NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

APPLYING NETWORK THEORY TO DEVELOP A DEDICATED NATIONAL INTELLIGENCE NETWORK

by

James A. Tindall

September 2006

Thesis Advisor:	Robert Simeral
Thesis Co-Advisor:	Richard Bergin

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY	**2. REPORT DATE** September 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Applying Network Theory to Develop a Dedicated National Intelligence Network			**5. FUNDING NUMBERS**
6. AUTHOR(S) James A. Tindall			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Adaptive terrorist organizational structure and the lack of intelligence sharing were to blame for terrorist attacks on September 11, 2001. Because terrorist groups are moving toward a less predictable, but more diverse, dynamic, and fluid structure, effective combativeness of terrorism requires fighting terrorists with a network. This network must be capable of collecting and sharing credible, reliable and corroborative information on an unprecedented scale, transcending geographic, agency, and political boundaries.

This thesis demonstrates utilization of a network-theory approach for sharing information, which will be argued, can provide insight into the system dynamics of the U.S. IC because it allows a systematic, comparative analysis of the system representation and fundamental problems associated with information sharing. The problems associated with past intelligence failures can be overcome with such a system because the use of a dedicated, nationally networked system will allow completion of three primary tasks: (1) examination of the strength of criminal/terrorist connections, (2) identification of suspects and mapping of networks, and (3) prediction of future behavior and better likelihood of prevention, response, and prosecution. A dedicated national networked intelligence-sharing system called DNIN (Dedicated National Intelligence Network), including geographic areas, regional centers, personnel, computer IT networks, and policy options is discussed.

14. SUBJECT TERMS Network theory, intelligence, knowledge management, intelligence sharing, radicalization, data warehousing, transactive memory systems, terrorist networks, economy of scale, organizational structure, comparative analysis, network centric	**15. NUMBER OF PAGES** 186
	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	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

APPLYING NETWORK THEORY TO DEVELOP A DEDICATED NATIONAL INTELLIGENCE NETWORK

James A. Tindall
Scientist, U.S. DOI – Geological Survey, National Research Program
B.S., Brigham Young University, 1979
M.S., Brigham Young University, 1982
Ph.D., University of Georgia, 1990

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

NAVAL POSTGRADUATE SCHOOL
September 2006

Author: James A. Tindall

Approved by: Robert Simeral
Thesis Advisor

Richard Bergin
Co-Advisor

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Terrorist networks have evolved from locally-oriented political organizations into complex, adaptive, loosely structured groups that span international borders to promote larger regional and global goals through violent asymmetric attacks dependant on compartmentalization and deception. This adaptive terrorist organizational structure and the lack of U.S. IC and LE intelligence sharing were to blame for the terrorist attacks on September 11, 2001. Because terrorist groups are moving toward a less predictable, but more diverse, dynamic, and fluid structure, effective combativeness of terrorism will require fighting terrorist networks with a network capable of collecting and sharing credible, reliable and corroborative information on an unprecedented scale, transcending geographic, agency, and political boundaries.

This thesis demonstrates how the utilization of a network-theory approach for sharing information will allow the U.S. intelligence community (IC) and law enforcement (LE) to work and act in concert by building better relationships through organizational innovations, interagency networking, eliminating compartmentalization, and implementation of correct policy options. The utilization of network theory, it will be argued, can provide insight into the system dynamics of the U.S. IC because it will allow a systematic, comparative analysis of the system representation and fundamental problems associated with information sharing. A regional to national networked intelligence-sharing structure termed the Dedicated National Intelligence Network (DNIN) is discussed. This includes geographic areas, regional centers, personnel, computer IT networks, and policy options, as well as intelligence sharing from a network-centric approach. The discussion also includes a dedicated, national-scale intelligence-collection system, the necessary computer system architecture, intelligence analysis in a network perspective, the psychology of sharing, and the strategy for implementing DNIN. The problems associated with past intelligence failures can be overcome with such a system because it will allow completion of three primary tasks: (1) examination of the strength of criminal/terrorist connections, (2) identification of

suspects and mapping of networks, and (3) prediction of future behavior and better likelihood of prevention, response, and prosecution.

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis would not have been possible without the support of a great many people. A debt of gratitude is owed to the professional staff of the Center for Homeland Defense and Security at the Naval Postgraduate School for their unending support of program participants and for this thesis. I would like to express my thanks to the following people who helped make this thesis a reality:

- My family, especially Felisha Scott and my friends for thoughtful support during the many hours of research and writing;
- Captain Robert Simeral for his wealth of knowledge on intelligence issues, his accessibility and willingness to tirelessly encourage an all-encompassing approach to intelligence sharing, the relationships among the intelligence community, and his great sense of humor;
- Dr. Richard Bergin for his expertise and knowledge in computer systems, dynamics, databases, and software, his ability to provide critical comments on networking models and interrelations with other systems technology, and for being there during the long haul;
- Dr. Lauren Wollman for her encouragement, tireless support, and dedication through the research and thesis process;
- Heather Issvoran, Tom Mastre, Kristin Darken, Mark Fischer, Greta Marlatt, and Debby Miller, the rocks of the CHDS professional staff, who made it fun and who were always there for support and assistance;
- My friends and colleagues of Cohorts 0501 and 0502, especially Captain Dan Castro of the Philadelphia Police Department, for the great experiences we all shared that made this journey of learning so worthwhile;
- Dr. Andrew A. Campbell whose life-long work in counter intelligence, counter espionage, and counter-terrorism is of great value within the intelligence community and who has been a true mentor in international

intelligence and the issues involved that affect both the national security of the United States, as well as international security and stability of countries around the world;

- Drs. Phillip Zimbardo and Jim Breckenridge for their insights into psychology;
- Major Clay Boyd (USMC Ret.) who has always been an inspiration and a father figure on my journey through life;
- The Naval Postgraduate School for providing me the opportunity to contribute to national intelligence efforts and to perform research at an institution of such great tradition and stature.

EXECUTIVE SUMMARY

This thesis discusses a networked-based approach to intelligence sharing that is national in scope. This networked approach has been named DNIN (Dedicated National Intelligence Network). Though intelligence communities and law enforcement agencies utilize a hierarchal organization, the networked process described herein outlines an approach for intelligence collectors, analysts, and consumers to operate cohesively against increasingly complex enemies. Providing more intelligence to customers is simply not the answer, but having the capacity to analyze more intelligence, to scrub it as it goes up the chain, and share it with those who need it most is imperative and is the subject of this thesis.

The Department of Homeland Security began work in 2004 on a Joint Regional Information Exchange System (JRIES) to exchange information with other participants. Although JRIES does increase connectivity and provides more efficient responses to deter, detect, prevent, or respond to terrorist attacks, it has the shortcoming that it operates at the Sensitive-but-Unclassified level for most of the participants excepting state offices where it operates at a Secret level. Other programs such as RISS, LEO, and state fusion centers address primarily criminal related activities, but also have limited sharing abilities due to database incompatibility, IT platform issues, and other problems. However, through the process of what is now termed "radicalization" in which individuals move from having fundamentalist views to becoming a terrorist threat, as well as other issues, all three of these programs would be necessary to effectively deal with intelligence that affects homeland security on a national scale. The DNIN was designed for this specific purpose, to provide the priority capabilities necessary on a national scope and to work at any level of secrecy from a need-to-share basis, as well as provide the communications, collaboration/analysis, and information desired. The DNIN will also achieve the objectives desired by DHS that include focusing more power on combating terrorism by capitalizing on the collection capabilities of 800,000 law enforcement personnel who will collect most of the data. This will leverage federal, state, local, rural, and tribal anti-terrorism assets, and perform secure, real-time

collaboration and information sharing at not only local, state and regional levels, but on a national level and with the 16 member agencies of the intelligence community. DNIN can maximize analysis and intelligence sharing capabilities across all intelligence components, whether working with border surveillance and reconnaissance intelligence and capabilities, terrorist intelligence, radicalization, or criminal activity. A major problem within the intelligence network that DNIN will also overcome is information overload.

Information overload encourages intelligence failures; the DNIN networked process is designed to overcome this problem. A network approach will allow pattern recognition at a heightened level. Although it will not change the need for qualified and experienced analysts and other intelligence and LE personnel, it will assist them in detecting the "needle in the stack," i.e., let us move the stack and find the needle and not look through all the hay. Past intelligence failures have been the result of interagency non-cooperation, differing agency focus, and other factors. Application of a networked approach can help solve these problems by organizational innovations, interagency networking, eliminating compartmentalization, and implementation of correct policy options. The process of getting to the answer, i.e., actionable intelligence, especially on complex intelligence problems against a networked adversary, is fundamentally a social one. A network-centric approach such as that discussed herein will address these problems by emphasizing the sharing of information and expertise among stakeholders. If there is one key to a successful team outcome it would be efficient collaboration built on mutual trust, which can best be accomplished in a networked, multidisciplinary approach to intelligence sharing. Mutual trust is described well by transactive memory theory (detailed in Chapter VII). A networked, multidisciplinary approach will change agency cultures that keep the sum of the parts separated, causing animosity and lack of cooperation as well as adapting a need-to-share rather than a need-to-know policy. Factually, the application of network theory to agency wide structure and to intelligence collection and sharing will reduce much of the impedance in the sharing process. This will be accomplished through flattening of organizations, developing and using social network maps to determine key knowledge connectors and information transfer

bottlenecks (the latter is similar to transactive memory systems), developing better filters for information and better ways of organizing, indexing, sorting, and archiving it for later retrieval to differentiate between useful and useless information, and expanding risk and knowledge management and transfer processes (these issues are more thoroughly discussed in Chapters V, VI, and VII).

Although the popular focus is on collection and the DNIN described focuses on collecting a wealth of information, it also focuses on analysis. Most of the major failures in intelligence are due to inadequate or nonexistent analysis, and most of the rest are due to a failure to act on that analysis, which is political rather than collection or analysis oriented. Intelligence is about reducing uncertainty by obtaining information that the opponent in a conflict wishes to deny you; a network-centric capacity for obtaining that information can overcome this. Uncertainty is reduced because, in a real sense, the DNIN system arms the analyst with an arsenal of databases, resources, checklists, and variables that can be used to validate inferences, probabilities, and hypotheses. Once data are consolidated, a number of analytical techniques can be performed against the data to develop a model. At the initial stage an analyst seeks to identify potential targets, relationships, associates, time lines, and other information. Each piece of information is carefully analyzed. To avoid incorrect assumptions at this phase, the results should be reevaluated against the "big picture" in order to validate them, which is particularly necessary since terrorist groups are known to have sleeper cells. After comparing against the "big picture," spatial and temporal analysis and other quantitative techniques can be applied to further refine the product. During analysis one the focus is not solely on one-on-one relationships so that other associations are not missed. Consequently, analysts cannot rely upon only one method to verify information, which is why a network-centric approach will deliver intelligence that is credible, reliable, and corroborative (see Chapter V). While most methods of intelligence and non-intelligence research are identical, there is one important distinction. When accurate information is not available through traditional and less expensive means, a wide range of specialized techniques and methods unique to the intelligence field can be called into play. DNIN is yet another tool to use with existing techniques that can be applied to this problem.

The goal of DNIN is to achieve a network-centric approach to intelligence analysis and sharing and to construct a shared picture of the target(s) from which all participants can extract the elements they need to perform their job. This is not a linear process, it is a highly complex networked process, a social process in which all participants are focused on the objective — to accurately analyze and effectively share intelligence information. This collaborative and networked team approach has the potential for addressing two significant problems that intelligence analysts, law enforcement, and the intelligence community faces today:

- *Information Overload* — An overwhelming amount of information is available. The DNIN approach will expand the analyst team to include knowledgeable personnel from the collector, processor, and customer groups that can each take a portion of information glut to filter irrelevant material and, thus, constrain information to smaller and smaller amounts (the information is scrubbed) as it moves from local, regional, and up to the national level (an example of this is transactive memory systems/theory described in Chapter VII).
- *Customer Demand for Enhanced Detail* — Customers are demanding more detail about the target(s) since they have become more complex and our capabilities to deal with them have also become more robust. A networked approach that delivers intelligence of all kinds, from mapping and imaging, OSINT, building floor plans, information from databases that may contain persons of interest, critical infrastructure, GIS, and other types, can give that necessary detail since the indexing, sorting, and organizing of data will be complimentary and will allow "drill-down" capabilities within the network and, from any level.

All significant intelligence targets are complex systems in that they are nonlinear, dynamic, and evolving. To counter opposing networks, Al Qaeda as an example, the intelligence network must be highly collaborative, but large intelligence organizations such as those in the U.S. intelligence community (U.S. IC) provide disincentives to

collaboration. These include, but are not limited to, individual fear of lack of opportunities to climb the promotion ladder, loss of job, and disapproval of one's superiors, which serve as strong psychological fear barriers to go against the grain and to share information. Additionally, competition between employees for both pay and promotion for a fixed number of career-level slots creates an atmosphere of non-sharing as does competition and intelligence returns between agencies for justification of budgeted funds. The management of knowledge should be the primary focus. To do this efficiently will require placing one agency or group such as Department of Homeland Security Intelligence and Analysis (DHS IA) into a central role of being the hub for both domestic and foreign intelligence in regard to Homeland Security. The Department of Homeland Security Information Analysis and Infrastructure Protection (DHS IAIP) Directorate was established after 9/11 to enhance domestic intelligence collection and sharing and other duties. The Homeland Security Act of 2002 established IAIP (which has since been split into IA and IP), by Congressional Mandate to provide this integration and to merge into one organization the capability to identify and assess future terrorist threats and to make recommendations as necessary. Because the IAIP has the Congressional Mandate to fulfill this role, this thesis utilizes the DHS IA as the assumed "Central Hub" for the DNIN. The creation of DNIN will allow DHS to accomplish the six intelligence goals advocated by the IAs Chief Intelligence Officer Charles Allen, which are: (1) Requirements, Collection, and Dissemination; (2) Analysis and Warning; (3) Information Sharing & Knowledge Management; (4) Mitigation, Prevention, and Readiness; (5) Mission Advocacy; and (6) Culture and Business Process.

Because of the complexity of the intelligence needs of DHS IA, the IC, law-enforcement groups, and other agencies, this thesis discusses intelligence sharing from a network-centric approach — the development of regional to national-scale intelligence collection centers, the necessary computer system architecture, intelligence analysis in a network perspective, the psychology of sharing, and the strategy for implementing DNIN. Problems with information technology (IT) such as those with the FBI "Carnivore" system can be overcome because the technology is now available to make such a system a success. The incorporation of current fusion centers is briefly discussed; it will require

cooperation, and could be a complex undertaking in regards to budget, coordination, standards, training, and restoration of the network from old to new, but it can be accomplished. The computer IT architecture of the DNIN will overcome the failure of the former system, and has been designed, but is beyond the scope of this thesis (contact the author for additional information).

This thesis also discusses the six keys of analysis of information within a networked context (see Chapter V) and the relational databases and multi-dimensionality this entails. Incorporation of the six keys, combined with immediate analyst access to the databases gives the analyst a very powerful tool, especially on a preventive basis due to timely analysis of information. Associated with this process are workload sharing, expediting analysis, pooled intelligence, and shaping forces of networks. The DNIN approach will tend toward agility by focusing on organizational analysis through examining size and capabilities, assessing effectiveness and structure, and analyzing the relationships among groups in the organizational structure. Further, to effectively achieve intelligence sharing we need to ensure a national/international strategic approach in addition to improving the present poor cooperation between the intelligence community and law enforcement groups (see Chapters VI and VII). This will require development of a mutual operations doctrine analogous to that of the military, appointment of a single intelligence authority to own DNIN, development of good personnel policies, civil liberties, and other issues.

The strategy for implementing DNIN is addressed in regard to its problems and advantages and its strengths and weaknesses. It is estimated that utilization of the DNIN approach will allow collection of data a hundred fold greater than that now collected by the IC. DNIN will improve the quality of intelligence analysis, promote integration of intelligence from all sources and particularly DHS, provide the necessary national architecture for a dedicated intelligence network, ensure that homeland security and intelligence is melded with the IC, and hopefully solidify DHS relations with not only other IC members, but congress as well. Finally, the operational network principles of DNIN will allow for proper analysis and dissemination of this information, which could

make significant progress in intelligence and information sharing within the U.S. and reduce the risk of future terrorist attacks as well as threats from domestic groups and organized crime.

THIS PAGE INTENTIONALLY LEFT BLANK

I. NETWORKING AND INTELLIGENCE

Since the terrorist attacks against the World Trade Center on September 11, 2001 (9/11), intelligence sharing between the intelligence community (IC) and law enforcement (LE) has clearly become a critical issue. Director of National Intelligence John D. Negroponte defended his first year on the job by citing institutional innovations that have been achieved, but many disagree.[1] Advancing technology utilizes capabilities that have continually gained distance from the target from which the data is being collected. This technological shift, which occurred decades ago, has created serious intelligence collection problems with the agile adversary the U.S. is now facing — an adversary who has no mobile armies or fixed infrastructure from which war is waged. The new war and threat are asymmetric in nature and thus are forcing change on the way we deal with intelligence collection. A large component of intelligence collection since 9/11 has become sharing among the intelligence community (IC) and law enforcement (LE) in an effort to thwart the new adversary. A congressional critic noted: "The CIA continues to excessively compartment sensitive reporting and fails to share important information about reporting and sources with IC analysts who have a need to know."[2] The lack of sharing intelligence product, rather than the complex task of collection, has plagued counter-terrorist efforts against Al Qaeda and other transnational and domestic terrorist groups. This problem within the continental United States (CONUS) has become greatly exaggerated since most of the intelligence is gathered by LE and the U.S. does not have a domestic intelligence (DI) agency. This is especially true in regard to Homeland Security in which sharing collected intelligence between the CIA, FBI, and LE agencies (LEAs) is problematic. Several factors have contributed to the failure to share product: (1) a reduction of funding for intelligence in general; (2) the shift toward TECHINT; (3) an attitude of need-to-know versus need-to-share; (4) the problem of compartmentalization of human intelligence (HUMINT); (5) policies that have impeded information sharing; and (6) agency culture and other factors.

[1] Walter Pincus, "Negroponte Cites 'Innovations' In Integrating Intelligence," *WashingtonPost.com*, April 20, 2006; available from http://www.washingtonpost.com/wp-dyn/content/article/2006/04/20/AR2006042001785.html. [cited May 1, 2006].

[2] John LeBoutillier, "Congress Let Us Down Too," *NewsMax*, September 24, 2001; available from http://www.newsmax.com/archives/articles/2001/9/24/83522.shtml. [cited January 15, 2006].

Perhaps the most recent examples that exemplify this problem are those associated with the 9/11 attacks. From the beginning the FBI was the agency most singled out for intelligence failures that led to the attacks. Pre-9/11, the FBI had attempted reforms to strengthen its terrorist-intelligence abilities. Many believed the reforms failed because of the occurrence of 9/11; Louis Freeh, FBI director from 1993 to 2001, rejected these criticisms saying the FBI, despite resource constraints, did all it could to prevent terrorism, indicating terrorism was not a national issue at the time — the issue of terrorism was absent from the 2000 presidential campaign, despite Al Qaeda's attack on the USS Cole on October 12, 2000, in Port Aden, Yemen. Looking back on 9/11, various agencies had dropped the ball. Janet Reno said, "The FBI didn't know what it had. The right hand didn't know what the left hand was doing."[3]

A classic example of 9/11 intelligence failure is the CIA response. The U.S. IC was close to thwarting the Al Qaeda plot. They had tracked Khalid al-Midhar and Nawaf al-Hazmi to the Malaysia meeting in Kuala Lumpur and knew that one of the men had a visa that would allow U.S. entry. The intent was to follow these men after the meeting. However, the alert to agents in Bangkok arrived too late and the trail was lost. Directly after the attack on the USS Cole the FBI attempted to locate those responsible. One, apparently by the name of Khallad, jumped to the top of the list because it was believed that Khallad and Midhar may be the same person. The FBI began working with the CIA. The investigation revealed that Khallad and Midhar were not only different people, but they were a higher up Al Qaeda official and foot soldier, respectively. The most blatant criticism was that the two agencies did not meld separate pieces of intelligence. This lack of intelligence sharing became a critical issue; follow-through issues also became a problem. Investigating cables from the Malaysia meeting, the FBI decided something "bad" would happen, but while the FBI focused on Malaysia, the CIA's attention was on overseas events.[4] The FBI focus was to build a criminal case — the "who" — while the CIA used a more broadly focused intelligence purpose — the "where." The conundrum between culture and sharing is therefore manifest. If the CTC/CIA and FBI had been working with a sharing information model, the outcomes would have been undoubtedly

[3] *The 9/11 Commission Report* (New York: W.W. Norton & Company, 2004).

[4] Ibid.

different. The big question is how can we increase intelligence sharing and distribute that intelligence to those who need it most? The Global War on Terror (GWOT) is against transnational terrorist networks. This thesis therefore examines the need for devising counter-terrorism intelligence-sharing strategies within a network context that will allow for more efficient and rapid sharing.

