kills Soldier Outside Recruiting Station." *New York Times*, (June 2, 2009). http://www.nytimes.com/2009 /06/02/us/ 02recruit.html (accessed January 10, 2010).

Bender, Bryan. "Fort Hood Suspect was an Army Dilemma." *The Boston Globe*, (February 22, 2010). http://www.boston.com/news/nation/washington /articles/2010/02/22/ ft_hood_ suspect_was_army_dilemma/ (accessed March 6, 2010).

Cohen, Eliot. "What's Different About the Obama Foreign Policy?" *Wall Street Journal*, August 2, 2009. http://online.wsj.com/article/SB10001424052970203946904574300402 608475582.html (accessed December 12, 2009).

Cooper, Aaron, with Tedd Rowlands, Barbarra Starr, and Brian Todd. "Fort Hood Suspect Charged with Murder." *CNN*, (November 12, 2009). http://www.cnn.com/2009/ CRIME/11/12/fort.hood.investigation/index.html (accessed March 6, 2010).

Curtis, Lisa, with Matt Mayer, Jena Baker McNeill, and Charles Stimson. "Christmas Day Terror Plot Highlights Need to Sharpen Intelligence System." Web Memo No., 2751, *Heritage Foundation*, (January 8, 2010). http://www.heritage.org /Research/Reports/2010 /01/Christmas-Day-Terror-Plot-Highlights-Need-to-Sharpen-Intelligence-System (accessed March 4, 2010).

Elliot, Phillip. "Quiet Christmas Day for Obama's in Hawaii." *The Seattle Times*, December 25, 2009. http://seattletimes.nwsource.com/html/nationworld/ 2010598353_obamaday26.html (accessed January 9, 2009).

"Fort Hood Shootings: the meaning of 'Allahu Akbar.'" *The Telegraph.* (November 6, 2009). http://www.telegraph.co.uk/news/worldnews/northamerica/ usa/6516570/ Fort-Hood-shootings-the-meaning-of-Allahu-Akbar.html (accessed January 16, 2010).

Griffin, Drew, with Elaine Quijano, Carroll Cratty and Brian Todd. "Profiler: Fort Hood Suspect a Loner." *CNN*, (November 12, 2009). http://www.cnn.com/ 2009/ CRIME/11/11/ texas.fort.hood.investigation/index.html (accessed March 6, 2010).

Jakes, Larra, and Devlin Barret. "AP Sources: Rampage Gun Purchased Legally." *Seattle Times*, (November 6, 2009). http://seatletimes.nwsource.com /html/politics/ 2010219175 _apusforthoodshootinggun.html (accessed March 10, 2010).

Jenkins, Brian, Michael. "Opinion: How a Decade of Terror Changed America." *AOL News*, (December 30, 2009). http://www.aolnews.com/opinion/article/opinion-how-a-decade-of-terror-changed-america/19298174 (accessed January 25, 2010).

Johnston, David, and Scott Shane. "U.S. Knew of Suspect's Tie with Radical Cleric." *New York Times*, (November 10, 2009). http://www.nytimes.com/2009/11/10/us/ 10inquire. html?_r=1 (accessed March 5, 2010).

"Judge Denies Bail to Accused Shoe Bomber." *CNN*, (December 21, 2001). http://archives.cnn.com/2001/US/12/28/inv.reid/ (accessed January 22, 2010).

Jurkowitz, Mark. "The Army Base Massacre Dominates the Week." *Pew Research Center's Project for Excellence in Journalism (PEJ)*, (November 2-8, 2009). http://www.journalism.org/index_report/pej_news_coverage_index_november_28 _2009 (accessed January 12, 2010).

"Key Dates Surrounding the Christmas Day Attack." *ABC News*, (December 2009). http://abcnews.go.com/Business/wirestory?id=9506563&page=2 (accessed March 6, 2010).

Meserve, Jeanne, and Pam Benson. "Official: Apparent Contact between Abdulmuttalab and Radical Cleric." *CNN*, (December 31, 2009). http://www.cnn.com/2009 /POLITICS/12/31 /abdulmutallab.terror.radical. cleric/index.html (accessed January 12, 2010).