A. TWO CASE STUDIES

Two case studies will be addressed in this thesis to illustrate (1) lack of information sharing and (2) the strengths and principles of networking. Each will be briefly described (a more complete accounting and how things may have been different using a networked intelligence-sharing approach is given in Chapter II).

The first case study is Al Qaeda — for two and a half weeks before the 9/11 attacks, the U.S. government knew the names of two hijackers (Khalid al-Midhar and Nawaf al-Hazmi), that they were Al Qaeda, and that they were already in the United States. More importantly, acting on legal counsel, senior FBI officials refused to involve its criminal investigators alongside intelligence agents to track down and arrest these terrorists because of possible legal issues. The following partial email message is one of many that were exchanged between FBI agents regarding this issue. In a reply message, a New York agent protested the ban against using law enforcement resources for intelligence investigations in what became prophesy, "Some day someone will die — and wall or not — the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.' Let's hope the lawyers who gave the advice will stand behind their decisions then, especially since the biggest threat to us now, UBL (Usama Bin Laden), is getting the most 'protection.'"[5]

The second case study is the "Malaysia Meeting" in Kuala Lumpur that occurred January 2000. The key intelligence questions were not asked: What was the significance of the Malaysia meeting? Who attended? Where are they now? Why are they here? Who are they meeting? The Malaysia meeting included the two leading Al Qaeda 9/11 cell members (mentioned in the first case study) who infiltrated into the U.S. These two

[5]Stewart Baker, "Wall Nuts: The Wall between Intelligence and Law Enforcement Is Killing Us," *Slate.com*, 2003. [cited May 1, 2006].

individuals were listed in the white pages under their true names.[6] If the full significance of the Malaysia meeting had been recognized and shared it is possible that 9/11 may have been disrupted. The local service that conducted the surveillance restricted itself to video and not audio surveillance. Total coverage would have been necessary to assess the full significance of the meeting. The four-day meeting of the terrorists and CIA's failure to ensure the meeting was the target of total surveillance represent arguably the most egregious intelligence failure of this decade, illustrating the consequences of the lack of sharing intelligence. Further, asking the correct questions would have led to a network structure of the terrorists that possibly could have prevented their catastrophic actions.

How can the principles of network theory and applications be applied to intelligence-sharing policies and practices? How would this improve delivery of relevant, timely and accurate information among the IC and law enforcement?

U.S. intelligence agencies are bureaucratic, not unlike major corporations.[7] To survive in the new technology age, corporations have been forced to adopt a flattened management structure to remain competitive[8] while U.S. intelligence agencies have changed little. For example, beginning in the late 1990s, as a result of the economic downturn in the industry, aerospace companies found themselves embroiled in a crisis and responded creatively by using organizational changes and a multitude of strategies. With looming budget cuts and restrictions, these companies adapted their organizations to survival mode. "Three types of competitive organizational structures have emerged from the forces shaping the industry. Companies will compete as technology leaders, cost leaders or adaptable niche leaders. There is a necessity to downsize and the strongest technology and cost leaders are going to do it through innovation, acquisition and abandonment."[9] To achieve the greatest success in both gathering and sharing intelligence information, there is an urgent requirement to review current thinking and

---

[6] Gerard L. Posner, *Why America Slept: The Failure to Prevent 9/11* (New York: The Random House Publishing Group, 2003), 48.

[7] Bruce D. Berkowitz and Allan E. Goodman, *Best Truth: Intelligence in the Information Age* (New Haven, CT: Yale University Press, 2000), 137.

[8] Kenneth C. Loudon and Jane T. Loudon, *Essentials of Management Information Systems: Managing the Digital Firm*, Sixth ed. (Upper Saddle River: Pearson Prentice Hall, 2005).

[9] W.V. Dee, "Defense Contractors Must Change to Survive in the 1990s," *Aviation Week & Space Technology* 131, no. 3 (1997).

outdated hierarchal interests with consolidation and cooperation between IC agencies and a new approach toward intelligence sharing. This thesis will examine the problem from both a qualitative and quantitative perspective. An example of the qualitative component would be describing the most suitable method of sharing HUMINT or other intelligence collection information.

The quantitative perspective will be development of a network-based sharing model. The model can be only quantitatively described through incorporation of network theory. As an example, if private sector corporations have been forced into a flattened management structure utilizing network theories to compete because of new technologies and foster new cooperation among management to reduce resource cost and remain effective and competitive, what does this portend for the U.S. IC? This thesis makes the case for changing policies to intensify intelligence collection, sharing, and the network or organizational theories and methodology necessary to achieve it.

Competitive intelligence is information that is critical to the survival, growth, and development of companies. Intelligence relating to national security is even more critical, especially given the level of threat from Chem-Bio and WMD attack. Al Qaeda has been attempting to obtain WMDs since 1993. The U.S. IC learned of these attempts from a "walk-in" at a U.S. Embassy in a foreign country.

The Robb-Silberman Report found there was no evidence that Iraq had capabilities of WMDs.[10] Further, intelligence was very fragmented regarding WMDs that Iraq supposedly possessed as well as the capabilities to develop new WMDprograms.[11] The lack of HUMINT, subsequently admitted to by former CIA Director Tenet, meant that the CIA was vulnerable to fabricators exemplified in the notorious "Curveball" case.[12] Through the summer of 2001 the CIA repeatedly warned the White House of attacks because the CIA knew that an attack was imminent in 2001,

[10] Charles S. Robb and Laurence H. Silberman, "The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction" (Washington, D.C.: Commission on the Intelligence Capabilities of the United States, 2005), 50.

[11] Anthony Glees and Philip H.J. Davies, *Butler's Dilemma* (2004); available from http://www.socialaffairsunit.org.uk/digipub. [cited January 29, 2006].

[12] Ibid.

but had no tactical intelligence to counter the threat.[13] If this information had been fused with information collected by the FBI and other agencies and shared it is likely that 9/11 may not have occurred. One can conclude that the development of HUMINT and other intelligence-sharing programs could prevent costly intelligence failures in the future and thwart such attacks as 9/11.

The necessity of credible, reliable, and corroborative intelligence was succinctly stressed in the UK (United Kingdom) working paper, "The failure to find WMDs (weapons of mass destruction) in Iraq six months after Saddam was toppled was a failure of intelligence, not of Government."[14] Lack of HUMINT and other forms of intelligence has plagued collection operations against terrorist groups including Al Qaeda because the CIA did not have any penetrations into the Al Qaeda leadership. Admittedly, Al Qaeda is a hard target as it is based on kinship and primordial affiliations, and recruitment is carefully conducted although a number of U.S. citizens managed to join Al Qaeda and meet with bin Laden as did a number of U.S. journalists.[15a, b] Advances in technology necessitate a change in information sharing and organizational structure if the United States IC is to maintain its leadership and advantage edge and have the capability to defeat an asymmetric enemy that long ago accomplished these changes. Because current technology and continued enhancement of capabilities in this area are rapidly advancing so too must the methods used to share collected intelligence, or the technological advantage decreases. The U.S. Government must develop and institutionalize sharing methods to keep pace with our technological advantage as well as the terrorists' technological advantage. Application of network theory and principles into intelligence-sharing practices can accomplish this goal.

B. NETWORK THEORY APPROACH

The network-theory approach to counter-terrorism began in the late 1990s. John Arquilla and David Ronfeldt, widely recognized experts in terrorist networks, argue that

---

[13] Posner, *Why America Slept*.

[14] Ibid.

[15] Milt Bearden and James Risen, *The Main Enemy: The Inside Story of the CIA's Final Showdown with the KGB* (New York: Random House Publishing Group, 2003).

it will take "strong networks to fight networks" and further state that, "The strongest networks will be those in which the organizational design is sustained by a winning story and a well-defined doctrine, and in personal and social ties at the base. Each level, and the overall design, may benefit from redundancy and diversity. Each level's characteristics are likely to affect those of the other level."[16]

1. Defining a Network

In the context of this thesis, networks, whether social or technical, are defined as computer based and are stable sets of relationships (links) between two or more entities (nodes) that can be agencies, groups, or individuals. Network theory is based on the premise that networks grow and evolve. Links are not randomly added but attach to the nodes by the principle of preferential attachment. An excellent analogy is terrorist cells. Within the U.S. IC there are both a technical network and a social network, which follows the principles of network theory. A social network is a social structure between individuals and organizations; an analysis of that network is often termed network theory. Such networks operate on many levels and play a critical role in determining the way problems are solved, agencies are run, and the degree to which an individual(s) succeeds in achieving goals, and perhaps more importantly, how information is shared. The shape of a network will determine its usefulness. Perhaps the single most important mistake assumed about networks, especially terrorist networks, is that they are organized in a hierarchal manner. In his study of organized criminal activity, Klerks argues that we should not assume hierarchal organization just because most law-enforcement agencies and other groups are organized in this manner.[17]

Terrorist networks have evolved from locally oriented political organizations that engage in acts of terror into complex, adaptive systems of loosely structured organizations that work across national borders to promote larger regional and global ambitions primarily through violent and surprise attacks that depend on compartmentalization and deception.[18]

---

[16] John Arquilla and David F. Ronfeldt, *Advent of Netwar* (Washington, D.C.: RAND Corporation, 1996), 119.

[17] P. Klerks, "The Network Paradigm Applied to Criminal Organisations: Theoretical Nitpicking or a Relevant Doctrine for Investigators? Recent Developments in the Netherlands," *Connections* 24, no. 3 (2001).

In the 1970s and well into the 1980s, social scientists working from a social-network analysis perspective explored the informal functioning of social networks. They developed theories and new understanding about human behavior in complex societies. Research during this period showed that informal network organization offered particular kinds of advantages over more formalized, hierarchal, functionally organized groups.

Milgram coined the phrase, "the strength of weak ties."[19] Individuals (or organizations) with many diverse ties adapt to changing circumstances, are more resilient, and have a greater coping capacity than those with fewer but "stronger" ties; they are also more agile. An excellent example of this is the flexibility of local agencies and first responders who are proactive and respond more quickly than the U.S. Federal Government. For example, Al Qaeda terrorist cells and those from other terrorist organizations discovered the principle that business organizations (and social network theorists) have long known. Network-like structures of cooperating organizations can augment manpower, increase available information and expertise, improve access to critical resources, shorten critical paths to goals, and create useful redundancies to ensure mission success. While first responders and Al Qaeda are very agile due to the networked process, the IC due to bureaucracy is not agile and therefore poorly equipped to deal with a networked adversary. However, the necessary features to make an IC agency agile should become manifest when network theory is applied to intelligence sharing.

Social network theory assists in understanding Al Qaeda's success, which is partially due to its loosely knit networked organization. This model presupposes that the system of reciprocities, rewards, and advantages are clearly understood and accepted and that these outweigh costs and risks. Networks and network theory can be a very powerful organizational and operational tool. For example, Al Qaeda's relationship with the Taliban government in Afghanistan enabled it to take over and maintain MAK's camps. Al Qaeda also trained recruits in Sudan, Yemen, Chechnya, Tajikistan, Somalia, the

[18] Paul K. Davis and Brian Michael Jenkins, *Deterrence and Influence in Counterterrorism: A Component in the War on Al Qaeda* (Washington, D.C.: RAND Corporation, 2002).

[19] Stanley Milgram, "The Small World Problem," *Psychology Today* (1967).

Philippines, and Indonesia. Estimates of the number of graduates of these camps range from 25,000 to 50,000 non-Afghan nationals.[20]

The Al Qaeda network also developed cooperative relationships with Hezbollah, who lent bomb experts to assist in technical training of Al Qaeda members. The technical excellence of training provided by Al Qaeda has drawn top quality students to its camps who later return to their local Islamist organizations deeply indoctrinated with the Al Qaeda message of the importance of working against the West and also that further increased the strength, flexibility, and effectiveness of their network structure. The "Hamburg Cell" is a paradigm case.

Gunaratna, an expert on Al Qaeda's organization and history, notes that the Islamic Group of Egypt has "merged with Al Qaeda at strategic, operational and tactical levels and functions almost as one organization — Al Qaeda pursues its objectives through a ***network*** of cells, associate terrorist and guerilla groups, and other affiliated organizations and shares expertise, transfers resources, discusses strategy, and even conducts joint operations with some or all of them. While Al Qaeda cells mostly operate in the West, its associate groups are more numerous in the South or developing nations, while its affiliates operate in Muslim societies or countries within Islamic communities. Al Qaeda's cadres are better motivated, trained and disciplined than its own members and tend to be more mobile and have a wider reach, while Al Qaeda's associates operate on a local level. While associate groups tackle tactical targets, strategic targets are Al Qaeda's responsibility. According to the CIA, Al Qaeda can draw on a support base of six to seven million radical Muslims worldwide, of which 120,000 are willing to take up arms.[21]

Networks concern different types of relationships, whether objective and measurable as a resource, or subjective, like effective links. They can serve tactical, strategic, or other purposes. Utilizing a network theory approach to sharing information

[20] Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror* (New York: Columbia University Press, 2002).

[21] Ibid., 97.

will allow groups, agencies, and individuals to work and act in concert although they operate on a need-to-know basis and on the principle of compartmentalization and cell structure.

The utilization of network theory, it will be argued, could provide insight into the system dynamics of the U.S. IC and the intelligence network because it will allow a systematic, comparative analysis of the system representation and fundamental problems associated with information sharing for the GWOT. Networks occur in nature, such as neural networks, or they can be human artifact, such as power distribution grids. Using network theory, Tremayne discovered that news Web stories contain links to external sites less frequently today than just a few years ago. As each organization builds its own archive of Web content, the new content material appears to be favored over content that is offsite.[22] Each Web page has links to other pages (nodes). It has been discovered that a scale-free power-law distribution develops from the Web network.[23] Eventually there are many Web pages with few links and others with hundreds or thousands of links, the latter being called hubs. This process develops rather naturally due to freedom of access by almost all who share the information.

In contrast, within the U.S. IC each agency, group, local entity or individual would be a node. If network theory can be applied to the intelligence-sharing process, natural hubs would evolve within the IC that would share the intelligence needs of all. But, information in the IC is restricted by a "need-to-know" basis to prevent source identification and ensure collection methods are not compromised. Compartmentalization that can become ritualistic may be the enemy of sharing product. The concern therefore is not only to develop the method but to clarify policies and ensure that intelligence product is shared and distributed to the appropriate agency or individual from a need to share approach.

This will require both a social network and a technical network. The technology for the technical network already exists for achieving the technical component of the sharing problem. One example is the Semantic Web. The Semantic Web is a new

[22] Mark Tremayne, *Internet Newspapers: Making of a Mainstream Medium* (Austin: Lawrence Erlbaum Associates, 2004).

[23] Ibid., 3.

approach to using information online. The Semantic Web gives one the ability to find what they need, when they need it, and prevent too much information overload.[24]

The coordination of the complex elements within the U.S. — law enforcement, Homeland Security, intelligence collection processes and policy, economic and political, to name a few — is exceedingly difficult, but the challenge must be met to deal with the scope of the threat. Intelligence collection and sharing for Homeland and National Security requires a unified entity that links agencies; this will be greater than the sum of IC parts, which is the advantage of network principles. A network approach is best able to accomplish our goal of intelligence sharing. Unless intelligence is shared with local law enforcement, which can use local-area knowledge and ground truth for counter-terrorist operations, terrorists will continue to adhere to the motto, "*think locally; act globally*."

The GWOT requires new information and theory-centric techniques and more intelligent methods of warfare such as those utilized by network theory. The trend away from HUMINT to technical intelligence has further reduced and constrained the intelligence-sharing process between agencies due to lack of personal contact and mutual trust and informal social networks. This has contributed to the stovepipe problem. Excellent examples are the two cases briefly mentioned above; also, the literature is replete with copious information within the U.S. about how "the wall" still persists five years after 9/11.

As wedged, the process that advances in technology and coupling those advances with the power of network principles argue that the same technology can be utilized to remove the wedge and integrate the IC into a stronger sharing-based entity. It can and will be shown mathematically that, as the proposed network is constructed, the additions of agencies and links will make the network stronger, not weaker. Theoretically, for this to happen, R, the distance between nodes in terms of radius, will become shorter, which signifies a stronger relationship. Therefore, the same technologies that prevented the sharing of information prior to 9/11 can be utilized to enhance information sharing.

[24] Jennifer Golbeck, Aaron Mannes, and James Hendler, "Semantic Web Technologies for Terrorist Network Analysis," in *Emergent Technologies and Enabling Policies for Counter Terrorism* (Piscataway, NJ: IEEE Press, 2005).

Further, it has been proposed that a specific agency, the DHS IAIP (Information Analysis and Infrastructure Protection, now the IA) for example, needs to be named to promote information sharing and dissemination of domestic intelligence throughout all levels of government as well as budgetary oversight by DHS. This issue has been closely studied by the House Permanent Select Committee on Intelligence (HPSCI).[25] After four years, little has been done to rectify this problem. While this argument does not negate the need for HUMINT or other intelligence, it exemplifies the need for sharing that intelligence as we must first create the methodology before defining the sharing agency and its responsibilities; i.e., the cart must not come before the horse. Through the utilization and application of principles of network theory and social engineering we can more fully develop and enhance interagency intelligence-sharing practices. Such a proposal is not a matter of "connecting the dots;" we need to increase relationally and connectively to ensure that not just "dots" are "connected." Network theory, applied to either or both a technical or social network can give us the tools we need to effectively share intelligence between and among the IC, from local LE to the Pentagon. Law enforcement agencies and the Pentagon can also network with each other.

C. POLICY OPTIONS

Policies issues are (i) who needs to know; (ii) how much can be shared; and (iii) that at least for Homeland Security, one agency should serve as a central hub for dissemination of the intelligence collected from all sources. To address these concerns, the following policy issues will be discussed:

- Implementation of a mutual operations doctrine
- A single authority
- Development of a regional structure
- Leadership

The anticipated output of this thesis will be the development of a national scale model based on network theory that demonstrates the most effective way to share Homeland Security intelligence among the IC and LE from local to Federal levels. The

[25] Richard Best, "The Intelligence Community and 9/11: Congressional Hearing and the Status of the Investigation," ed. Congressional Research Service (Washington, D.C.: National Printing Office, 2002).

policy options portion of the thesis will investigate and make recommendations on the best policy approach that will ensure success of model implementation within the U.S. IC.

D. SUMMARY

Since 9/11, it has become clear that intelligence sharing problems exist between law enforcement and the intelligence community as well as within the IC. In part, these problems exist due to:

- Interagency non-cooperation.
- Differing agency focus — arrest versus surveillance.
- Inability to connect the dots.

These problems can be solved in part by:

- Organizational innovations (a modification of organizational structure).
- Utilization of interagency networking theory for sharing intelligence.
- Applying network theory to collection processes to reduce errors.
- Eliminating compartmentalization.
- Implementing correct policy options.

THIS PAGE INTENTIONALLY LEFT BLANK

II. INTELLIGENCE FAILURES

A. MALAYSIA MEETING — A CASE STUDY IN SHARING INFORMATION

The initial reaction among the press and government directly after 9/11 was to look for scapegoats to blame for the attacks. From the beginning the FBI was the agency most singled out for the intelligence failures that led to 9/11. Focusing on this one agency obscured the big picture. Another question that arose due to the 9/11 attacks was whether or not there was enough actionable intelligence. The White House specifically noted that all the briefings it received from the various agencies gave no "actionable" intelligence, i.e., where and/or when an attack would occur. Instead, there was only supposition by the IC. The argument pressed the White House into a corner, emerging with a new query, which was whether it would be up to the White House to pump the IC for information or for the IC, especially the FBI and CIA, to pump better data to the White House.[26] Thus, the ensuing Washington two-step of shifting and relegating blame slowed and obscured real solution(s) to the intelligence-sharing problem.

Another example of 9/11 failures is the response of the CIA. According to the 9/11 Commission reports, the U.S. IC was very close to thwarting the Al Qaeda plot. Looking back, connecting the dots was relatively easier than during the turmoil that led up to 9/11. The CIA had tracked Khalid al-Midhar and Nawaf al-Hazmi to the Malaysia meeting in Kuala Lumpur Malaysia and knew that one of the men had a visa that would allow U.S. entry. The intent was to follow these men after the meeting. One, by the name of Khallad, jumped to the top of the list because it was believed that Khallad and Midhar may be the same person. The FBI began working with the CIA. However, the investigation revealed that Khallad and Midhar were not only different people, but that they were a higher up Al Qaeda official and a foot soldier, respectively. The most blatant criticism was not that each agency did not do an outstanding job of using the same source to identify the men; the tragedy is that the agencies did not talk with each other and mesh their separate pieces of intelligence. Thus, lack of communication or rather intelligence

[26]Gail Russell Chaddock, "Was There Enough Intel to Act?" *Christian Science Monitor*, April 15, 2004; available from http://www.csmonitor.com/2004/0415/p01s03-uspo.html. [cited February 28, 2006].

sharing, became an issue. Follow-through issues also became a problem. Investigating cables from the Malaysia meeting, the FBI decided something bad would happen, but while the FBI focused on Malaysia, the CIA's attention was on overseas events.[27] This problem is an age-old one and illustrates why many do not believe the FBI should be in charge of domestic intelligence since their focus in this case was to build a criminal case against one person, while the CIA had a more broadly focused intelligence purpose. The FBI focus was on who, while the CIA focused on where. There should be some middle ground between these extremes for domestic intelligence (DI) to function properly. It would appear that perhaps the best focus for DI would be an all threat/all hazard approach on whom, where, and how. To accomplish this will require many fragments of information coming from a variety of sources being analyzed properly. In hindsight, the FBI and CIA opened a case, but they did not share information because of the well-known "wall" that exists between agencies in the IC and especially between the CIA and FBI. While each had a specific expertise, neither referred to the other or cooperated to leverage that expertise, which is common among poorly-communicating teams as described by mutual trust or more technically as transactive memory systems (see Chapter VII).

Can "the wall" be overcome? Can the intelligence divide that exists within the IC and LE be bridged? Do these questions relate to merely communication between agencies, or do they go deeper into the culture of those agencies? For example, the FBI appointed an Office of Law Enforcement Coordination, and then FBI director Mueller appointed Louis Quijas, former police chief of High Point, North Carolina as assistant director of the new department.[28] Mr. Quijas pointed out that there are 800,000 police officers in the U.S. representing 18,000 agencies and 27,000 FBI agents, only 11,400 of whom are in U.S. Despite this change, which was an attempt to foster cooperation, Baltimore Police Commissioner Edward Norris, even though he possesses a top-secret clearance, still was unable to obtain information about on-going investigations.[29] This lack of sharing, according to Norris, was eerily similar to a 1990 murder investigation

[27] Chaddock, "Was There Enough Intel to Act?"

[28] Faye Bowers, "How FBI Is Remaking Intelligence Functions," *Christian Science Monitor,* May 19, 2004; available from http://www.csmonitor.com/2004/0519/p02s02-usju.html. [cited February 28, 2006].

[29] Ibid.

where an Egyptian had been apprehended and several cab drivers interviewed because the suspect jumped into a cab to get away. Norris, after talking to several cab drivers, was convinced the suspect had gotten into the wrong cab or he would not have been caught. However, Norris was instructed to focus only on the murder, not the conspiracy — the FBI would do that. Three years later (1993), one of the cabbies Norris interviewed drove a van loaded with explosives into the World Trade Center.[30] Again, this illustrates lack of intelligence sharing, which would be prevented by such a network as the proposed DNIN. It is akin to putting a jigsaw puzzle together when different parties have pieces of the puzzle; either party is not likely to get the complete picture.

Culture is at the core of good intelligence sharing. For example, William Rosenau, a political scientist at the RAND Corporation and co-author of "Confronting the Enemy Within," a study of four domestic intelligence services, stated that the FBI sees itself as the crime-fighting elite, much like the Marine Corps sees itself as an elite military force.[31] While the FBI is brilliant at apprehending kidnappers, organized crime figures, and bank robbers, terrorism is a new tack and requires new thinking. The only way to acquire this new type skill is a rethinking of the culture. For those who have been exposed to the cultures of different large agencies and corporations, the predominant view that arises from the company/agency and personnel is that they do in fact view themselves as better/superior to everyone else. This is usually not true, however, and it denies those in other agencies who have great ideas from expressing them and therefore contributing to the problem at large — terrorism in this case. Culture keeps the sum of the parts separated and causes animosity and lack of cooperation, not only within an agency itself, but between other groups. This in turn fosters the premise of the need-to-know, which is most often based on a personal relationship so if one is outside the agency there exists less likelihood of a personal relationship, which results in a lack of intelligence sharing. Without a personal relationship a presumed "not a need-to-know" exists despite the fact that almost all agencies use the DoD model for obtaining a top-secret clearance. In his testimony before congress, Charles Allen (DHS Chief Intelligence Officer) alluded to the prolonged problem of the inability to obtain security

[30] Bowers, "How FBI Is Remaking Intelligence Functions."

[31] Ibid.

clearances quickly enough for essential personnel.[32] The conundrum between culture and intelligence sharing will remain until this problem is overcome.

B. AL QAEDA — A CASE STUDY IN NETWORKING PRINCIPLES AND STRENGTHS

The news media would have one believe that Al Qaeda is everywhere and that the national security of the U.S. is at risk, that another 9/11 disaster could happen at any moment. While the latter is true, because of Al Qaeda's strong network links, there is no consensus among experts about the magnitude of the threat posed by Al Qaeda against U.S. interests. However, one startling fact about Al Qaeda and from which it derives its strengths is the networking principles it uses.

Let us begin with a brief history of Al Qaeda so the development of the networking principles the group uses is clear. The primary founder of Al Qaeda is Osama bin Laden, the son of a Saudi construction magnate of Yemeni origin. While most Saudis practice the Sunni Muslim conservative views, bin Laden adopted the more radical Islamic militant views. When the Soviets invaded Afghanistan in late 1979, bin Laden traveled to the battle front using personal funds[33] to establish himself as a donor to the Afghan *mujahedin* and a recruiter of Arab and other Islamic volunteers for the war.[34] Ironically, because of the feelings of the U.S. toward the Soviets and the invasion, the volunteers recruited by bin Laden as well as himself were considered allies and were funded (the *mujahedin*), covertly for 10 years (1981 to 1991). A colleague of bin Laden, Azzam, helped bin Laden establish a network to help recruit fighters and funds. This network was called the Maktab al-Khidamat (Services Office), also known as Al Khifah.[35] Thus, early on, this first use of a network and its principles helped propel bin Laden and Al Qaeda forward. After the Soviet withdrawal from Afghanistan, bin Laden wanted the recruits to return to their respective home countries for future efforts to topple

---

[32] Charles Allen, *Hearing of the Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee of the House Homeland Security Committee Subject: Examining the Progress of the Chief Intelligence Officer* (Federal News Service, 2006); available from http://www.fnsg.com. [cited July 5, 2006].

[33] *9/11 Commission Report*.

[34] Kenneth Katzman, *Al Qaeda: Profile and Threat Assessment*, ed. Congressional Research Service (Washington, D.C.: Library of Congress, 2005).

[35] Ibid.

pro-Western Arab leaders such as President Hosni Mubarak of Egypt.[36] In control of the Maktab, bin Laden had the resources to work at will and promote his own ideas and ideology. Apparently, it was the Iraqi invasion of Kuwait in August 1990 and ensuing U.S. and multilateral peacekeeping forces (Operation Desert Storm) that turned bin Laden into an adversary of the U.S. He began lobbying Saudi officials to expel U.S. troops from Saudi Arabia. The Saudi royal family rejected his petition and there was a rift between the two parties and a strong difference of ideas and philosophies. During the 1990s bin Laden and his Egyptian confidant, Dr. Ayman al-Zawahiri, operational leader of Al Jihad in Egypt, transformed Al Qaeda into a global threat from a coalition of factions that originated from the Soviet-Afghanistan war. While it can be said that the climax of Al Qaeda operations was the 9/11 attack, there exists no good intelligence for the world-wide numbers involved in Al Qaeda and who is currently in charge. This is a testament to the strength and operational tactics of a network that has grown stronger with each passing year. Even though one cell is destroyed, the remaining cells continue to operate in seclusion or through cooperation with other cells. Even the pressure applied during the Clinton Administration through covert operations against Al Qaeda in 1999-2000 and consideration by the Bush Administration of arming anti-Taliban oppositions groups in Afghanistan have failed to disrupt Al Qaeda.[37] Because Al Qaeda is so decentralized through use of networked principles, only one individual has been arrested as a result of the 9/11 attacks, Zacharias Moussaoui, a U.S. citizen.[38] Other top leaders of Al Qaeda have been captured or killed, but some senior leaders are believed to be in Iran, which that government has admitted but has also refused extradition for punishment.[39] Thus, while it is likely that the core of Al Qaeda has suffered damage to its leadership, organization, and capabilities, its tentacles through networking with other groups have allowed it to continue to spread its anti-Western ideology across wide geographic regions. Some of these groups include the Islamic Group and Al Jihad (Egypt); the Armed Islamic Group and the Salafist Group for Call and Combat (Algeria); the Islamic

[36] Katzman, *Al Qaeda: Profile and Threat Assessment*, 2.

[37] *9/11 Commission Report*, 117.

[38] U.S. Department of Justice, *United States of America v. Zacharias Moussaoui* (2001); available from http://www.usdoj.gov/ag/moussaouiindictment.htm. [cited March 10, 2006].

[39] U.S. Department of State, *Patterns of Global Terrorism* (2003); available from http://www.state.gov/s/ct/rls/pgtrpt/2003/c12153.htm. [cited March 10, 2006].

Movement of Uzbekistan (IMU); the Jemaah Islamiyah (Indonesia)[40]; the Libyan Islamic Fighting Group (Libyan opposition); Asbat al-Ansar (Lebanon); other groups out of Pakistan (Harakat al-Mujahedin, Jaish-e-Mohammad, Lashkar-e-Tayyiba, and Lashkar-e-Jhangvi).[41] Other groups include Al Qaeda in the Arabian Peninsula, as well as emerging threat groups in Africa (particularly Somalia) and Europe.[42]

Why is the Al Qaeda network so strong and resilient? When Lawrence led the Arab revolt against the Turks during WWI, he did so with a community, not an army. This community group was simply a variety of ordinary individuals and tribes recruited for a cause. Does this sound familiar? How was this Arab group organized? First, it was small groups of relationships as there was little if any formal structure. Second, recruits participated at will depending on how much ego, honor, or religious fervor they had. Third, this community was formed in response of one primary goal, to expel the Turks from Arabia, which is analogous to the desire of Al Qaeda and participating terrorist groups, specifically Hezbollah, to expel the U.S. and other westerners from the Middle East. In a very real sense this group exhibited patterns of community, which is an ancient method of warfare, and through the development of the Internet, cell phones, e-mail, and similar tools, has been drastically and efficiently modernized. In networking terms, this type of community, which Al Qaeda through the efforts of bin Laden has adapted, is of the emergent type.

Emergent communities in terms of terrorist tactics exhibit several distinct patterns, yet are difficult to detect because of networking principles. These communities are composed of four segments or parts: (1) leadership, (2) active cell members, (3) individuals seeking active membership, and (4) potential members. Many believe that the Al Qaeda leadership is diminished due to captured or killed leaders and that as a result another attack such as 9/11 is unlikely; this may not be the case. Why? First, this terrorist community is geared toward open source warfare, as is evidenced by its advancing tactics in explosives and communications, and it possesses a resilience of

[40] For more information on this and related groups operating in Southeast Asia, see CRS Report RL31672, *Terrorism in Southeast Asia*; available at http://fpc.state.gov/documents/organization/27533.pdf. [cited May 1, 2006].

[41] Ibid.

[42] Katzman, *Al Qaeda: Profile and Threat Assessment*, 9.

networking principles. Second, the core leadership is still intact and active. Although they have not been physically present, their positions have been enhanced through acknowledgments of the state, particularly the U.S. and the media. They have substituted direct presence with messages that have been broadcast by a variety of technological means, particularly television through delivery of taped statements and through the Internet. Third, the very nature of terrorist networks makes the largest portion of the community, i.e., the members, impossible to detect. If we assume that, of the four components discussed earlier, this portion is approximately one-third of the whole, there is a significant number of terrorists who, as long as the leadership is expressing views and remains intact and active through the means discussed, without physical presence, will carry out attacks to achieve community goals. Fourth, those seeking active membership in the group can form teams with active cell members and still carry out large-scale attacks such as 9/11 through what may be termed "organic" formation, and thus, have the necessary resources for high-capability teams. Finally, other groups such as Hezbollah, who have significant capabilities and appear to be State sponsored, are also networked and have the same goals as Al Qaeda. There is a clear example of this in network technology within the Internet (which was designed to be attack proof), which is the advent of packet switching that sends packets of information through various routes that is then compiled at the end point into a congruent message as if it had never been divided. If one were to disable or attack multiple computer systems and nodes on the Internet, these packets would still get delivered as if nothing had happened. So, too, it is with Al Qaeda and other terrorist groups; this is a testament to network principles and strengths, which implies that fighting this network will require another network — not a grouping of agencies that is as disjointed as is the current IC, but a cooperative network with a common goal. This will require integrated intelligence components.[43]

The terrorist group responsible for the London bus and subway attacks operated through network principles. Observance of any of the maps of the attacks quickly indicates a rule of thumb high-value node selection for disruption rather than symbolism since the attacks were placed on the four points of the compass, i.e., simple rules of city-

[43] Allen, *Hearing of the Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee*.

wide disruptions. The attacks were repetitive, which may indicate that repetition is more important than size of the attack; the D.C. sniper case is an example of this. Perhaps more important the London attacks were rapidly executed, which indicates network design since it is easier to recruit terrorists from an emergent community for a simple disruption rather than for suicide bombings. This is an indicator of participating at will, as discussed previously based on personal conviction or fervor. There are other network principles that Al Qaeda has used and continually gains advances in; an example is global swarming. This is particularly important since bin Laden himself has expressed desire to defeat the U.S. economically and the goal of terrorist swarming will likely converge on urban infrastructure attacks that will cause significant damage and result in economic attrition. As with a packet sent across the Internet, terrorists will continue to use network principles to finance (which can be done via focused attacks to manipulate the stock market, drug sales, black-market guns, and other means) their operations, remain elusive and highly mobile by leveraging encrypted Internet communication globally and public transportation systems, all of which work through networked principles, i.e., nodes and links.

The terrorist network depicted in Figure 1 was developed using social network analysis (a mathematical method for connecting the dots). This network is a representation of the terrorists tracked by the CIA and FBI. Through extended surveillance, the network slowly emerged through results of the Malaysia meeting, the 9/11 attacks, and other events. Such network maps are constructed utilizing typical surveillance and investigative methods such as tracking back a visitor through a car license plate traced back to a rental company at an airport, telephone calls, and so forth. Initially, the network may not make sense of bits and pieces of data; but with time, direct links and nodes are visible. Although the network illustrated in Figure 1 was developed through hindsight, it shows two important features: (1) the strength of the Al Qaeda network; and (2) the number of links developing around Mohammed Atta (near top one-third in center — green square) indicating his importance as a developing central hub.

The Al Qaeda network depicted in Figure 1 is but a small sample of the entire terrorist organization. This network only denotes the cells that were relatively or closely associated with the 9/11 attacks. If the scale of Figure 1 was magnified to show the entire

Al Qaeda network and those who are affiliated with Al Qaeda from other terrorist groups, the true scale and strength of this network would be staggering. It would be worthy of our attention because of its complexity and for its networking strength, which helps terrorists remain undetected. Perhaps a good analogy is that Figure 1 is similar to an ice-berg for which the tip is but a very small representation of the whole. As mentioned previously, the only way to fight such a network will be with another network. Network theory and methodology will be discussed more fully in Chapter III.

The goal of LE or the IC would be to remove nodes (representative of terrorists) from the graph (Figure 1) by apprehension or death so that the organizational structure is disrupted. Mathematically, the question would arise as to how many nodes must be removed before the cell or organization becomes disconnected or separates into two or more pieces. We can write an equation, based on ordered sets in network theory that will quantify the effectiveness of an operation against an Al Qaeda cell for how effective LE or the IC has been in disrupting a particular terrorist cell. For example,

$$\Pr(\Gamma, k) = \frac{Cut(\Gamma, k)}{\frac{n}{k}} \tag{1}$$

where Pr(Γ,k) is the probability that the cell, Γ, has been disrupted once *k* members have been apprehended or killed. Cut(Γ,k) is the number of cutsets in the ordered set Γ with *k* members. Also, $(\frac{n}{k}) = (\frac{n!}{k!})$ (n-k)! and r! = r(r - 1)(r - 2) · · · 3 · · · 2 · · · 1 for a positive whole number *r*. However, the purpose is to demonstrate that terrorists work through a networked approach; therefore, to be effective at fighting them, so too must LE and the IC.

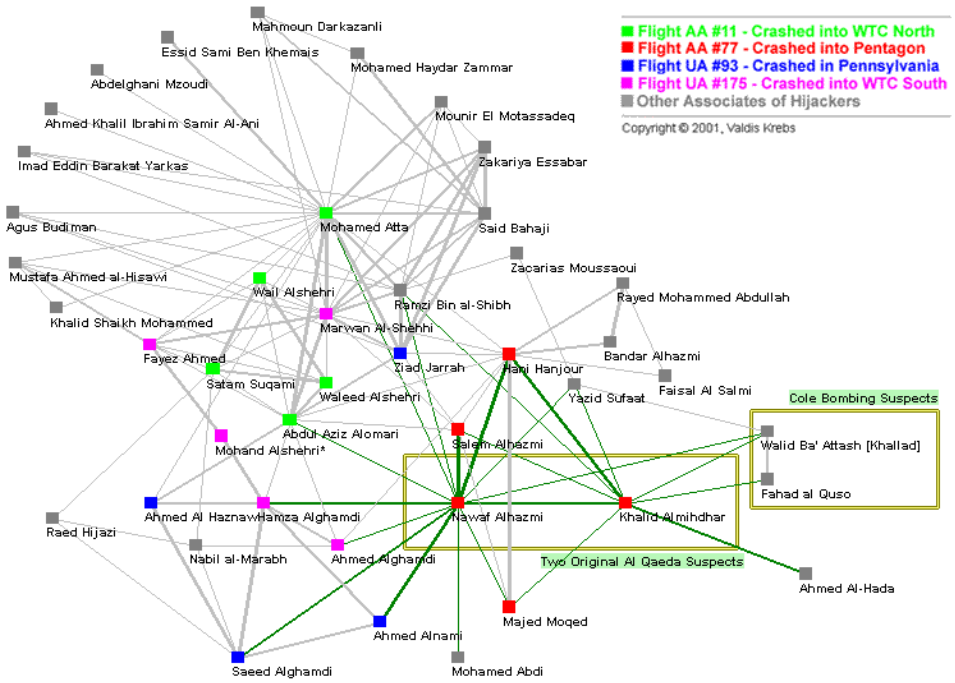


Figure 1. Network analysis of terrorist (groups) involved in the World Trade Center attacks (From: Valdis Krebs).[44]

C. SUMMARY

Intelligence failures have not occurred because of lack of technology, but persist due to:

- Agency cultures that keep the sum of parts separated, causing animosity and lack of cooperation.
- Need-to-know rather than need-to-share attitude despite the fact that almost all IC and LE groups use the DoD security-clearance model.

Failures in intelligence can be reduced by:

- Applying network theory to agency-wide structure and to intelligence collection and sharing processes.

44 Valdis Krebs, "Connecting the Dots - Tracking Two Identified Terrorists," *Orgnet.com*, 2005; available from http://www.orgnet.com/prevent.html. [cited May 1, 2006].

III. NETWORK THEORY AND METHODOLOGY DEVELOPMENT

A. BASIC THEORY

For about the past 10 years, mathematicians, physicists, and sociologists have advanced the scientific study of networks and have identified surprising commonalities among various industries and other relationships such as the way airlines route flights, interaction of individuals at social events, distribution of electric power, and even the way the Internet connectivity works in regard to communication between individuals. Network theory is able to map non-obvious connections and relationships (links) between nodes (individuals or groups) with the goal to expose patterns that are not recognizable or apparent. However, while American scientists and others seem to be just discovering the complexities and strength of network theory, terrorist adversaries appear to have substantial experience in this field. Terrorists have carefully nurtured their networks and intelligence agencies are just beginning to catch on; but what goals and hidden agendas can spies uncover that will help protect the homeland? Are these networks so strong and embedded that they are impregnable, or will the intelligence priorities and operational objectives be able to identify them? Regardless, one important aspect to remember is that networks are not random. They are much like terrorism, well planned, complex and dynamic.

Whether working in domestic or international intelligence, at least in terms of a network theory-approach we must ask, what are the priorities for intelligence collection and sharing? The goal is to connect the dots or utilize the links between the nodes. Thus, the key to effective intelligence is link analysis, i.e., identifying the strength of the relationship, which was not done during the Malaysia meeting investigation. As a matter of fact, this is generally the cause of our intelligence failures. In simplistic terms, we call this pattern recognition because we are attempting, through extraction of large, almost overwhelming volumes of information from whatever the source, to detect a pattern between seemingly unrelated people, events, and other details. By setting the right priorities we can connect the nodes or entities because link analysis will help determine the relationship or pattern between those entities. In general terms the problem is making

sense of the wealth of information at our disposal. To separate the "white noise" from the pertinent information sought, priorities must be set. First, management of knowledge rather than information is a necessity. It must be decided how information can best be managed to support the critical objectives of the enterprise/agency. The knowledge sought can be obtained through various sources, especially data mining, pattern recognition engines, and mental models. Second, the latest and best knowledge of what actually works must be used. No intelligence entity can rely on obsolete knowledge. To be effective, reliance on good intelligence and analysis must be based upon evidence-based management. Third, in terms of domestic intelligence and even international cooperation, intelligence from Federal sources must be passed to local police, and vice versa, in an efficient and timely manner. Because almost all agencies use the DoD model for security clearances, the need-to-know for those who have the clearance is an obsolete knowledge and reflects gross mismanagement of intelligence as well as cultural bias. The current border security problems along the U.S. southern border with Mexico are an excellent example.[45] Further, DNIN would help solve many of the intelligence capturing and dissemination problems associated with border security and intelligence.