Mazzetti, Mark, and Eric Lipton. "Spy Agencies Failed to Collate Clues on Terror." *New York Times*, (December 31, 2009). http://www.nytimes.com/2009/12/31/us/ 31terror.html? pagewanted=all (accessed March 5, 2010).

McCaffrey, Barry, General (Ret.). Interview with CNN Anchor, Anderson Cooper. "Investigating Fort Hood Massacre." CNN, *Anderson Cooper 360 Degrees*, November 6, 2009. http://transcripts.cnn.com/TRANSCRIPTS/0911 /06/acd.01.html (accessed March 6, 2010).

McFadden, Robert, D. "Army Doctor Held in Fort Hood Rampage." *New York Times*, (November 6, 2009). http://www.nytimes.com/2009/11/06/us/ 06forthood.html? _r=1&pagewanted=2 (accessed March 8, 2010).

McKinley, James, C., Jr. "Second Officer Gives Account of Shooting at Fort Hood." *New York Times*, (November 12, 2009). http://www.nytimes.com/2009/11/13/us /13hood.html ?pagewanted=1&_r=3&hp (accessed March 8, 2010).

McNeill, Jena, Baker. "Six Questions for Detroit Terror Plot Hearings." WebMemo No. 2749, *The Heritage Foundation*, (January 8, 2010). http://www.heritage.org /Research/ HomelandSecurity/wm2749.cfmn (accessed January 22, 2010).

Netter, Sarah. "Jasper Schuringa Yanked Flaming Syringe out of Abdulmutallab's Pants." *ABC News, Good Morning America*, (December 28, 2009). http://abcnews.go.com/GMA/ northwest-flight-253-hero-yanked-flaming-syringe-abdulmutallab-pants/ story?id= 9432099 (accessed March 6, 2010).

Ornstein, Norman J. "Congress Must Re-examine Its Role on Security Matters." *American Enterprise Institute*, (January 13, 2010). http://www.aei.org /article/101522 (accessed February 22, 2010).

"PHOTOS Passengers help foil Christmas Day attack on Detroit-bound plane; terrorist charged." *Naplesnews.com*, (December 26, 2009). http://www.naplesnews.com /news/2009/dec/26/ terrorist-attempt-passengers-help-foil-christmas-d/ (accessed March 4, 2010).

Rittel, Horst, W.J., and Melvin W. Webber. "Dilemmas in the General Theory of Planning." *Policy Sciences 4*, Amsterdam: Elsevier Scientific Publishing Company, (1973). http://www.metu.edu.tr/~baykan /arch467/Rittel+Webber+ Dilemmas.pdf (accessed March 15, 2010).

Ross, Brian, and Rhonda Schwartz. "Major Hassan's email: 'I Can't Wait to Join You' in Afterlife." *ABC News*, (November 19, 2009). http://abcnews.go.com/Blotter/ major-hassans-mail-wait-join-afterlife/story?id=9130339 (accessed January 12, 2010).

Shapiro, Jeremy, "Managing Homeland Security, Developing a Threat-Based Strategy." *Brookings Institution*, (February 28, 2007). http://www.brookings.edu/ papers/2007/0228terrorism_shapiro_Opp08.aspx (accessed October 30, 2009).

Stratton, Allegra. "Full-body Scanners Ordered for Airports says, Gordon Brown." *The Guardian*, (January 10, 2010). http://www.guardian.co.uk/world/2010/jan/03/ gordon-brown-airport-body-scanners (accessed March 2, 2010).

Williamson, Elizabeth. "Obama Connects al Qaeda to Jet Plot." *Wall Street Journal*, (January 2, 2010). http://online.wsj.com/article/SB126242308343313439.html (accessed January 30, 2010).

U.S. Government Documents:

Alaska Division of Homeland Security and Emergency Management. *Situation Report 09-358*, December 24, 2009. http://fc.ak-prepared.com/dailysitrep/I011FBFA4.0/DHS&EM%20Daily (accessed March 15, 2010).

Brennan, John, O. Memorandum to Cabinet Principals. *"Strengthening Information Sharing and Access."* Washington, D.C.: Office of the Assistant to the President for Homeland Security and Counterterrorism, July 2, 2009. http://www.fas.org/sgp/obama/brennan 070209.pdf (accessed December 12, 2009).

Congressional Research Service (CRS) Report for Congress. *Homeland Security: Roles and Missions for United States Northern Command.* Order Code RL34342. Washington, D.C.: January 28, 2008. http://www.fas.org/sgp/crs/ homesec/ RL34342. pdf (accessed September 9, 2009).

_____.*The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns.* Order Code R41022. Washington, D.C.: January 15, 2010. http://www.fas.org/sgp/crs /intel/ R41022.pdf (accessed January 26, 2010).

Information Sharing Environment (ISE). *Enterprise Architecture Framework version 2.0.* Washington, D.C.: PM-ISE, September 2008. http://www.ise.gov/docs/eaf/ISE-EAF_v2.0_20081021.pdf (accessed September 15, 2009).

_____. *Progress and Plans, Annual Report to Congress.* Washington, D.C.: PM-ISE, June 30, 2009. http://www.ise.gov/docs/reports/ISE_2009-Annual-Report_FINAL_2009-06-30.pdf (accessed November 30, 2009).

Intelligence Reform and Terrorism Prevention Act of 2004. Public Law 108-458. 118 Stat. 3638, 108th Cong. December 17, 2004. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi? dbname=108_cong_public_laws&docid=f:publ458.108.pdf (accessed November 29, 2009).

McConnell, J., M. Intelligence Community Policy Memorandum Number 2007-500-1. *"Subject: Unevaluated Domestic Threat Tearline Reports."* Office of the Director of National Intelligence (ODNI), (Washington, D.C.: November 19, 2007). http://www.dni.gov/electronic_reading_room/ICPM%202007-500-1,%20Unevaluated%20Domestic%20Threat%20Tearline%20Reports.pdf (accessed December 2, 2009).

The 9/11 Commission Report. *Final Report of the Commission on Terrorist Attacks Upon the United States*. Washington, D.C.: U.S. Government Printing Office, 2004. http://www.9-11commission.gov/ report/911Report.pdf (accessed August 29, 2009).

Office of the Director of National Intelligence (ODNI). Interagency Threat Assessment and Coordination Group (ITACG). *"Intelligence Guide for First Responders."* (2009). http://www.ise.gov/ docs /ITACG_Guide.pdf. (accessed November 29, 2009).

U.S. Congress. Senate. Committee on Homeland Security and Governmental Affairs. "Testimony by Mr. Timothy J. Healy, Director, FBI Terrorist Screening Center." *Federal Bureau of Investigation.* Washington, DC: March 10, 2010. http://www.fbi.gov/congress /congress 10/healy031010.htm (accessed March 13, 2010).

_____. Committee on Homeland Security and Governmental Affairs. "Statement by Juan Carlos Zarate. The Fort Hood Attack: A Preliminary Assessment." *Center for Strategic and International Studies (CSIS)*, November 19, 2009. http://hsgac.senate.gov/ public/ ndex.cfm?FuseAction=Hearings. Hearing& Hearing_ID=70b4e9b6-d2af-4290-b9fd-7a466a0a86b6 (accessed December 12, 2009).

U.S. Customs and Border Protection. *National Targeting Center Keeps Terrorism at Bay.* Washington, D.C.: March 2005. http://www.cbp.gov/xp/CustomsToday/2005 /March/ntc.xml (accessed March 2, 2010).

U.S. Department of Defense. Independent Review Related to Fort Hood. *Protecting the Force: Lessons Learned from Fort Hood.* Washington, D.C.: January 13, 2010. http://www.defense.gov/pubs/pdfs/DOD-ProtectingTheForce-Web_ Security_HR_ 13Jan10.pdf (accessed January 15, 2010).

_____. *Information Sharing Implementation Plan.* Washington, D.C.: Office of the Assistant Secretary of Defense for Network and Information Integration, April 2009. http://cio-nii.defense.gov/docs/DoD%20ISIP%20-%20APR%202009 _approved.pdf (accessed November 30, 2009).

U.S. Department of Homeland Security. Office of the Inspector General. *DHS' Efforts to Develop the Homeland Secure Data Network.* OIG-05-19, Washington, D.C.: April 2005. http://www.dhs.gov/xoig/asserts/mgmtrpts/OIG_05-19_Apr05.pdf (accessed September 15, 2009).