The priorities are weighed against the information obtained, which can come from a wide variety of sources such as local law enforcement, HUMINT agents, news feeds, press releases, Websites, magazine articles, keynote addresses, Web blogs, corporate strategies, geospatial information, panel discussions, marketing materials, and more - especially, transaction space. The list is virtually endless.

B. REQUIREMENTS FOR COOPERATION AND INFORMATION

The requirement for greatest chances of success for consistent cooperation and information to and between IC agencies and to local LE and other necessary parties is that one group or agency becomes the central hub for both foreign and domestic intelligence coordination. This restructuring may have been solved by the creation of the Office of Intelligence and Analysis within the Department of Homeland Security. Mr. Charles Allen, the recently appointed director of that office, set forth priorities for the

[45] Chris Strohm, "Border Intelligence Plan Still in 'Early Stages,' Official Says," *GovExec.com*, June 6, 2006; available from http://www.govexec.com/dailyfed/0606/062806cdpm1.htm. [cited July 5, 2006].

organization in testimony before Congress.[46] The DHS IA has the Congressional Mandate to fulfill this role and thus, will be used as the "Central Hub" or the owner of DNIN.

C. RELATIONS AND CONNECTIONS — CONNECTING THE DOTS

The term "connecting the dots" has become quite prevalent since 9/11, perhaps more for the intent to make needed changes to the IC than to assign blame for the failures of 9/11. Thus, most frequently this term is used in the past tense. Given the term denotes connecting a relationship to an entity or person, this concept of connecting the dots should be used to help fight the GWOT because in a real sense, it infers a networked approach to gathering intelligence. Two key cases illustrate this point. First, after 9/11 and throughout the Commission Report hearings, LE and the IC presented great amounts of testimony about the relationship of the hijackers with each other, Al Qaeda, where they had come from, and what the implications were. The Malaysia meeting was a case of connecting the dots, although linking the individuals with the organizations proved to be difficult. Second, perhaps one of the best cases was during the end of the Cold War when the CIA believed the Soviet economy was growing at a constant rate, but in fact it was not. HUMINT from the streets of Moscow and other large Soviet cities soon indicated the economy was about to implode.[47] This intelligence insight provided President Reagan the information necessary to spur the end of the Cold War. A simple matter of "connecting the dots" and analyzing the correct relationships between the economy and various industries played a key role. Further, the information was not secret at all; it was gained from everyday occurrences on the streets of Moscow — from workers complaining about lack of soap and other products, factories closing from lack of raw goods, and workers rioting. Suddenly, almost as quickly at it had begun, the Cold War was over. However, we now find ourselves in a new war that we have been very poor in performance of network analysis, i.e., "connecting the dots" between one of the earliest

---

[46] Charles Allen, "Written Statement before House Committee on Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment." Department of Homeland Security House Permanent Select Committee on Intelligence Subcommittee on Terrorism/HUMINT Analysis and Counterintelligence, 2005.

[47] Herbert E. Meyer,"Connecting the Dots," *National Review*, April 8, 2004; available from http://www.nationalreview.com/comment/meyer200404080954.asp. [cited March 13, 2006].

incidences of terrorist attacks beginning in 1993 — the first attack on the World Trade Center. A string of attacks ensued throughout the 1990s, the Khobar Towers in 1996, Kenyan and Tanzanian Embassies in 1998, and the USS Cole in 2000. The dots or rather the links, were always there; war had been declared on the U.S. and its allies, but the IC did not "connect the dots." Rather than declare war in word, it had been declared in deed, and because the incidents were linked to terrorists, they were treated as separate incidents and not as the beginning of a global movement, perhaps because the attacks were not attributable to a state or standing army. Also, like the streets of Moscow and the free-flowing intelligence in them, LE does the same on the streets of America today. Working in tandem with network-sharing principles and with the IC, perhaps they, too, can force the terrorists to fall.

Many believe that Al Qaeda has few teeth left to mount a serious attack against the U.S. or its allies akin to 9/11. However, connecting the dots of the past to those of the future would defy this notion, i.e., it would give us insights. A good example is the London attacks on July 7, 2005, in which a group called the "Secret Organization of Al Qaeda in Europe" claimed responsibility.[48] This clearly demonstrates that, although Al Qaeda itself did not carry out the attacks, another network that supports Al Qaeda in common goals did. Additionally, there have been various other global events that illustrate this same pattern such as the Madrid, Spain, train attacks in 2004. While it was initially believed the ETA was responsible, Al Qaeda, through a video, claimed responsibility.[49] There are many terrorist groups that have been influenced by and psychologically link to Al Qaeda and therefore, terrorists need to be viewed in terms of a global network and not in terms of separate or specific groups. Treating terrorists as a global network will allow fighting a network with a network.

Connecting the dots has become increasingly more difficult because of technological advances. The IC and other private and public sector agencies are literally drowning in data. There is so much data that it is difficult to collect, process, analyze and obtain actionable intelligence. It is becoming increasingly more important to have the

[48] MSNBC Staff, "Islamic Group Claims London Attack," *MSNBC News*, 2005; available from http://www.msnbc.msn.com/id/8496293/. [cited March 13, 2006].

[49] BBC News Staff, "Al-Qaeda 'Claims Madrid Bombings'," *BBC News*, 2004; available from http://www.news.bbc.co.uk/2/hi/europe/3509426.htm. [cited March 13, 2006].

ability to identify threats in the out-of-the-ordinary data or what has also been termed non-obvious recognition. As the terrorist adversary has become much more mobile, smaller in size, and agile compared Soviet forces during the Cold War Era (which was less mobile and much larger), the sifting of data for pre-established patterns is less useful. This has caused a paradigm shift to look for non-obvious patterns because looking for pre-established patterns has become ineffectual. This also requires sifting and sorting much larger volumes of data, as well as forward rather than backward thinking. Post mortems always illustrate evidence that should have given clues that an attack was imminent 9/11, for example. However, using the same evidence and moving forward to the next dot gives a completely different picture, which is why it is important to connect the dots by using non-obvious patterns and then predicting forward.

D. SHARING DEVELOPMENT AND IMPLEMENTATION

The Japanese attack on Pearl Harbor on December 7, 1941, and the terrorist attack on the World Trade Center on September 11, 2001, have emphasized an important point — care must be taken not to lose the important information in day-to-day events, i.e., the signal must be higher than the signal-to-noise ratio. The IC, LE groups, and others must mimic the adversary; we must respond quickly, be flexible, and adapt easily. The bureaucratic policies of the past must make way for a networked sharing, multi-agency cooperation. This is the only way to reduce the number of future catastrophic events. As an example, during the Cold War, the Soviets changed slowly due to their size and scope of operations. Contrasting this to present day, terrorists and other criminal groups are very agile, adapt quickly, and are very small. Today's terrorist organizations can attack from many directions, disperse their assets globally, and use a variety of unconventional tactics to evade the IC and attack the U.S. and other peaceful nations. States utilizing terrorist tactics can employ these same methods. What would happen if 40,000 suicide bombers were released on 29 American and British targets? Dr. Hassan Abbasi, head of the Center for Doctrinal Strategic Studies in the Revolutionary Guards in Iran, who is under the authority of President Mahmoud Ahmadinejad, has informed Western sources that these suicide bombers are poised and ready to strike if the U.S. or Israel attacks its

nuclear sites.[50, 51] Because these terrorists are so scattered and mobile, it is imperative that to detect the new threats, data must be collected from a wide variety of sources that will vary with time. To analyze this data properly, it will need to be shared with a great many experts with the goal of connecting the dots. Using a networked approach this will be advantageous since it is impossible to investigate every piece of information and also maintain a high alert status. Agility will be the key to adaptation so that the IC and LE groups can make a concerted effort at the right time for resource concentration against the problem. Using a networked approach, the IC will be able to move people and resources quickly, deliver information easily to those who need it, and draw on expertise from around the Nation and the world and from multiple agencies to deliver a useable product. This would be particularly useful for border-security issues and intelligence to address the concerns of congress.[52] Networking will allow this agility. Also, networks operate from four primary factors: (1) trust; (2) tasks; (3) money (including resources); and (4) strategy or goals. A combination of all four factors develops the strongest networks.

E. THE SHARING MODEL

Development of a sharing model must consider the potential components that it may involve. These components are geographic, personnel, computer networks, regional centers and connecting participants, and nodes and links. The initial stage of the sharing model is adopted from the U.S. Census Bureau because, while there is much talk about how to share intelligence, little has been written about where that intelligence comes from. Within the U.S. that intelligence will come from states, localities within the state, across regions and finally encompassing the entire U.S. This is a fairly accurate premise about how the original censuses were set up and taken. In fact, the data-requirements analysis of the Census Bureau had substantial impacts on the history of computing, which has become the most significant tool for intelligence collection and sharing.

---

[50] Fox News Staff, "Tehran Threatens West with Homicide Attacks," *Fox News.com*, 2006; available from http://www.foxnews.com/printer_friendly_story/0,3566,191910,00.html. [cited April 24, 2006].

[51] Marie Colvin, Michael Smith, and Sarah Baxter, "Iran Suicide Bombers 'Ready to Hit Britain'," *London Times*, 2006; available from http://www.timesonline.co.uk/article/0,,2087-2136638,00.html. [cited April 24, 2006].

[52] Strohm, "Border Intelligence Plan Still in 'Early Stages,' Official Says."

Herman Hollerith built tabulators under contract to the Census Bureau to dramatically speed the process of analyzing the 1890 census, which was an important step in establishing a market for automated data processing. Most of the major census bureaus around the world leased his equipment and purchased his cards (key-punch cards). To make his system work, he invented the first automatic card-feed mechanism, the first key punch, allowing a skilled operator to punch 200-300 cards per hour. Holleriths's company (Tabulating Machine Company) later merged with other firms to become the Computing Tabulating Recording Corporation, which, under the presidency of Thomas J. Watson, was renamed IBM in 1924.[53]

Geographically, the Census Bureau is composed of four regions and nine divisions (see Figure 2). The regions are not grouped by geographical, historical or cultural bonds, but were initially set up by population base, which has significantly changed with time as many areas have become much more populated due to the influences of agriculture, water supplies, manufacturing trends, marketing and transportation. At the same time, these trends have caused a variety of infrastructure developments within geographic regions of the census map. For example, in California, New York, and New Orleans, sea ports represent a significant infrastructure, whereas in Houston, Dallas, and Lincoln, rail transport is a more critical infrastructure. Because of this change in population and infrastructure, the census regions, for purposes of homeland security and population base, have been changed to form the new base for the geographic component of the sharing model (Figure 3). Each separate region on the new map ranges in population from about 40 to 55 million. While the Midwest region makes up the largest geographic area, it also has the smallest population. An approximately equal population base will allow development of an adequate computer/IT network in one geographic region that can be mirrored in another and deliver economy of scale.

Richard Armitage (Deputy Secretary of State) said, "Probably the most dramatic improvement in our intelligence collection and sharing has come in bilateral cooperation with other nations — those we considered friendly before 9/11, and some we considered

[53] Wikipedia Contributors, "Herman Hollerith," 2005; available from http://en.wikipedia.org/w/index.php?title=Herman_Hollerith&oldid=61950396. [cited December 9, 2005].

less friendly."[54] Such strides in intelligence sharing, while important will accomplish little if intelligence sharing cannot occur effectively within the U.S. The sharing model must include a regionalized structure for agencies, regionalized databases, specific regions, specific IT functions, and other necessary components. These must all feed back to a central hub in charge of DI, i.e., the DHS IA and Chief Intelligence Officer. Thus, this model must begin at the physical layer (as described above) — geographical, computer sharing/IT, intelligence collection/analysis — and include the central office where final collection and processing will occur.

Figure 2. Map of U.S. Census Regions.
(From: http://www.census.gov/geo/www/us_regdiv.pdf)

The primary purpose of the geographic component for the sharing model is that information must come from somewhere, and organizational development on the geographic level will expedite model development. This base will consist of a regional structure that will become the sharing and dissemination parties, a central hub, 16 member agencies of the IC, nationwide LE groups, and a method of sharing, i.e., computer systems and IT. The proposed network structure is illustrated in Figure 4 and is

[54] Richard Armitage, *Intelligence Sharing and September 11 Attacks* (U.S. Department of State, September 19, 2002); available from http://www.state.gov/s/d/former/armitage/remarks/2002/13566.htm. [cited March 20, 2006].

designed in this manner due to the attributes of network principles which is why link and nodal network analysis is so important. Additionally, the cities of Los Angeles, Denver, Dallas, Chicago, Atlanta, and New York were chosen as regional centers not only for population, but more importantly for the significant LE resources these cities possess. For example, social network analysis (SNA) is the mapping and measuring of relationships and flow between people, groups, organizations, computers, and other information and knowledge-processing entities. The intelligence-sharing network is composed of all these components. As with a terrorist network, this sharing network must have strong links between all entities. As an example, link analysis is about making connections (connecting the dots) that represent meaningful links between data elements that will allow detection of complex relational structures to indicate patterns of interest. Post-9/11, connecting the dots was relatively easy, but it was not connecting the dots that caused the greatest difficulty. Rather it is deciding, which dots to connect that is most important; this argues why the sharing network must be a true network and why it is so important for all IC and LE groups to work together for the common goal.

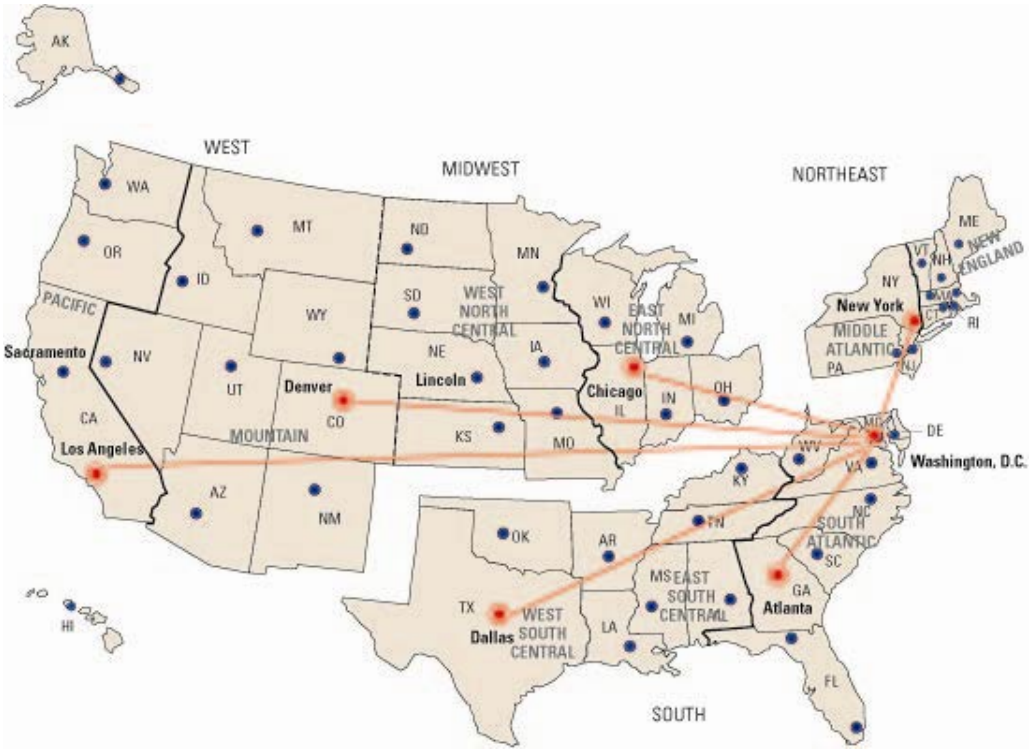


Figure 3. Six Region Intelligence-Sharing Model for the U.S.

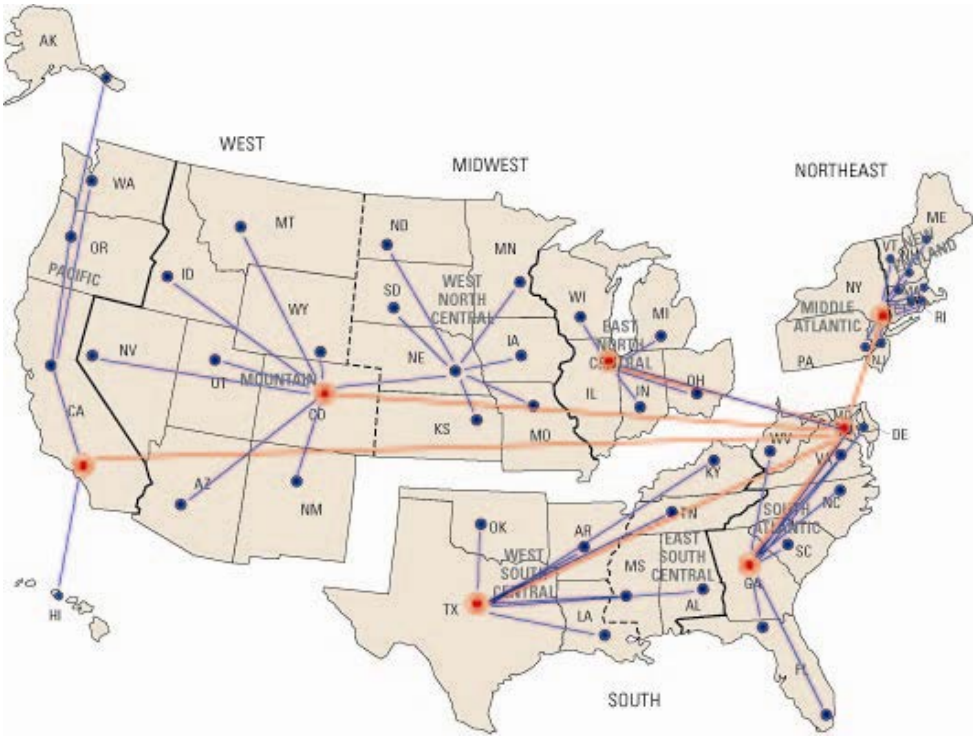


Figure 4. Six-Region Networked Intelligence-Sharing Model for the U.S.

Why is a network-centric approach so important? There is so much information that all agencies are becoming overwhelmed with information overload. Further, past experience has shown that information overload in intelligence makes failures inevitable.[55, 56] A network approach will allow pattern recognition at a heightened level. Although it will not change the need for qualified and experienced analysts and other intelligence and LE personnel, it will assist them in detecting the "needle in the stack," i.e., let us move the stack and find the needle and not look through all the hay.

Let us investigate a possible scenario. A deputy from the Los Angeles County Sheriffs Department (LASD) is told by an informant that word on the street indicates a shipment of explosives, possibly a WMD, will be smuggled into the Los Angeles area next month. By itself this is a small piece of non-actionable intelligence; there is no pattern and it may not be true. However, the informant has always been known to be reliable, and the deputy passes along the information. The task now becomes one of

55 Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 31, no. 1 (1978).

56 Richard J. Heuer, Jr., "Psychology of Intelligence Analysis," Center for the Study of Intelligence (Langley: Central Intelligence Agency, 1999).

making connections between otherwise meaningless bits of information, which will be at the core of transnational threat analysis. The information from LASD is quickly reported to the regional centers in Los Angeles, Dallas, Denver, Atlanta, Chicago, and New York. At the same time it is reported to the central hub (DHS Office of Intelligence Analysis) in Washington, D.C. In a matter of minutes the other 15 member agencies of the IC also have the information. Upon further investigation, the LASD deputy learns from DEA the nearest source from the informant was a past accountant for a Cali, Columbia drug cartel. Hence, the first connection or link in what may become a network is identified. A few days later the informant indicates the type of bomb is termed a backpack explosive; this is of great concern since it could be a Russian backpack nuclear weapon made in the 1960s for use against NATO targets in time of war and consisting of three "coffee can-sized" aluminum canisters that must be connected before detonation. Formerly in custody of the Ninth Directorate of the KGB and having a 3-5 kiloton yield and at the upper range, the explosive would be about one-third the yield of the Hiroshima bomb during WWII. U.S. intelligence sources have believed that Osama bin Laden or other groups could have obtained some of these weapons.