_____. Office of the Inspector General. *Homeland Security Information Network Could Support Information Sharing More Effectively*. OIG-06-38, Washington, D.C.: June 2006. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_06-38_Jun06.pdf (accessed January 15, 2010).

_____. *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*. Washington, D.C.: January 2009. http://www.dhs.gov /xlibrary/ assests/NIPP_Plan.pdf (accessed September 15, 2009).

_____. *Quadrennial Homeland Security Review (QHSR) Report: A Strategic Framework for a Secure Homeland.* Washington, D.C.: February 2010. http://www.dhs.gov /xlibrary/assets/qhsr_report.pdf (accessed March 11, 2010).

U.S. Department of Justice. *Baseline Capabilities for State and Major Urban Area Fusion Centers, a Supplement to Fusion Center Guidelines.* Washington, D.C.: September 2008. http://it.ojp.gov/documents/baselinecapabilitiesa.pdf (accessed December 2, 2009).

_____.Fusion Center Guidelines. *Developing and Sharing Information in a New Era.* Washington, D.C.: July 2006. http://www.it. ojp.gov/documents/fusion_center _guidelines.pdf (accessed November 12, 2009).

_____. *Robert S. Mueller, III: Congressional Testimony before the Senate Committee on the Judiciary*. Washington, D.C.: Press Room, Federal Bureau of Investigation, January 20, 2010. http://www.fbi.gov/cpngress/congress10/mueller 012010.htm (accessed March 6, 2010).

U.S. District Court, Eastern District of Michigan, Criminal Complaint Affidavit. "U.S. v. Umar Farouk Abdulmutallab." *New York Times*, (December 26, 2009). http://graphics8. ytimes.com/packages/pdf/national /20091226Complaint Affidavit.pdf (accessed March 6, 2010).

U.S. Government Accountability Office (GAO). *Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to be Better Coordinated with Key State and Local Information-Sharing Initiatives.* GAO-07-455 (Washington, D.C.: GAO, April 2007). http://www.gao.gov/highlights /d07455high.pdf (accessed August 29, 2009).

U.S. House of Representatives. Hearing before the Subcommittee on Intelligence Information Sharing, and Terrorism Risk Assessment. Committee on Homeland Security. *A Report Card on Homeland Security Information Sharing.* H. Rpt. 110-141, September 24, 2008. http://homeland.house.gov/hearings/index.asp?ID=169 (accessed January 11, 2010).

U.S. President. Executive Order 13228 (EO 13228)."Establishing the Office of Homeland Security and Homeland Security Council." *Federation of American Scientists* (October 8, 2001). http://www.fas.org/irp/offdocs /eo/eo-13228.htm (accessed 11 January 2010).

_____.Homeland Security Presidential Directive-6 (HSPD-6). "Directive on Integration and Use of Screening Information to Protect Against Terrorism." *U.S. Government Printing Office*, (September 16, 2003). http://www.gpo.gov /fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf (accessed January 16, 2010).

_____. Address. “Remarks Following a Meeting on Improving Homeland Security.” *U.S. Government Printing Office*, (January 5, 2010). http://www.gpoaccess.gov/presdocs/2010/DCPD-201000005.pdf (accessed January 10, 2010).

The White House. *Briefing by Homeland Security Secretary Napolitano, Assistant to the President for Counterterrorism and Homeland Security Brennan, and Press Secretary Gibbs, 1/7/10.* Prepared by the Office of the Press Secretary. Washington, D.C.: January 7, 2010. http://www.whitehouse.gov/the-press-office/briefing-homeland-security-secretary-napolitano-assistant-president-counterterroris (accessed January 25, 2010).

_____. *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing.* Washington, D.C.: October 31, 2007.

_____. *Memorandum for the Heads of Executive Departments and Agencies, Subject: Attempted Terrorist Attack on December 25, 2009: Intelligence, Screening and Watchlisting System Corrective Actions.* Washington, D.C.: January 7, 2010. http://www.whitehouse.gov/sites/default/files/potus_directive_corrective_actions_1-7-10.pdf (accessed January 7, 2010).

_____. *Summary of the White House Review of the December 25, 2009 Attempted Terrorist Attack.* Washington, D.C.: January 8, 2010. http://www.whitehouse.gov/ sites/default/files/summary_of_wh_review_12-25-09.pdf (accessed January 8, 2010).