The DEA is able to determine that the Cali cartel member has ties to Al Qaeda operative in Yemen who the FBI linked to the USS Cole bombing. The CIA and DIA have additional information on links from Yemen of these same individuals with ties to Pakistan and Iran. One of the individuals in Pakistan was linked directly to a Russian nuclear physicist and an Iranian physicist. Suddenly, analysts in the central hub notice a pattern emerging as previously obscure links between individuals appear much stronger. Through data mining, intelligence reports, transaction space and other records, central hub analysts are beginning to put pieces of the puzzle together using the DNIN network-centric approach. The Atlanta regional office garnered information about a shipment of car parts destined for New Orleans via India, but India does not make car parts. As a result of the regional office report, DHS IA requests the Office of Naval Intelligence to become involved and track the maritime cargo shipment. Additional CIA reports arrive, linking various individuals to relationships with an incident in September 2001 in which Israeli security arrested a man linked to Osama bin Laden with a radiological backpack bomb as he attempted to enter Israel from the Palestinian Territories via a border

checkpoint at Ramallah. Within this new sharing paradigm, the FBI, working closely with CIA and DHS, detects a relationship between the Yemen and Pakistan ties to specific individuals in New Orleans, New York, and Los Angeles. Additional reports from the LA TEW, provides evidence of stronger individual ties. A pattern is emerging that signifies a serious threat, and combined criminal fighting and intelligence efforts have been able to detect it, when likely in the past they would not have been able to do so. A planned attack that was to involve transport of a small nuclear device from the shipping port at New Orleans to the city of Los Angeles has been thwarted, and the terrorists, at least those within CONUS, have been taken into custody. This is the power of the DNIN networked intelligence sharing. This ability has come not from the creation of a new domestic intelligence agency but through giving oversight to one group to act as a collector through and from all others and the authority to develop a dedicated national intelligence network that shares multiple databases and resources of all types and that crosses criminal, border, terrorists, and other intelligence segments.

F. THE NETWORK ORGANIZATIONAL STRUCTURE

The goal of this network structure is to prove quantitatively that, constructed in the proper manner links become shortened and thereby stronger, which will qualitatively allow better information sharing. Let us suppose that the regional intelligence-sharing centers are as suggested in Figure 4. From east to west, these centers are New York, Atlanta, Chicago, Dallas, Denver, and Los Angeles and of course the central hub, which is in Washington, D.C., the single intelligence authority. As mentioned previously, even businesses now realize that the old hierarchal structure is no longer competitive due to global changes in technology, management, manpower, outsourcing, and many other factors. Put in hierarchal form, the regional structure shown in Figure 4 would appear as in Figure 5.

The round nodes at the bottom of Figure 5, below the named triangle, can represent individual cities, police forces, government or non-government organizations, or other entities, and on a regional basis, there could be a great many of these. The links from round node to triangle and from triangle to triangle represent the relationship between each entity for reporting and/or data flow. As represented, this organizational

structure is hierarchal and has been used extensively in the past for IC management. It is not very flexible or adaptable to change. However, utilizing a network approach, the regional centers must not stand alone, reporting only to the central hub; they must share knowledge among each other to integrate the system. Linking the regions together flattens the structure and builds a networked community. The result of linking the regional centers is illustrated in Figure 6.

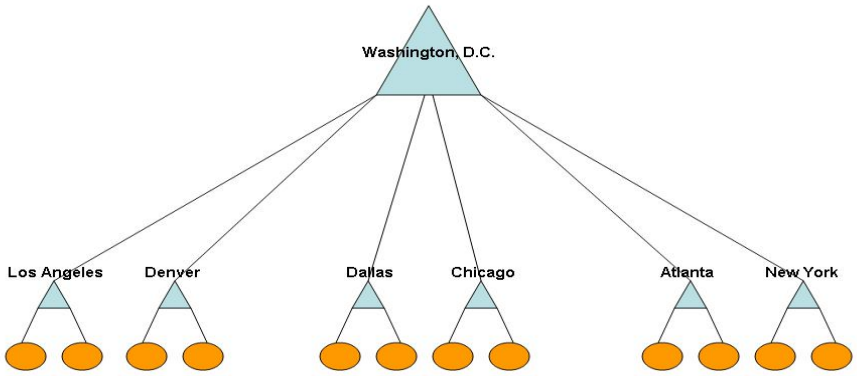


Figure 5. Six-Regions Hierarchal Organizational Structure — Intelligence-Sharing Model for the U.S.

While there may be some management problems in terms of accountability with the networked organizational structure (Figure 6) it is very adaptable and agile and will perform rapidly in regard to information sharing. The idea in networking is not to pass the information through too many nodes — the fewer the better. This would typically indicate that personnel would not have to continually obtain directions from a central superior. Rather, they would be more autonomous, which means they can quickly combine key pieces of information and disseminate it according to protocol. In mathematical terms, linking the regions into a network shortens the path length of the relationship; the shorter the path, the better and quicker the sharing and, thus, the stronger

the relationship. The goal of course would be not only to link the regions, but to link the IC as well. If we now have an overview of the system, it is obvious that a network is beginning to emerge (see Figure 7).

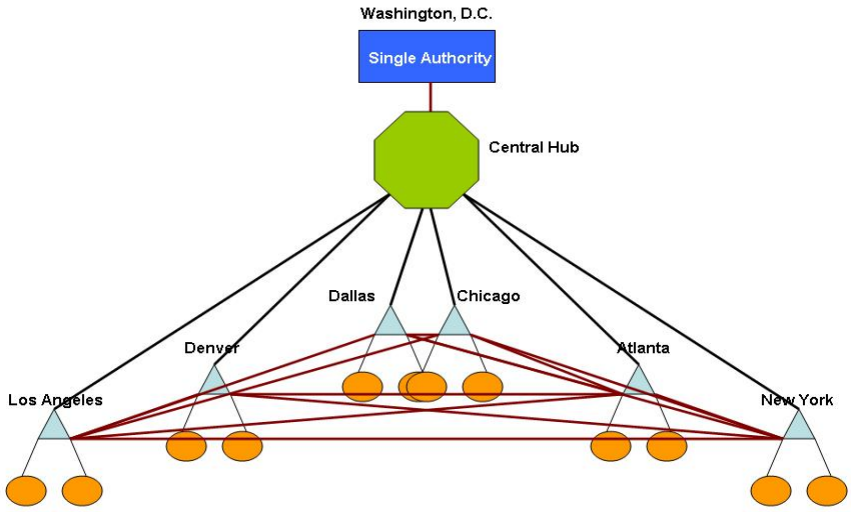
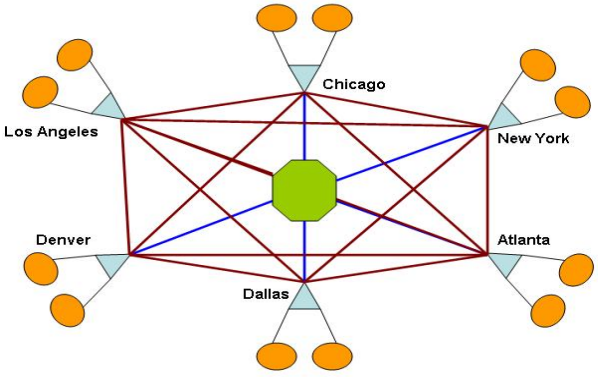


Figure 6. Flattened Organizational Structure — A Regionally Networked Structure.



.

Figure 7. An Emerging Network.

Within the IC there are 16 intelligence agencies, all collecting and disseminating information; but as has been shown, cooperation among agencies is lacking and therefore, sharing is minimal. Figure 8 shows an overview of the 16 member agencies of the IC. Note that in Figure 8 the IC members are connected to the central hub that has been denoted in Figures 5-7. The network architecture is becoming more complex so that the network capabilities are becoming much stronger. Assuming we connect the 16 member IC with the regional structure, a powerful networked intelligence-sharing community is created (Figure 9). To reduce clutter and illustrate the concept well, a side view with only two of the agencies connected to the central hub and to the regional centers is shown in Figure 10.

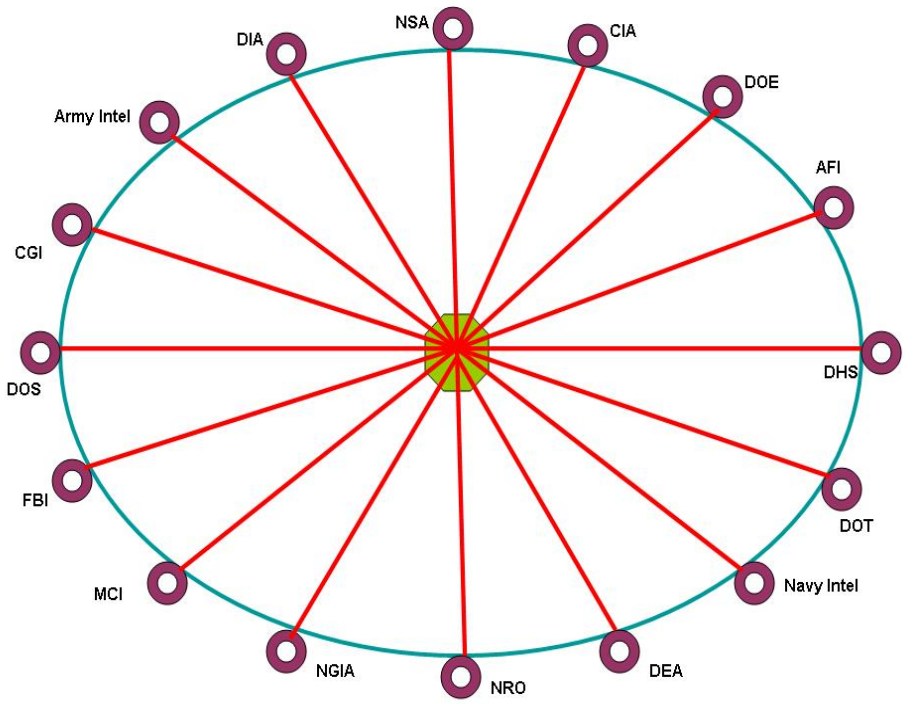


Figure 8. 16 Members of the IC Connected to a Central Hub (DHS IA).

The 16-member IC represented in Figure 9 is listed, beginning at left center and progressing in clockwise direction, as DOS (Department of State), CGI (Coast Guard Intelligence), Army Intel (Army Intelligence), DIA (Defense Intelligence Agency, NSA (National Security Agency), CIA (Central Intelligence Agency), DOE (Department of

Energy), AFI (Air Force Intelligence), DHS (Department of Homeland Security), DOT (Department of Treasury), Navy Intel (Navy Intelligence), DEA (Drug Enforcement Administration), NRO (National Reconnaissance Office), NGIA (National Geospatial-Intelligence Agency), MCI (Marine Corps Intelligence), and FBI (Federal Bureau of Investigation). The key to a strong network is the relationships among nodes (the link); *the shorter the link or path, the stronger the network.* This has been termed network metrics.[57] Assuming the President remains in his current position of the ultimate intelligence user the addition of the central hub (Figure 6) initially increases the path length of the President (Table 1), but as the network becomes more interconnected, the President's path length is shortened (Table 1). Further, as all the agencies are fully connected to each other and the regional centers within the network (shown in Figure 10), the path length shortens dramatically (Table 1) so that for the central hub, R=1 (where R is the radius — measured length).

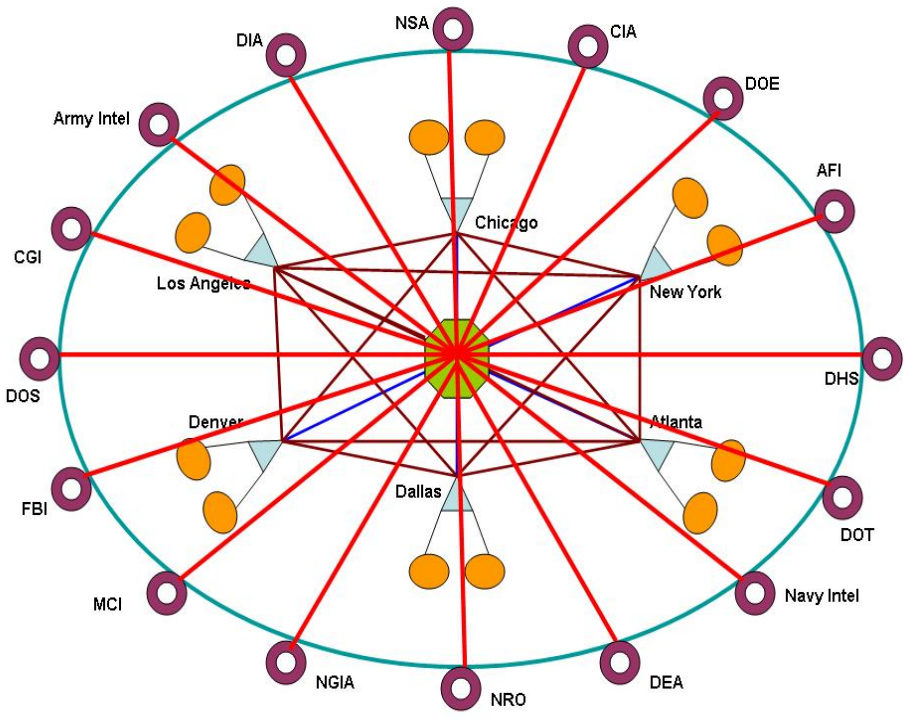


Figure 9. 16-Member IC Joined with the Regional Network Through Central Hub.

[57] Duncan J. Watts, *Small Worlds: The Dynamics of Networks between Order and Randomness* (Princeton: Princeton University Press, 1999).

The interconnected network, which now links all 16 members of the IC to the central hub as well as the regional centers, will shorten the path length for intelligence sharing, both mathematically and organizationally (Table 1). This shortening, in addition to strengthening sharing should thereby reduce intelligence failures.

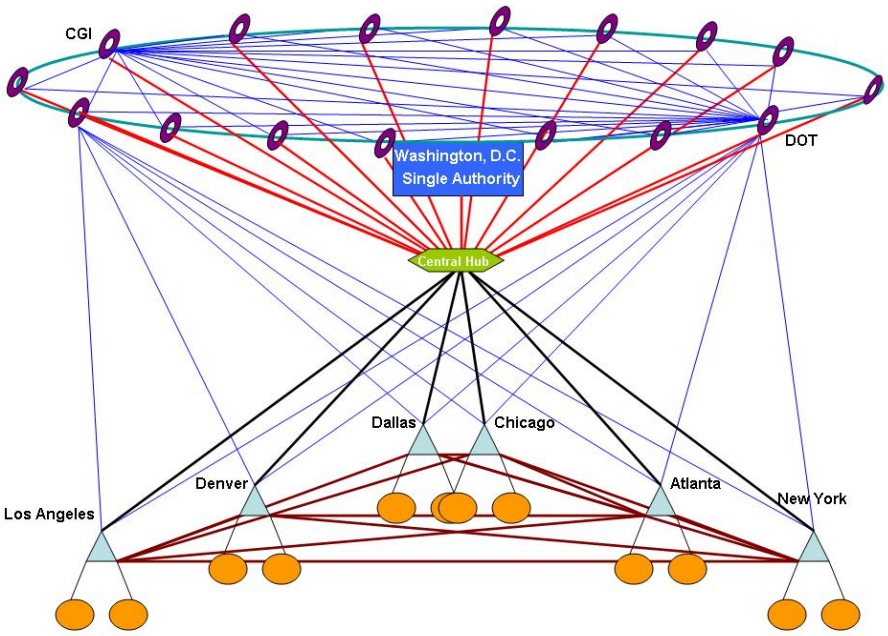


Figure 10. Side View of Entire Network Illustrating Connectivity of only two IC Members but Denoting the Enhanced Collection and Sharing Capabilities.

A commission report to the President delivered two specific findings: (1) "The Intelligence Community's performance in assessing Iraq's pre-war weapons of mass destruction programs was a major intelligence failure. The failure was not merely that the Intelligence Community's assessments were wrong. There were also serious shortcomings in the way these assessments were made and communicated to policymakers" and (2) "In sum, today's threats are quick, quiet, and hidden. We need an intelligence community that is truly integrated."[58] An integrated and network-based IC will help prevent such failures.

[58] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (Washington, D.C.: U.S. Government Printing Office, 2005).

Table 1. Shortened Path Length Between Nodes Denoting Increased Sharing Strength

Network Structure	Overall Agency/Regional Path	President's Path
Figure 4 Washington, D.C. Entity to Regional Center Disconnected Regional Center	 R=2 R=4 R=3	 R=2
Figure 6 Central Hub Entity to Regional Center Disconnected Regional Center	 R=2 R=3 R=2	 R=3
Figure 7 Central Hub Intelligence Agency	 R=2 R=3	 R=2
Figure 8 Central Hub Entity to Regional Center Disconnected Regional Center Agency to Regional Center	 R=2 R=3 R=2 R=3	 R=2
Figure 10 Central Hub Agency to Regional Center Central Hub	 R=1 R=2 R=2	 R=1

Clearly, a network has more distinctive features than conventional organizations that make it stronger for a great many contemporary evaluation tasks. First, focusing on the connections and "patterns" of relations between entities rather than attributes offers both a different conceptual and theoretical perspective. Second, shifting to a relational and systemic collection and dissemination process is more aligned to the context of the paradigm shift in technological abilities as well as the overload of information volume that confronts us. Network analysis also lends the ability to examine and analyze relationships at a different level, whether single or interrelated. Finally, network analysis permits a description of very complex processes as well as a capacity to draw on a range

of methods that can be integrated qualitatively, graphically, and quantitatively, which will allow a more thorough or, in intelligence terms, more "fine-grained" analysis. An example of this analysis can be seen in Figure 11 in which a network analysis of the new, networked community was performed to determine allocation of resources and current risk. Note that the blue lines in Figure 11 represent the links/relationships of each agency to the central hub in the center (surrounded by a green line); the six regional intelligence-sharing centers are in the lower right quadrant. Thus, in addition to strengthening intelligence sharing, the network itself is granted powerful tools for self analysis. Perhaps the greatest weakness of a network is that, in order to acquire network data sets and to obtain a full response rate, there is a need to establish a relationship with the network and its members. This will have immediate implications in the accuracy of reported data and possible loss of objectivity.[59]

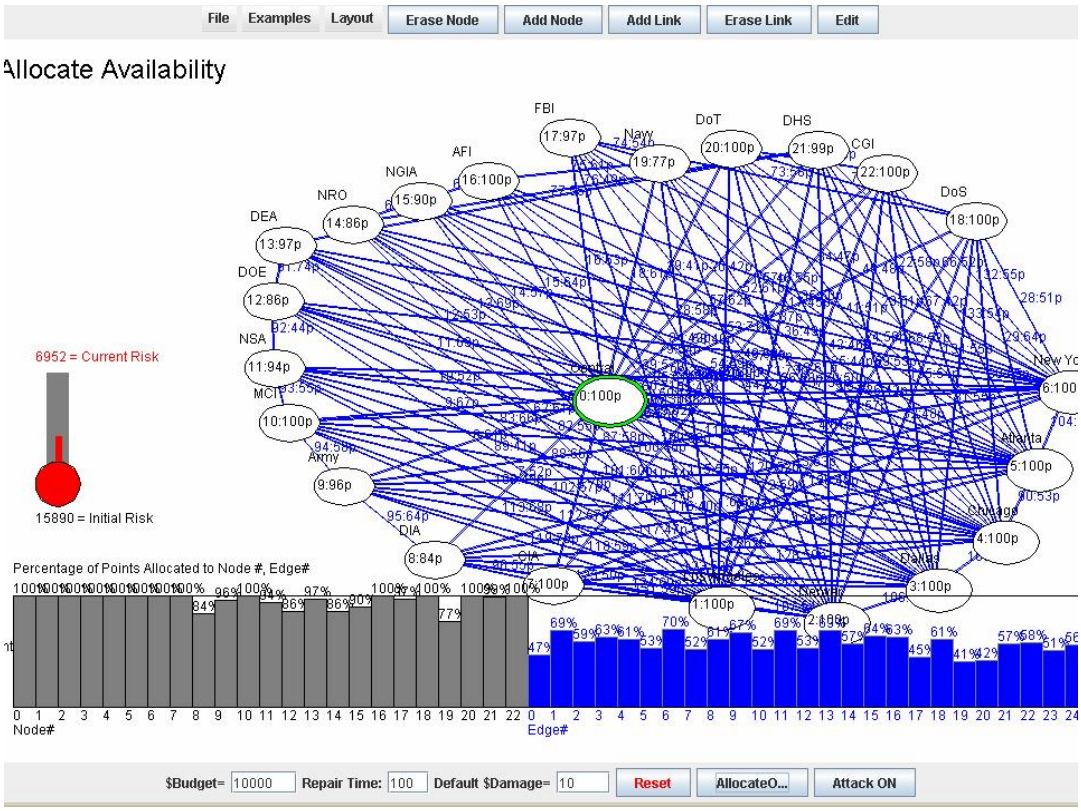


Figure 11. Network Analysis of Regional Intelligence-Sharing Network when Connected to Central Hub and 16-Member IC.

[59] R.A.W. Rhodes, "Putting People Back into Networks" (paper presented at the Australasian Political Science Association 43rd Annual Conference, Brisbane, Australia, September 24-26, 2001).

The development of such a strong network would allow law enforcement, homeland security, and the intelligence community to accomplish three primary tasks. First is the ability to examine ties between suspected criminals or terrorists and determine whether these ties are weak or strong. For example, because the dynamics of a network are constantly changing the ability to determine who is "in" or who is "out" would become a valuable tool (to identify patterns). Second, the best practical application of network analysis could be used to identify suspects and then map their networks to determine where they lead. Third, this network would allow for better prediction of certain future behaviors, making for clearer evidence and a better likelihood of prevention, response, and prosecution.

G. SUMMARY

The goal of effective intelligence is to connect the dots. This can be accomplished by the IC and LE communities by:

- Instituting organizational structures supportive of network processes and principles.
- Setting priorities to allow link analysis.
- Identifying relationship strengths.
- Replacing the obsolete need-to-know with need-to-share policy.
- Making knowledge a primary focus.
- Instituting evidence-based management for intelligence collection.
- Placing one agency or group such as DHS IA into the central role of being the hub for both domestic and foreign intelligence coordination.
- Developing agility — only networked principles will allow this.
- Operating from the four primary factors of networks — trust, tasks, money, and strategy/goals. These factors develop the strongest networks.
- Developing regional sharing centers due to the scale, scope, and volume of U.S. domestic intelligence. This will enhance sharing by fostering

cooperation and strengthening relationships (see Chapter VII). Network analysis lends the ability to examine and analyze relationships.

The use of networked operations through regional centers will allow completion of three primary tasks: (1) examination of the strength of criminal/terrorist connections, (2) identification of suspects and mapping of networks, and (3) prediction of future behavior and better likelihood of prevention, response, and prosecution, all of which are goals of DHS IA and other IC members.[60] It will also improve the quality of intelligence analysis across DHS and participating agencies, increase overall intelligence production, promote integration of DHS intelligence, ensure the priorities of DHS within the IC, and increase analytic capabilities, which are primary DHS IA goals.

[60] DHS Staff, "Homeland Security Information Network to Expand Collaboration, Connectivity for States and Major Cities" (Washington, D.C.: Department of Homeland Security, 2004); available from http://www.dhs.gov/dhspublic/display?content=3350. [cited July 3, 2006].

THIS PAGE INTENTIONALLY LEFT BLANK

IV. THE COMPUTER NETWORK — A CENTRIC APPROACH

A. COMPUTER NETWORKS — THE BACKBONE OF SHARING

The field of terrorism research has experienced tremendous growth. As the field has benefited greatly from recent advances in information technologies, more complex and challenging new issues have emerged from numerous counter-terrorism-related research communities as well as governments of all levels. Advanced methodologies must be sought for analyzing terrorism research, terrorists, and the terrorized groups (victims). In this age of advancing technology, the computer is the backbone of national and global information sharing and is thus a networked system. Once completed, the system can become a major sharing and learning resource and tool. Information-related issues, such as the communication and sharing of research ideas among counter-terrorism researchers and the dissemination of counter-terrorism knowledge among the general public, become critical in detecting, preventing, and responding to terrorism threats. The recent advances in information technology, especially Web technology has alleviated these problems to some extent. However, more complex and challenging issues continue to emerge from terrorism-related research communities as well as local, state, and Federal governments. Terrorism threats have a wide range that spans personal, organizational, and societal levels and have far-reaching economic, psychological, political, and social consequences.[61, 62]

The first factor of information sharing and terrorism challenges is primarily associated with data collection, searching, and knowledge management. Currently, there are large and scattered volumes of terrorism-related data from a wide variety of sources available to analyze terrorist threats and system vulnerabilities.[63] Maximizing the usefulness of the data is a challenge because of (1) the lack of counter-terrorism-related databases that integrate these diverse sources; and (2) the absence of advanced as well as new methodologies to identify, model, and predict linkages among terrorists (connect the

[61] S. Cutter, ed., *Geographical Dimensions of Terrorism* (Abingdon, UK: Taylor & Francis, 2003).

[62] L.W. Kennedy and C .M. Lunn, *Developing a Foundation for Policy Relevant Terrorism Research in Criminology* (New Brunswick: Rutgers University, 2003).

[63] National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington, D.C.: Government Printing Office, 2002).

dots), their supporters, and other perpetrators. Further, information access and management are major challenges, especially in reference to identifying where to start, what to focus on, what types of data are available, where to obtain such data, who controls the data, data accuracy, if the data can be shared, and perhaps more importantly the cultural differences in the sharing attitude among the major players, e.g., the IC and LE. Thus, advanced techniques to support intelligent information searching and techniques to analyze and map terrorism knowledge domains are urgently needed.

The second factor of information sharing and terrorism challenges is mostly associated with how to trace dynamic evolution of terrorist groups and how to analyze and predict terrorist activities, associations, and threats. While the Internet has evolved into a global platform for anyone to use in disseminating, sharing, and communicating ideas, we cannot negate the fact that terrorists are also using the Internet to their own advantage. Terrorist-owned Websites and other terrorist-associated Internet content and terrorist-generated information are commonly referred to as the "Dark Web." Terrorist-generated online contents and the terrorist Internet usage patterns could be analyzed to enable better understanding and analysis of the terrorism phenomena. Unfortunately, such terrorist-generated information has seldom been used in traditional terrorism research. On the other hand, since the amount of terrorist-related information has well exceeded the capability of traditional analysis methods, applying advanced techniques such as network theory and social network analysis are required and may provide a significant added value. The final factor of information sharing and terrorism challenges involves how to successfully grant systematic access to system-level intelligence in regard to security. Thus, how to utilize various information technologies in achieving these goals remains an interesting and challenging problem.

The use of networked computers will enhance the capabilities of a truly networked IC and help eliminate the "stovepiping" that is so prevalent within the IC among the different agencies and also among LE groups. It is well known that agencies tend to stovepipe (hide) their activities, especially with respect to information under the cloak of "need-to-know." The proper network will collect and disseminate critical information that is located in many disparate data sources, especially on a national level. This will not only counter the stovepipe tendency, but will promote collaborative

information sharing. On the other hand, whoever owns the network will stovepipe automatically because it is the culture to stovepipe and not the nature to share; thus, we are fighting a human problem (see Chapter VII). However, one way to lessen this problem is to ensure access to data in the system by those who submitted it, which means regardless of security level, the generator of the information always maintains access of the data they submitted. Finally, the use of such a networked computer system will increase connectivity and provide more efficient responses to deter, detect, prevent, and respond to terrorist attacks as desired by DHS IA.[64]

Similar to the regionalization process that involved network principles, computer linkage within and across regions will also follow a network pattern and principles, as well as allow a dedicated, national network. The collected data must follow a process that will remove the great volume of extraneous information by data mining and other techniques so that the relevant information remaining is converted to usable knowledge, i.e., we must be able to separate the non-obvious to develop patterns that are recognizable. The general flow of data would follow similar to the schematic in Figure 12. Because there will be such large volumes of data, not only from input from areas within each region from the LE and IC groups, but also because of the large volumes of OSINT, several factors must be considered. These include (1) basic theory; (2) search engines, especially meta-search engines; (3) information portals; (4) information analysis; (5) social network analysis and/or network theory; (6) chatterbot techniques; (7) archiving data; (8) transmitting data; (9) data warehousing and data mining. It must also consider incorporation of data from existing fusion centers and other programs and agencies.

1. Basic Theory

First, the computer network and database(s) would need to consider or address the challenges associated with the information-collection and sharing problem. Examples would include the support of intelligence Web searching and mining of terrorism or criminal-related information, to analyze knowledge creation and information dissemination patterns, and to map terrorist domains and related, recognized patterns.

64 Allen, *Hearing of the Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee*.

Also, the network would need to examine how the Internet is used by terrorist and criminal groups for propaganda, training, and targeting and to map the dynamic evolution of these groups, or in other words to analyze and predict criminal and terrorist activities. This step would require development of and/or use of existing information portals from which to extract information through the use of meta-searchers and other search engines, keyword suggestion, document summarization, categorization, and visualization. For example, document summarization would use sentence-selection heuristics to rank text segments, which could reduce redundancy of information in a query-based summary. The summarizer would flexibly summarize Web pages by using a few sentences, and users could invoke it by choosing the number of sentences for summarization via a pull-down menu under each result.

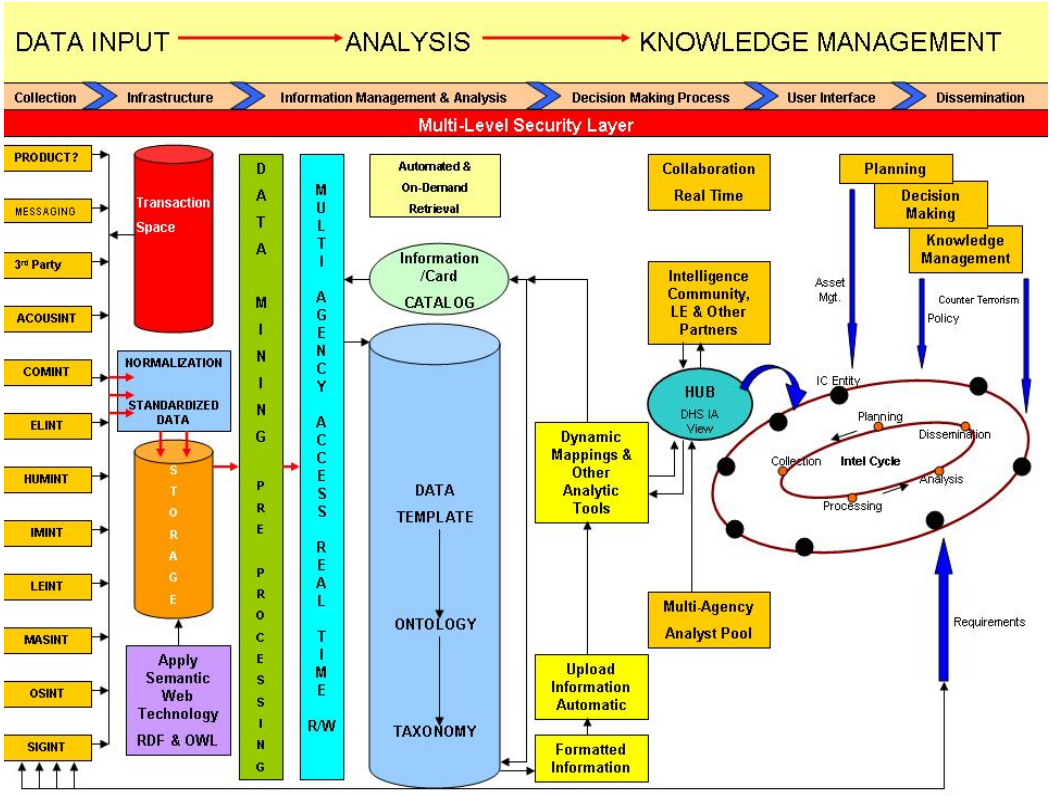


Figure 12. Proposed intelligence sharing computer network system architecture.

Second, the system would need to address knowledge representation such as Web-based user interface, domain knowledge visualization of required processes, terrorist activities and relationship visualization, and a chatting interface. Categorization

would simply place the information into a variety of folders labeled by key phrases for easier access and analysis. These phrases could be automatically based on part-of-speech tagging and linguistic rules. An indexing program could calculate the frequency of occurrence of these phrases and select the most frequently occurring phrases to index the results. Since a folder may contain more than one indexing phrase, the categorization is nonexclusive.

Third, knowledge discovery would be required in the areas of post-retrieval analysis (key words, phrases, categorization, summarization, and so forth), biometric analysis and social network analysis, script parsing, breaking encryption, and pattern matching. Finally, data collection would need to be addressed due to the overwhelming volumes of information. This could theoretically include many diverse areas such as search engines, meta-search engines, Web crawlers, Dark Web collection, multilingual domain spiders, terrorism domain knowledge, and a host of other factors. Ideally, the network would be treated as a graph in which nodes represent individuals, and links represent relations between them. Logically, these would be analyzed by node, link, group, overall structure, and dynamics. For instance, Sageman partitioned the terrorist network, Global Salafi Jihad, into four groups: Central Staff, Maghreb Arabs, Core Arabs, and Indonesians. In each group are a hub and several gatekeepers. An example of this is shown in Figure 13 — Osama bin Laden is the hub of the Central Staff cluster and issues commands to the whole network through his gatekeepers. The ability to visualize relationships is crucial. For example, Atta's group (represented left in yellow) was responsible for the 9/11 attacks; the Indonesian group (top right, green) was responsible for the Singapore Plot (2001), Bali bombings (2002), and Jarkarta bombings (2003); the Nashiri group (middle bottom, yellow) was responsible for the 1998 embassy bombings; the Maghreb Arabs (bottom right quadrant, blue) were responsible for numerous bombings including France 1995, LAX 1999, Casablanca 2003, Istanbul 2003, and others.

2. Search Engines

Many search engines are available on the Internet. Each has specific performance characteristics primarily defined by its own algorithm for indexing, ranking and visualizing Web documents. As an example, AltaVista and Google allow users to submit

queries and retrieve Web pages in a ranked order, while Yahoo! groups Web sites into categories, creating a hierarchal directory of a subset of the Internet. Internet spiders known as Web crawlers have been used as the main program in the back end of most search engines. These are programs that collect Internet pages and explore outgoing links in each page to continue the process, i.e., they build a relationship link or network as they work outward from the originating pages. An example is the World Wide Web Worm.[65] The majority of search engines, such as Google, are keyword-based. Although these engines have rapid search speeds, search results are often overwhelming and imprecise, further adding to the information overload problem. Low precision combined with low recall rates make it difficult to obtain specialized, domain-specific information from these search engines, which means little intelligence but lots of information. However, understanding the keywords of the search and the data one is seeking can increase search precision. Such a search can be accomplished by utilizing custom search software within the network architecture. This would take place in the data mining (pre-processing) step illustrated in Figure 12.

Because there is no central hub or agency in charge of all the collection and knowledge-management processes that occur within the U.S., i.e., the "Central Hub" listed in Figure 6, there can be no joint effort in fighting terrorism (it should be noted that the HUB in this instance refers to DHS IA). As an example, remove the central hub from Figure 6, where does the data then go? Removing the hub cripples the database and information retrieval, exactly as the current structure of disjointed intelligence sharing has done for the U.S. in terms of struggling against terrorism. Chief Intelligence Officer Allen specifically mentioned that the DHS and the IC must come together and the development of DNIN, along with its enabling information enterprise will provide the knowledge management system that will accelerate intelligence integration on a national scale.[66] A single hub is essential for this to happen. Further, DHS IAIP was mandated by Congress to fulfill this very role.[67]

---

[65] O. McBryan, "Genvl and WWW: Tools for Taming the Web" (paper presented at the Proceedings of the First International Conference on the World Wide Web, Geneva, Switzerland, 1994).

[66] Allen, *Hearing of the Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee* .

[67] Ibid.

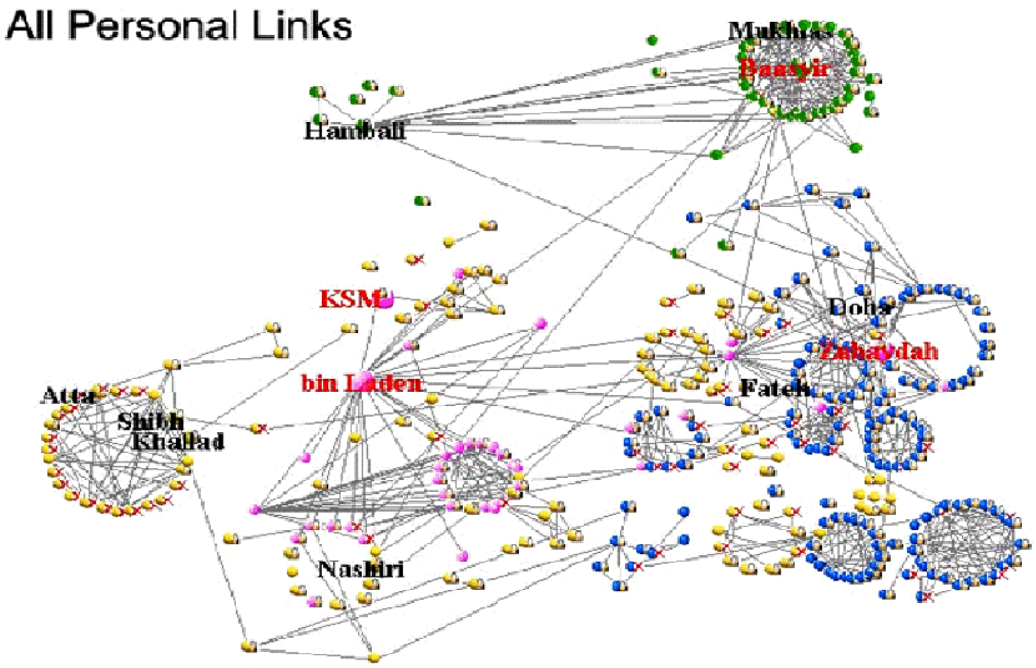


Figure 13. Example of visualized network of the Global Salafi Jihad where pink color represents core staff; yellow color represents core Arabs; green color represents Indonesian terrorists; and blue color represents Maghreb Arabs (From Sageman).[68]

Reliance solely on one search engine can cause users to miss over 77 percent of the references or OSINT they might find most relevant because no single search engine is likely to return more than 45 percent of relevant results.[69] Factually, most Internet search engines cannot keep up with the net's dynamic growth, and each search engine covers only about 16 percent of the total Web sites.[70] The emergence of meta-search engines provides a credible resolution of the aforementioned limitations by triangulating outputs from several engines to arrive at relevant results. Several server and client-based meta-search engines, such as Copernic (http://www.copernic.com) "search the search engines."[71] The results from other search engines are combined and presented to users. Copernic has now developed personal computing software such as "Copernic Agent

[68] Mark Sageman, *Understanding Al Qaeda Networks* (Cambridge, MA: Harvard University, 2005); available from www.bfrl.nist.gov/PSSIWG/presentations/Understanding_al_Qaeda_Networks.pdf. [cited May 4, 2006].

[69] E.Selberg and O.Etzioni, "Multi-Service Search and Comparison Using the Metacrawler" (paper presented at the Proceedings of the 4th International World-Wide Web Conference, Boston, 1995).

[70] S. Lawrence and C.L.Giles, "Accessibility of Information on the Web," *Nature* 400 (1999).

[71] Selberg and Etzioni, "Multi-Service Search and Comparison Using the Metacrawler."

Professional" that can be installed onto a computer and utilized for very specific searches of the Internet. Although the information returned is comprehensive, the problem of information overload worsens if no post-retrieval analysis is provided; thus, it is akin to intelligence analysis.

3. Information Portals

Web or information portal services provide another approach for retrieving information. In the field of terrorism, there are numerous portals provided by specialized research centers such as the Center for the Study of Terrorism and Political Violence (CSTPV), located at St. Andrews University in Scotland and directed by noted terrorism researcher, Professor Paul Wilkinson and formerly co-directed by Dr. Bruce Hoffman, Rand Corporation. These centers conduct terrorism research and provide portals that cater to the needs of academics, journalists, policymakers, students, and the general public. Such portals primarily provide information retrieval and dissemination services except for a few organizations such as the Terrorism Research Center (TRC), the National Memorial Institute for the Prevention of Terrorism (MIPT), that have expanded their functions to include personalization, and the Emergency Responders Knowledge Base (MIPT). For example, the TRC, founded in 1996, has the highest number of portal features including four terrorism databases, and is highly recommended with about 5,000 incoming links.[72] The most frequently identified features of these portals are information retrieval and dissemination services.

4. Information Analysis

Information portals provide access to a diversity of unstructured (e.g., reports, news stories, transcripts) and structured (database) information, but offer limited tools for integrating the resources and information fusion (including post-retrieval analysis). After a search, the user has to manually browse through the list of retrieved documents to locate relevant resources and then establish relationships among the documents. Automatic indexing algorithms have been used widely to extract key concepts from textual data. It is widely known that automatic indexing is as effective as human indexing, which is greatly improving as computer and software technology progress. Many proven techniques have been developed such as information extraction (IE), which

[72] Terrorism Research Center, "About the Terrorism Research Center," (Tampa: Terrorism Research Center, 2003).

is the use of noun phrasing to perform indexing for phrases rather than just words. These techniques are useful in extracting meaningful terms from Web and text documents for both retrieval and further analysis. Because of the large volumes of information there has been an increased interest in the use of data and Web mining and machine learning techniques that focus on identifying patterns in data. These techniques have been applied to the analysis of news articles (such as in the Message Understanding Conference or MUC), online information sources (e.g., the Columbia University's News blaster system), and high-speed data streams that are processed and mined in a Distributed Mining and Monitoring System at Cornell University.[73] New data miners are capable of processing 25,000 pages of documents per hour, and software ability is constantly improving, which means this rate will increase significantly during the next several years. Incorporation of various components into the computer network system and databases will be necessary for adequate sorting of collected information and data analysis. In addition to data mining, these include the development and integration of information fusion technologies such as biometrics and collaborative and knowledge discovery technologies that identify and display links among people, content, and topics to counter "asymmetric threats" such as those found in terrorist attacks. The computer network and database(s) associated with DNIN will support analysts in the IC and LE.