Internet Sources:

Baird, Zoe and Michael A. Vatis. “Creating a Trusted Network for Homeland Security, Second Report of the Markle Foundation Task Force.” *The Markle Foundation Task Force on National Security in the Information Age*, (December 3, 2003). http://www.markle.org/ downloadable_assets/nstf_report2_full_report.pdf (accessed August 29, 2009).

Baird, Zoe, and Jim Barksdale. “Nation at Risk: Policy Makers Need Better Information to Protect the Country.” *The Markle Foundation Task Force on National Security in the Information Age*, (March 10, 2009). http://www.markle.org/downloadable_assets/20090304_mtf_report.pdf (accessed January 14, 2010).

Bean, Hamilton. “Exploring the Relationship between Homeland Security Information Sharing & Local Emergency Preparedness.” *Homeland Security Affairs*, Volume V, No. 2 (May 2009). http://www.hsaj.org/pages/volume5/issue2/pdfs/5.2.5.pdf (accessed December 12, 2009).

Collins, Susan. Senator (R-ME). "Transcript: GOP Weekly Radio Address." RNC Blog, entry posted January 30, 2010. http://rncnyc2004.blogspot.com/2010/01/senator-susan-collins-weekly-republican.html (accessed January 30, 2010).

Dempsey, Jim. "CDT Analysis of Privacy Guidelines for the Information Sharing Environment for Terrorism Information." *Center for Democracy and Technology (CDT)*, (February 2, 2007). http://www.cdt.org/security/20070205 iseanalysis.pdf (accessed March 3, 2010).

Edgar, Timothy, H. "How "Patriot Act 2" Would Further Erode the Basic Checks on Government Power That Keep America Safe and Free." *American Civil Liberties Union (ACLU)*, (March 20, 2003). http://www.cdt.org/ security/patriot2/030320aclu.pdf (accessed March 25, 2010).

International Criminal Police Organization (INTERPOL). *Terrorism Fact Sheet: Fusion Task Force.* COM/FS/2010-02/PST-01, February 2010. http://www.interpol.int /Public/ICPO/FactSheets/PST01.pdf (accessed March 30, 2010).

_____. *MIND/FIND: Integrated Solutions to Access INTERPOL's Databases—an Overview*. 2006. http://www.interpol.int/ Public/FindAndMind/ FINDandMind.pdf (accessed March 30, 2010).

Laipson, Ellen, Julie Fischer, Peter Roman, and Jesper Gronvall. "New Information and Intelligence Needs in the 21st Century Threat Environment." *The Henry L. Stimpson Center*, Report No. 70 (September 5, 2008). http://www.stimson.org /domprep/pdf/SEMA-DHS_FINAL.pdf (accessed November 28, 2009).

Wagner, Lisa, Walbolt. Justice Research and Statistics Association. *Information Sharing Systems: a Survey of Law Enforcement.* Washington, D.C.: July 31, 2006. http://www.jrsa.org/pubs/reports/improving-crime-data/Info_Sharing.pdf (accessed February 4, 2010).

White Paper. "GIS Supporting the Homeland Security Mission." *Environmental Systems Research Institute (ESRI)*, (Redlands, CA: May 2007). http://www.esri.com /library/whitepapers/pdfs/gis-supporting-hls.pdf (accessed March 15, 2010).

Television and Broadcast Source:

"The Underwear Bomber: Detroit Plane Plot," *The Discovery Channel*, (originally aired on March 11, 2010).

U.S. Joint Staff and U.S. Army Doctrinal Sources:

Joint Publication 3-27 (JP 3-27). *Homeland Defense.* Washington, D.C.: Chairman of the Joint Chiefs of Staff, 12 July 2007.

U.S. Army Field Manual 3-0. *Operations*. Washington, D.C.: 27 February 2008.

U.S. Army Field Manual 5-0. *The Operations Process.* (Final Approved Draft). Washington, D.C.: 25 February 2010.

U.S. Army Field Manual-Interim (FMI) 5-2, *Design (Draft).* Washington, D.C.: Headquarters, Department of the Army, 20 February 2009.

U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-5-500. *Commander's Appreciation and Campaign Design* (CACD). Fort Monroe, VA: 28 January 2008.