5. Social Network Analysis

Existing terrorist network research is still at its beginning stage. Although previous research has emphasized new approaches for terrorist network analysis, studies have remained mostly small-scale and have used manual analysis of a specific terrorist organization. For example, Krebs manually collected data from public news releases after the 9/11 attacks and studied the network surrounding the 19 hijackers and tracked two of them.[74] The Global Salafi Jihad network consisting of 171 members has also been analyzed using a manual approach, providing an anecdotal explanation of the formation and evolution of this network.[75] None of these studies used advanced data-mining

[73] National Science Foundation, "Data Mining and Homeland Security Applications" (Washington, D.C.: National Science Foundation, 2003); available from www.bfrl.nist.gov/PSSIWG/presentations/Understanding_al_Qaeda_Networks.pdf. [cited July 26, 2006].

[74] Krebs, *Connecting the Dots*.

[75] Sageman, *Understanding Terror Networks*.

technologies that have been applied widely in other domains, such as finance, marketing, and business, to discover previously unknown patterns of terrorist networks. Moreover, few studies have been able to systematically capture the dynamics of terrorist networks and predict terrorism trends. What is needed is a set of integrated methods, technologies, models, and tools to automatically mine data and discover valuable knowledge from terrorist networks based on large volumes of highly complex data. Only a comprehensive networked IT system and database(s) can provide such methodologies; this is the intent of DNIN.

6. Chatterbot Techniques

The premise of a natural language program, e.g., a chatterbot, is to create an intimate atmosphere where individuals can converse with the program and receive meaningful and immediate responses to queries related to a specific domain without the necessity of searching the Internet for the answers themselves. Most chatterbot techniques rely on pattern-matching algorithms that (1) take inputs from the user; (2) parses and matches the input to questions in the query or script; (3) selects the appropriate response dictated by the script; and (4) displays it to the user. Examples include ALICE, ELIZA, and Parry.[76] Chatterbots can provide users with easy access to domain-specific knowledge and also can be used to provide the necessary knowledge of global terrorism phenomena.

7. Archiving Data

Within the IT realm the verbs "backup" and "archive" mean very different things. They are frequently used to describe the same action — namely, the process of moving data from an online storage tier to near-line or off-line storage. But backing data up and archiving data are distinct technology practices that have very different requirements. They also have very different advantages. To the extent that organizations are able to embrace data archiving as a means to reduce costs, improve performance, and satisfy regulatory compliance requirements, it is a potentially important distinction.

Archiving, in general, describes the process of consolidating and moving data from a primary online storage medium—such as a fiber-channel disk array—to less-

[76] A.J. De Angeli, I. Graham, and L.Coventry, "The Unfriendly User: Exploring Social Reactions to Chatterbots" (paper presented at the Proceedings of The International Conference on Affective Human Factors Design, London, 2001).

expensive near-line or (in some cases) off-line storage medium. In some cases — compliance, for example — archiving emphasizes data longevity and authenticity, especially for e-mails, instant message transcripts, documents, and other kinds of semi-structured or unstructured data. The kinds of data that would be collected within DNIN and cooperating intelligence groups.

Data archiving improves database performance and decreases storage networking complexity. Within DNIN, the amount of data that would be collected will be enormous, and it is ironic that much of this data that users store may seldom get looked at again. Yet organizations are compelled to store data for many reasons, often legal or regulatory. Storing data drags down database performance and gobbles up valuable storage capacity, creating a major IT operational management headache. Due to the nature of current technology and legal and regulatory requirements, not to mention agency requirements, collected data must be stored where it can be readily accessed in case questions arise. In most instances databases cannot be maintained indefinitely due to storage capacity limits and thus, archiving is necessary.

Archiving is intended to let organizations cull old data from their relational databases in a way that allows it to be easily restored or reexamined if necessary. It does this by simultaneously capturing the records to be removed, along with all the database associations. It then compresses the data for storage to online disks or an automated tape library. Should the data be needed in the future, it can be quickly retrieved and restored with all the necessary associations intact.

In all cases, archiving presupposes (comparatively rapid) file-level access to data, coupled (in many cases) with robust search and retrieval capabilities. Archiving is a repository, a large index repository of data that is designed for people to get to it and be able to search it. In this respect, archiving is fundamentally different from enterprise backup, which involves taking frequent snapshots of data to protect it against both routine and catastrophic loss. Organizations typically back up operating system — or application-specific data and configuration settings, frequently directly to tape — and sometimes retain backups for only a few days, at which point they are replaced (or overwritten) by newer volumes.

Whereas archiving is typically done onsite, backup can be done both on- and off-site, with deltas sent over a WAN connection to off-site libraries. In most large organizations aged backup data is frequently managed ("vaulted") by an off-site provider. However, within DNIN this may not be desired or practical, and thus, the archiving system (not discussed here due to lack of space; contact author for additional information) for DNIN was designed to allow on-site archiving and data backup. In backup, you are copying data, whereas in archive, you are actually moving the data.

The primary purpose of archiving data within DNIN for intelligence purposes is that this technology provides file-system-level access to archive data, such that it can be exposed to third-party storage management tools or, alternately, to collaborative and other kinds of applications. This is important because archiving has more uses than just compliance. For example, intelligence personnel would be looking at large archives of rich-media data. For this reason, a robust, high-speed file system is necessary that essentially presents near-line stored data as if it were on-line data.

Why archive? Or more to the point, why archive any more than you have to; for example, for the purposes of compliance? There are several reasons. First, archived media, which can consist of inexpensive NAS devices or (more frequently) large automated tape libraries, is less expensive than tier-one Serial ATA or SCSI attached devices. Second, archiving can help boost performance. Infrequently accessed files can be moved from primary storage into near-line archival storage. Third, archived data can be stored at separate locations thereby preventing catastrophic loss of data.

Data archiving is a widespread IT operations challenge. Enterprise-wide, mission-critical databases will grow thirty-fold during this decade, according to Meta Group, a consulting firm in Stamford, CT. The traditional way to handle this growth has been through storage management. But the magnitude of growth is forcing a new look at operational data management. The next step — operational informational management — will be a prerequisite for near-continuous information availability and will require new operations and tech support tools and techniques. Thus, data archiving is essential if users are to corral growth at thirty-fold during the decade and provide repeatable performance.

Data archiving, however, is viewed first as a way of improving relational database performance by separating old data from current and active data. Storage considerations are secondary. Archiving is really a database technology, but it does allow one to use storage more efficiently, especially after one has rebuilt the database index. Rather than substantially reducing the overall need for storage capacity, however, archiving will more likely slow the growth of database storage, allowing organizations to delay database-related storage purchases.

Organizations that will gain the biggest advantage from storage archiving are those with large relational databases, particularly those that support large packaged ERP, CRM, HR, and sales-force automation applications, organizations with large amounts of unstructured data such as DNIN, as well as large transaction-processing systems. These applications have complex database structures and create extensive relationships between the various pieces of data, which is what is necessary in intelligence collection and sharing. For organizations suffering a severe storage crunch, data archiving is unlikely to provide much of a solution. Rather, it should be considered an effective way to squeeze better performance out of rapidly expanding relational databases and free up some storage, at least temporarily, in the process.

An example of newer storage mediums for archiving and data backup that DNIN would use is Blu-ray Discs (BD), which is a next-generation format meant for high-density storage of video files and data. The name Blu-ray is derived from the blue-violet laser it uses to read and write to the disc. A BD can store substantially more data than a DVD because of the shorter wavelength (405-nm) of the blue-violet laser (DVDs use 650-nm wavelength red laser and an infrared 780-nm laser). This shorter wavelength allows more information to be stored digitally in the same amount of space. For example the BD has a capacity per layer of 25 gigabytes compared to 15 megabytes for a DVD or about 200 gigabytes storage capacity per disc compared to 600 megabytes for DVDs. Thus, this newer technology will require about one-half the space of current DVDs for data archiving and backup, but are significantly less voluminous than tape and other type backup systems.

A concept little known outside of IT is that all archived data must be rewritten to new media periodically. The physical archive media degrades over time. Magnetic tape has an average life span of 2 to 3 years. The CD-ROMs and DVDs used today last about 5 to 7 years. Not enough data has been collected on the life span of Blu-ray Discs. Once the physical media starts to degrade, data becomes unreadable. A few missing bits of data in a video of a busy street corner is survivable; a few missing bits of data in a list of financial transactions can lead to missing intelligence. Regardless of the technology used for data archiving and storage, this is an important component of the DNIN sharing model and will need to be continually updated.

8. Transmitting Data

Data transmission is the conveyance of any kind of information from one space to another. Historically, this could be done by courier, smoke signals, a chain of bonfires, or semaphore and later by Morse code over copper wire. In recent computer terms, it means sending a stream of bits or bytes from one location to another by using any number of technologies, such as copper wire, optical fiber, laser, radio, infrared or even the so-called Bluetooth. Practical examples include moving data from one hard disk device to another or accessing a Website, which involves data transfer from a Web server to a user's browser.

A related concept to data-transmission is the data transmission protocol used to make the data transfer legible. Current protocols favor packet-based communication. Most computer networks today use packet-based communications. The Internet is the largest packet-based network in the world and in history.

In a packet-based network, information is broken up into packets and sent to its destination. The packets can use different paths to reach their destination. Once all the packets have arrived, they are reassembled into the original information. A packet-based network is tolerant of faults in the physical structure of the network. Data will route around the fault and arrive at the destination. This methodology works as long as there are multiply paths for the packets to take.

A concept little understood outside of IT is that there are very few paths for packets to take in the U.S. Installing underground communication wire coast to coast is a

very expensive proposition. The current bills in front of Congress to make the Internet a "tiered" network are an attempt by the telecommunications companies to recover some of their costs. The Internet is thought to be a different network than a network used by a corporation to move data to field offices. However, in both cases the same physical wire is used, and since all data is broken up into packets that can not interact with each other, the illusion of private networks is created.

All networks have choke points. A failure at the choke point brings down the network. Our current networking technology is essentially electromagnetic. Thus, while fiber optic cable uses light pluses to move data, the controlling devices for the fiber optic cable are electromagnetic. There are many ways to destroy electromagnetic devices. Examples are water, tornadoes, solar flares or something more exotic like electromagnetic pulse weapons.

Multiple redundant communication methods not based on the same technology must be developed between the regional centers, the central hub (DHS IA), and 16 member agencies of the IC. Having the data at a regional center but not being able to transmit it is still a failure. This process too has been conceptually designed but not included within the thesis because of lack of space (contact author for additional information).

9. Data Warehousing and Data Mining

Data warehouses are composed of structure and data; the data can range from highly structured to loosely structured data. Most data warehouse implementations are designed for decision making in the corporate or business environments. Business data by default is highly structured. Data are extracted from transaction-processing systems as they are generated. This creates highly structured data that fits well into a highly structured warehouse, which is the easiest type of data warehouse to build, maintain, and use in terms of computer resources and staff. The search engine for this type of data warehouse can be rather "dumb" and still report the required data. Meta-search engines and chatterbots are not needed. The data is rarely exposed to the outside world, so it can not be considered an information portal, which is what would be preferred for the LE and

IC communities. The data is stored for querying rather than analysis. Thus, this type of data warehouse fits nicely into the hierarchal monolithic structures used today by American business.

Terrorism data is not highly structured. It is loosely structured at best. A shaky eyewitness report, a newspaper article, or the cop on the street all produce loosely structured data. Forcing loosely structured data into a highly structured warehouse invariably leads to data loss because the data does not "fit" the structure. This simple fact will force a loosely structured warehouse for terrorism data. Many recent systems that have failed encountered this problem; the FBI Carnivore system is an example.

The more "loosely" a warehouse is structured, the more difficult it is to build, maintain, and use in terms of computer resources and staff. In a very loosely structured warehouse, the warehouse consists of many key components where each component retains data. Each component has its own search engine. The meta-search engine must collate the outputs from the various search engines. While the search engines can have a moderate intelligence, the meta-search engines must have a very high intelligence. Without this high intelligence there is a risk that critical data will be missed. Consequently, there is a trade-off in that using a loosely structured warehouse for terrorism data, the meta-search engine used by LE and the IC must have a higher level of intelligence. Chatterbots will use the output of the meta-search engine to converse with the human users of the warehouse. While chatterbots are useful for retrieving data from a warehouse by a human who has little experience in information retrieval, chatterbots quickly show their limitations to experienced users because current capabilities in artificial intelligence are limited. A loosely structured warehouse can be used as an information portal. An interface layer will exist between the output of the meta-search engine and the outside world. The interface layer can have a range from a simple menu to a chatterbot. Other concerns relate to politics and system security. However, politics and security concerns of exposing terrorism data to the outside world is beyond the scope of this thesis.

Further, computerized information analysis may require some up-front computer programming before any analysis can begin. Computers are very capable and fast at

pattern matching. Pattern matching finds trends in data by finding the same item in two different collections of data. As an example, facial recognition programs are based on pattern matching. While the most common pattern-matching programs that use terrorism data have already been created, there is still a need for more "exotic" ways to match data. Pattern matching is easier in a highly structured data warehouse. In a loosely structured data warehouse there will be more data to retrieve and more methods to retrieve the data.

Data mining is the process of automatically searching large volumes of data for patterns. It also can be thought of as sending the output from a meta-search engine to computerized information analysis that uses the data to refine the search parameters or returns the answer. Once again, data mining is easier in a highly structured data warehouse.

When utilizing search engines, meta-search engines, information analysis, data mining, and chatterbots, the most critical component is determining how to ask the correct question. There can be various levels of "correctness." A chatterbot needs very little correctness because the chatterbots function is to help the user create the correct question that in turn leads to the answer. A search engine needs a very correct question or the search engine returns useless information. Because the Internet is the largest loosely structured data warehouse in history, this is why, when one queries the search engine, so many useless responses are returned. One can not easily find what one needs quickly without the proper knowledge and tools.

Companies that build data warehouses like to build highly structured warehouses using highly structured data. This is the easiest type to build and maintain and returns the highest profits. In short, these companies only deal with business data. Once again, the trade-off is that terrorism data, for the most part, is loosely structured and requires a differing approach and generally an associated higher cost due to less structure.

B. THE NETWORK ANALYSIS

The network shown in Figure 13 can be developed using a variety of software that is commercially available. An example of this software is “Network Analysis,” developed by Dr. Ted Lewis and colleagues at the Naval Postgraduate School. Such

software can be coupled into the computer system architecture so that the user can both analyze and visualize the system via network analysis; it would be more representative of social network analysis in this instance. Social network analysis has proven to be a useful tool for combating terrorism and crime as early as 1991.[77] Using Figures 12 and 13 as the example, the analysis of a terrorist or criminal network would consider five factors: (1) relationships (links); (2) nodes (individuals); (3) groups; (4) network structure; and (5) the dynamics. Each of these factors would be concerned with various components. For example, link analysis would consider link type and weight distribution; this is commonly called the shortest-path algorithm. Group analysis would generally employ either a hierarchal clustering and/or a factor analysis.[78] These of course would need to be compared to determine which method generated the closest match to the actual criminal or terrorist network. Once a group has been identified, a network structure analysis should be performed to determine structure, whether it is centralized or decentralized, and the degree of hierarchy. The dynamics analysis simply adds a time factor to the system analysis to help determine the importance or role of an individual or groups within the network. The “Network Data” illustrated in Figure 14 would represent the “Storage” component in Figure 12. Designed properly, changes of the network through time could be displayed. An example design of what this system architecture may resemble is illustrated in Figure 14.

Almost any number of components could be added to each section of the analysis. For example, node analysis can summarize financial, social, demographics, or other parameters of the group or individual. Quite simply, the criminal or terrorist network is treated like a graph and analyzed according to the five factors discussed directly above. For a greater quantitative analysis, additional factors could be added. However, such factors would greatly increase the complexity of the network analysis procedure, and after all it is the network view that is sought, not a mathematical justification of the model or numbers.

---

[77] M.K. Sparrow, "Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects," *Social Networks* 13 (1991).

[78] A.K. Jain and R.C. Dubes, *Algorithms for Clustering Data* (Upper Saddle River, NJ: Prentice Hall, 1988).

This network analysis architecture allows the integration of multiple databases and can advance the technology in combating terrorism, counter-intelligence and other fields and help overcome the problems associated with both analysis and intelligence sharing. The development of this architecture will be able to demonstrate the feasibility of the larger infrastructure of DNIN at both the regional and national level.

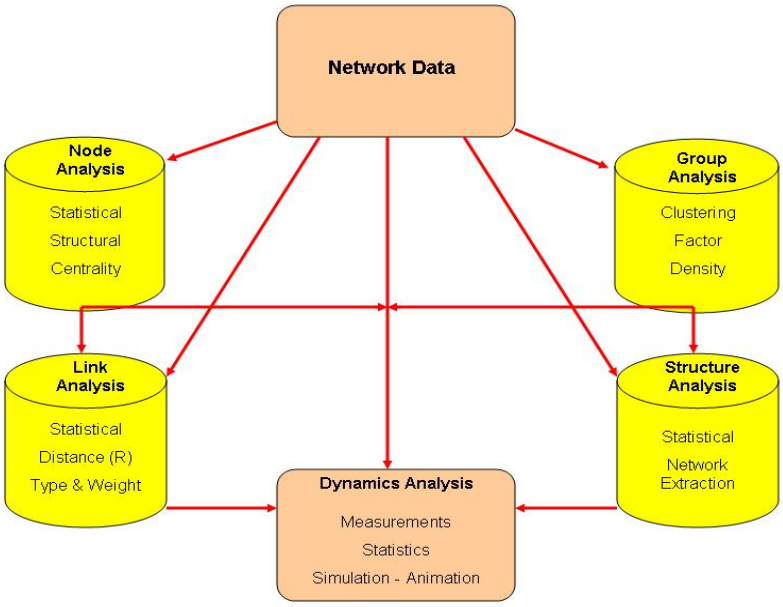


Figure 14. System Architecture for Network Analysis.

C. COUPLING NETWORK THEORY — INFORMATION SHARING EMPOWERED BY COMPUTER NETWORKS

In this age of advancing technology, the computer is the backbone of national and global information sharing and is a networked system.

Throughout the previous chapters I have discussed the operational network of DNIN through its regional and national centers, which would be staffed by personnel from a variety of agencies. Once completed, the system can become a major sharing and resource tool to fight not only terrorism, but organized crime of all kinds — the MS-13 Gang would be a good example. Sharing leads and information, counter-terrorism research and the dissemination of counter-terrorism knowledge among the LE and IC,

become critical in detecting, preventing, and responding to terrorism threats. But how are these leads shared? As with the system that has been described, the computer becomes the backbone of that sharing apparatus. For example, an analyst in Denver may share information with the regional center in New York or the National Center in Washington, D.C. This will take place over the computer network. Not only will it take place over the computer network, but the computer network will empower the individual with the tools to analyze all information collected throughout the network. Just as a network allows individuals and organizations to strategically compete with much stronger entities, so too will the computer network allow the analyst to have a greater tool and more powerful analytical processes to compete against asymmetric threats.

Ideally, just as a typical network is treated as a graph in which nodes represent individuals and links represent relations between them, the computer will be the node in a computer network and the link will be the method of connectivity of those computers. In this respect an analysis of the computer network utilizing links would consider link type and weight distribution (the shortest-path algorithm), and group analysis could be done utilizing a hierarchal clustering or a factor analysis of the regional centers. As an example, consider Figures 9 or 11, which show how DNIN is linked between the LE and IC; rather than thinking of these nodes and links as people and relationships, we can just as easily think of them as computers and electronic connections. The true beauty is that whether we discuss DNIN in terms of agencies networked together or computers, it is the computer that will empower this network and link the partnering agencies and staff. Analysts will be able to analyze and disseminate data much more rapidly.

One of the most empowering and comforting certainties of life is knowing what community one is part of, where it is located, and what its values are. Communities help define how people see themselves as individuals, and they create an extensive and complex set of relationships for anyone who chooses not to live a hermetic existence. Some of these communities are geographically related neighbors, citizens, or countrymen. Still others are joined or created by necessity, belief, interest, co-workers, religion, political parties, and teammates. In this instance the community (DNIN) is created out of the desire to defeat terrorism and keep America safe. New communities can be entered or abandoned; others remain the same throughout life. The word

"community" itself implies sameness of geographic space, of interest, or of governance. Examples include the IC and the LE communities. It also implies "sharing," either active or passive, and that is the element of community formation which is, at once, the most basic and yet most complex aspect of community building, probably because it is the most difficult to define. It is in sharing assets, ideas, and goals that the underlying sense of community, something which is common to its members, comes into play. Technology has always had an influence on individuals' and communities' ability to share, perhaps never more than it does today, at the beginning of the third millennium, when people are exposed to more information, more ideas, and more cultures than ever before. In the case of the IC and LE particularly, it is the exposure to an overwhelming volume of information that must be sorted, indexed, and analyzed in some way. As Stanley Brunn once commented, much of what we have learned about space and place at individual, community, national, and global levels has been turned "topsy-turvy." The national boundaries we have known are eroding, primarily due to new economic and supra-national communities (the EU, NAFTA, Mercosur, and ASEAN) and, concurrently with the disappearance of old states, new ones are emerging, putting new pressure on people to choose, or to identify with, a new communal identity, either at the personal, regional or national level. Terrorist organizations are a good example.

Technology, primarily telecommunications and the Internet, is making much of this possible. The Internet and other new communications technologies and applications have the potential to empower communities to form, develop, and most importantly, interact to develop shared goals and policies, allowing them to participate in arenas where, for varied reasons and to varying degrees, they have not been able to have influence. The Internet and its ability to empower communities are analogous to the empowerment of the computer for analysis of data that utilizes network theory.

In actuality, the computer network via connections to other systems, networks, agencies, and the Internet empowers information sharing and couples this process to network theory without effort, i.e., it becomes a natural phenomenon due to the network principles from which the Internet was derived. As an example, let us examine the recent death of Abu Musab al-Zarqawi, the leader of Al Qaeda in Iraq, on June 7, 2006 (yesterday at the time of this writing). There has been much postulation as to the effect

the death of al-Zarqawi would have on weakening Al Qaeda and continued attacks from the insurgency within Iraq on American forces, Iraqi nationals, and infrastructure. The author believes a brief analysis of network structure would lead to the preliminary conclusion that al-Zarqawi's death will have little effect on Al Qaeda or the number of attacks. Why? Observation of Figures 1 and 13 yield the answer. First, Al Qaeda is expert at utilizing network theory, which has given them great asymmetric strength against the U.S., Iraq, and other allies. Observation of the aforementioned figures and an understanding of network theory clearly illustrate that natural hubs exist within any group or organization, and if one connection is broken (al-Zarqawi in this case) a new hub will naturally develop. Second, networked organizations operate on much the same premise that the Internet does — that if it were attacked, a major attack in a particular location will not disable the network. Even with Osama bin Laden removed from the scene, little has changed concerning Al Qaeda's operational strength. The death of al-Zarqawi is an excellent analogy to this.

Finally, consider that al-Zarqawi may have been chosen because of his charismatic mannerisms and ruthlessness that promoted his ability to recruit for Al Qaeda. Network theory and social network analysis processes would lead one to believe that charismatic features could be replaced by other mannerisms, perhaps something as simple as a new leader that always appears masked, obscuring his identity and therefore adding mystery in place of charisma or, by no mannerisms at all. In this light, and applying the principles of network theory as in Figure 13, the death of al-Zarqawi would produce only a temporary respite in attacks and operational tactics by Al Qaeda. Thus little would change because of the strength of the network and network operational principles. Perhaps more pointedly, if we could map the current Al Qaeda organization as per Figure 13, we would be able to identify the person that will become the new leader for Al Qaeda in Iraq and take al-Zarqawi's place. *Five days after the author wrote the preceding account of al-Zarqawi, Al Qaeda in Iraq appointed a new leader (on June 12, 2006) named Abu Hamza al-Muhajer.*[79] In a human time scale, the appointment was very quick. The strength of a network and its operational principles is showing itself. As an

[79] USA Today, "Al-Qaeda in Iraq Names a New Leader," *USA Today*, June 12, 2006; available from http://www.usatoday.com/news/world/2006-06-12-zarqawi-successor_x.htm. [cited June 19, 2006].

example, in all large computer networks, dead nodes can be replaced with nodes of equal capability with no disruption to the network. Most large computer networks today are self healing. If a node goes down, the network either replaces the node automatically or the network routes around the dead node. Within such networks, critical nodes always have backups that can be made the primary in a few seconds. If the new node causes problems on a local scale, it can quickly be replaced. The dead terrorist, al-Zarqawi in this instance, was the critical node and, as was observed, had a backup who is now in charge — the backup was made the primary. In human terms, the new leader (Abu Hamza al-Muhajer) has the same capabilities. He will lead the terror attacks in Iraq, which have intensified, not diminished as U.S. forces had hoped and many terrorist experts failed to predict. Thus, like a computer network, the Al Qaeda in Iraq terrorist network is self healing. There was no disruption to the network. If the new primary causes problems on a local scale, he too will be quickly replaced.

This is the best example of how information and intelligence sharing is inextricably connected to and empowered by computer networks and how these systems follow network theory and principles, which further illustrates why it takes a network to defeat a network.

D. SUMMARY

The IT conceptual system architecture for DNIN as described in this chapter, including data archiving, storage, security, hardware, and other components, as well as fusion center and other data systems incorporation, has been conceptually designed and can be implemented (contact author for additional information). However, the architecture will not be discussed here due to space limitations and because it is beyond the scope of this thesis. Regarding the collection, dissemination, and archiving of computer-based information, several issues must be considered:

1. Cost is always a major consideration. A cheap functional system will always go farther than an expensive “pretty” system. As an example, the “Carnivore” system that was to be used by the FBI at a cost of almost

$300 million was a failure because it was an expensive system and at the time, in the FBI's defense, the technology simply was not available to make it successful.

2. The data should be stored in a format that is usable by all. Changing data formats during transmission is always fraught with problems.
3. Data security must be foremost. Who can change data, who can read data, and who can transmit data?
4. Data cleanliness and verification of data is important since there will always be inbound corruption from field and other offices.
5. Complexity of hardware and software systems becomes critical since the more complex a system is, the more difficult it is to repair. As a rule of thumb, the more complex a system, the greater the cost, the larger the required staff, and the greater the security risks.
6. The system must be redundant, easily replaceable, and easily upgradeable. Thus, commodity hardware and software should be used.

Additionally, there are many challenges in the field of terrorism that will be addressed through the networked, regional computer system of DNIN. These include:

- Information sharing related to data collection, sharing, and knowledge management.
- Information access and management.
- Tracing the dynamic evolution of terrorist groups and how to analyze and predict terrorist activities, associations, and trends.
- How to grant systematic access to system-level intelligence.
- Enhancing capabilities and reducing/eliminating stovepiping.

The computer network capabilities addresses search engines, information portals, information analysis, social network analysis and network theory, chatterbot techniques, data archiving, and data transmission. There are many different data formats in use today. Some are complex, some are confusing, some are proprietary, and some have become international standards. The international standards are usually the cheapest, the

simplest to use and maintain, the easiest to translate into different spoken languages, and are thus more reliable. An example is the Hypertext Markup Language and Extended Hypertext Markup Language (HTML/XHTML). These languages are the backbone of the World Wide Web, are full featured and easy to use, and can create output in most written languages. It would make logical sense that rather than attempt to reinvent the wheel as it were, we should attempt to design the DNIN to take advantage of these protocols. The question may also arise as to how current and future fusion centers can be incorporated into the DNIN. The DNIN will ensure compliance and standardization on a national scale, which fusion centers and other systems such as RISS and JRIES do not have. Although there are guidelines for fusion centers to follow, most are built based on stakeholder "buy in" and are thus, different in compliance standards and are not compatible with each other. As most of these may be considered legacy systems, at least current fusion centers, connecting them to the network will be a complex undertaking in regards to budget, coordination, standards, training, and restoration of the network from old to new, but it can be efficiently accomplished. Assuming each fusion center has access to the Internet the major problem with incorporation is the material within the fusion centers current database(s). Database compatibility has plagued many intelligence collection and dissemination efforts, which is why DNIN will have a compatible database that all users will access based upon security level. To incorporate a current fusion center will require that the center strips the data out of their database and send it to DNIN. This data will then become part of the larger data stream. Once the data from the center has been incorporated into the DNIN database, personnel at the center will then be able to access DNIN by connecting to any of the regional or national centers and retrieve whatever information they need and are cleared for. Security can be performed in a variety of ways. A common method is termed 3-Factor ID that incorporates biometrics such as a finger print or iris scan, passwords, and a token fob (a physical key). In lay terms this is knows as something I know, something I have, and something I am (a password, token fob, and finger print respectively). Thus, the process of incorporating a fusion center or any other location is not that difficult, nor is security. There are those who may consider such incorporation very difficult if not impossible, however, the U.S. Navy, prior to the advent of the Internet, ran a program called OSIS (Ocean Surveillance

Information System.[80] This system of intelligence collection and analysis had five to six centers that used teletypes and secure-line communications. OSIS worked exceptionally well because it had standards and followed specific compliance rules. The goal behind DNIN is to operate similarly, but with much increased technology.

[80] U.S. Navy, "Naval Intelligence Operations," in *Naval Doctrine Publication 2: Naval Intelligence* (Annapolis: U.S. Navy, 1994).

V. INTELLIGENCE ANALYSIS

A. UNDERSTANDING ANALYSIS

This section demonstrates that analysis is an integral part of DNIN. Analysis and analytic capabilities also are networked in approach, although not obvious at first glance. Analysis take place within the center section on Figure 12; it can also take place within the general intelligence cycle shown on the far right of Figure 12. As explained previously, DNIN would operate under the premise that the majority of intelligence input into the system, since it is primarily concerned with domestic intelligence, would come from the 800,000 LE officers across the U.S. Outside the field of terrorism research or the military there has generally been a lack of awareness, especially by LE, about the best method of dealing with terrorism analysis and related activities. There are several factors to be aware of that can impede progress in terrorism or criminal intelligence analysis within U.S., especially for LE. These include:

- The First and Fourth Amendments
- Freedom of Speech
- Reactive versus Proactive Policing
- Analysis before the fact, not after
- Lack of Qualified Analysts
- Integration of other Intelligence Programs[81, 82]

While this is by no means a complete list, it demonstrates obstacles to effective analysis. Generally, it has been stated that the FBI and other LE groups are reactive and are more interested in building a case for prosecution. As the criminal element changes (e.g., focus on terrorism), more patience is required and criminal and terrorist analysts must become more proactive and search for nontraditional suspects, i.e., connect the dots. For a large-scale system such as DNIN to work effectively, it is necessary that analytical

[81] Other intelligence programs would include the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), IC, RISS, JRIES, Homeland Security Operations Center (HSOC), Homeland Security Information Network (HSIN), Justice Department programs and others that are well described on the DHS Website at http://www.dhs.gov/dhspublic/display?content=3350[cited May 1, 2006].

[82] Allen, *Hearing of the Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee*.

requirements, practices, and procedures be standardized so that everyone is operating at the same level, i.e., "speaking the same language." This will require that we look at both crime analysis (who is doing what to whom) and compare it to intelligence analysis (a focus on the relationships between individuals and groups that are involved in conspiratorial activities).

To obtain a common ground, some of the axioms that should be used as guidelines for analysts have been set forth by Watanabe as follows:[83]

1. Believe in your own professional judgments.
2. Be aggressive, do not fear being wrong.
3. Avoid mirror imaging at all costs.
4. Intelligence is of no value if it is not disseminated.
5. Coordination is necessary, but do not settle for the least common denominator.
6. When everyone agrees on an issue, something is probably wrong.
7. The consumer does not care how much you know just tell him what is important.
8. Form is never more important than substance.
9. Aggressively pursue the collection of information you need.
10. Do not take the editing process too seriously.
11. Know your community counterparts and talk to them frequently (see transactive memory system discussion in Chapter VII).
12. Never let your career take precedence over your job.
13. Being an intelligence analyst is not a popularity contest.
14. Do not take your job or yourself too seriously.

In the current atmosphere of bureaucracy and budget restrictions, it is common practice to attempt to purchase the best computer systems at the lowest available price, which may meet the need of a specific agency but which also may lack compatibility with those whom you seek to share information. Because of this and due also to implementation phases, costs soar and little training is available, leaving the analyst to learn on the fly. This creates problems, especially since terrorists and criminals are

[83] F. Watanabe, "How to Succeed in the DI: Fifteen Axioms for Intelligence Analysts," *Studies in Intelligence* no. 1 (1997); available from http://www.odci.gov/csi/studies/97unclass/axioms.html.

becoming transnational and not all emanate from outside CONUS. This requires that the LE analysts understand theory, practices, culture, history, and other parameters prior to analysis. There are essentially six keys to analysis of information:

1. Seek both reported and unreported information.
2. Validate the accuracy of the information, i.e., corroborate it.
3. Know your resources, capabilities, and data.
4. Avoid one dimensionality, look at all factors: how do they relate?
5. Do not resort to extremes.
6. As an analyst, immerse yourself in the process.

Because LE numbers are so vast compared to the IC, prevention through proper and timely analysis of information is where LE can have the greatest impact. LE must look at deterrence and prevention in a proactive manner and not solely concentrate on arrest or target hardening in a reactive manner because neither of the latter addresses the factor of fear. Further, to enable a better analysis of data, LE must use taxonomy for terrorist or criminal groups and not treat each as an individual organization. For example, splitting domestic types taxonomically might yield hate groups, militia or patriot groups, white supremacy groups, tax protestors, environmental groups, and so forth. The reason behind this is that each group has differing goals, organizational structure, capabilities, and resources. Treating each the same will not yield good results from the associated databases and network architecture that was discussed in Figures 12 and 14.

1. Data Collection

Acquiring credible, reliable, and corroborative information is the key in the information collection process. The primary objective of intelligence gathering is to deal with future dangers, not punish past crimes.[84] This is especially true when dealing with terrorism, and the results obtained from the network data illustrated in Figure 14 will only be as good as the data that is input. In certain instances the information gathered by LE personnel may be more biased since a given LE entity has jurisdictional limitations. The intelligence reports will typically come from an offense or incident report, which automatically limits the information or, it may have limited value because it must be

[84] P.B. Heymann, *Terrorism and America: A Commonsense Strategy for a Democratic Society* (Cambridge: MIT Press, 1998).

reported and is, thus, reactive. This intelligence is also subjective because it is written from the responding officer's point of view; thus, as much information as possible should be collected and restrictions on that information should be exploited. The differences between a criminal and a terrorist should also be foremost on the minds of LE. Criminals do not seek to have encounters with the law but will generally not shy from them. In contrast, terrorists will expend great efforts to totally avoid LE and, thus, possible detection. Gathering information on terrorists requires analysts to think outside the box and to identify nontraditional sources of information. This factor requires proactive policing and paying particular attention to various considerations that should be recorded in great detail to obtain a more complete analysis. These would include the individual, relatives, employers, associates, phone logs or subscribers, organizations (groups or gangs), businesses, corporations, and educational background as a start. The collection of such data will aid in analysis and become greatly strengthened when shared with other agencies since they may have scraps of information that, while meaning little by itself, may allow immediate link analysis and readily demonstrate interrelationships and associations.

Because many agencies are understaffed, sharing workloads can offset the burdensome task of data collection. To alleviate this problem, the use of four working parts could be shared. These parts are group information, financial information, personnel data, and location data.[85] By splitting these among different groups or agencies, the workload for each is significantly decreased. Once the intelligence-gathering process is initiated and completed in detail, an analysis or interpretation process can begin. One analytical method for performing this task is termed the "loop effect" and is illustrated in Figure 15. Each collection effort or investigation has a starting point. Following Figure 15 from the case initiation (bottom center) in clockwise fashion, the first two steps in the loop effect are the data-collection steps. Analysts receive and categorize the information as it arrives in an attempt to prioritize according to protocol and to identify items needing immediate attention. The following steps follow in logical sequence, with the five "W's" being who, what, where, when, and why. Finally, the

[85] T. O'Connor, *Intelligence Gathering and Information* (Rocky Mount: North Carolina Wesleyan College, 2002; available from http://faculty.ncwc.edu/toconnor/392/spy/terrorism.htm. [cited May 12, 2006].

product is analyzed and disseminated and the cycle begins again. This is much like the general intelligence cycle and follows similar principles. It should therefore make it easier to transcend from reactive to proactive intelligence gathering and analysis by LE.

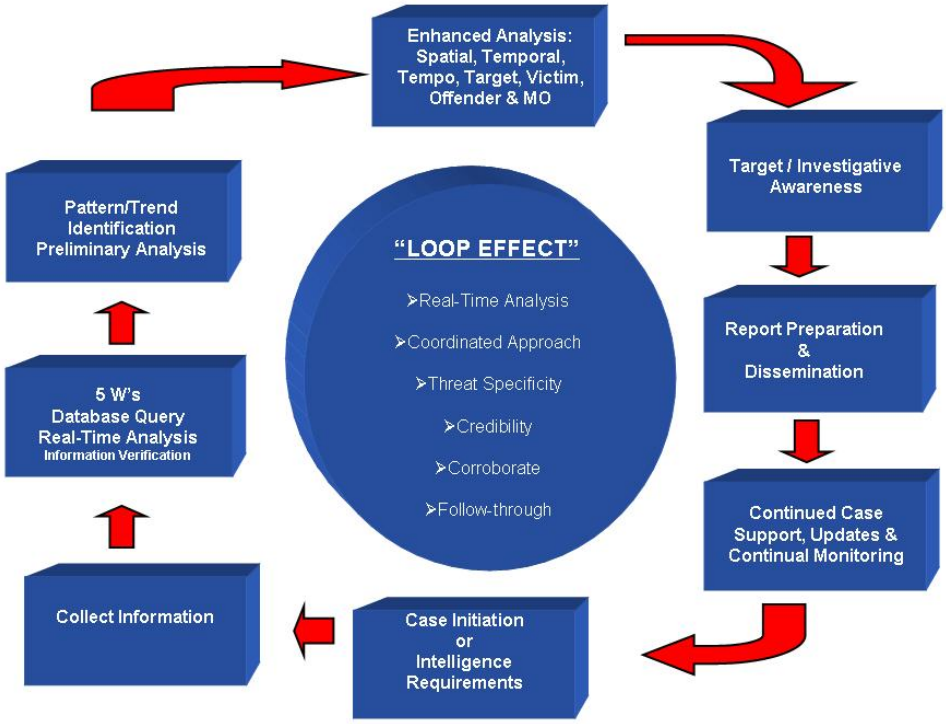


Figure 15. The "Loop Effect" (After Cooper, et al.)[86]

B. ANALYSIS — TRANSFORMING INFORMATION INTO INTELLIGENCE

Many steps are involved in the intelligence process, causing information to arrive at intermittent times, which makes organization of the information difficult. Generally, the goal is to deter or apprehend the terrorist or criminal before an attack occurs. Thus, the goal of information analysis in regard to terrorism is to anticipate the action of terrorist groups. Failure to do so could result in catastrophic consequences. And, while much has been said about the need for analysis of terrorist information, it should be

86 J. Cooper, E. Nelson, and M. Ronczkowski, "Tactical/Investigative Analysis of Targeted Crimes," in *Advanced Crime Mapping Topics* (Denver: National Law Enforcement and Corrections Technology Center, 2002).

realized that terrorists constantly learn from their predecessors. New generation terrorists analyze the mistakes made by former comrades who were captured or killed and plan their strategy accordingly. This added factor requires an even greater analytic capability among LE and the IC.

The DNIN system arms the analyst with an arsenal of databases, resources, checklists, and variables that can be used to validate inferences, probabilities, and hypotheses. Once data are consolidated, a number of analytical techniques can be performed against the data to develop a model. At the initial stage an analyst seeks to identify potential targets, relationships, associates, time lines, and other information. Each piece of information is carefully analyzed. To avoid incorrect assumptions at this phase, the results should be reevaluated against the "big picture" in order to validate them, which is particularly necessary since terrorist groups are known to have sleeper cells. After comparing against the "big picture," spatial and temporal analysis and other quantitative techniques can be applied to further refine the product. During analysis one should be careful not to focus solely on one-on-one relationships, or other associations may be missed. Consequently, analysts cannot rely upon only one method to verify information. Five of the most prevalent methods of intelligence analysis are link analysis, which is well suited to network theory, matrix Tables, timelines, event flow charts and the Heuer analysis of competing hypothesis (ACH).

1. Link Analysis Charts

Link analysis charts provide visual or graphical overviews of interrelationships and are excellent tools for long-term, complex investigation. Such analysis can be performed with a variety of standard software; Figure 13 is a good example of link analysis although it is somewhat more complex than an average investigation but is well suited to terrorist group analysis. There are two basic points to remember: (1) When connecting relationships by using lines confirmed relationships are denoted with solid lines and unconfirmed relationships are denoted with a dashed line. An arrow will indicate the direction of the relationship. (2) Groups are usually indicated by boxes, and individuals are represented by smaller circles or solid dots. Link charts can reflect individuals, infrastructure, currency, computers, or other parameters.

2. Matrix Tables

Matrix Tables are often directional and are generally used in support of a link analysis chart. These are commonly known Tables with the names of individuals generally entered alphabetically with the group name on the bottom line. As associations are uncovered, symbols for various criteria are entered into the appropriate boxes. The most commonly used symbols are circles, shaded and unfilled, plus signs, equal signs, and checkmarks. Matrix Tables are excellent analytical tools for tracking the flow of goods, weapons, money, and often drugs.

3. Event Flow Charts

These chart types are used as a visualization tool for relationships among events and are similar to time lines. The two most common methods are the Birch method and Mercer method. The Birch method uses similar rules as a link chart wherein if an event is confirmed, the box is drawn with a solid line; a dashed line is used if unconfirmed. The Mercer method places the year on the top line, the applicable months on the second line, and the years separated on the month line, using two vertical lines. An example is shown in Figure 16.

4. Heuer — Analysis of Competing Hypothesis (ACH) Assessment Method

The ACH is an eight-step process which is used to enhance judgment and minimize analytical pitfalls.[87] This eight-step process is outlined below:

1. Identify the possible hypotheses to be considered. Use a group of analysts with different perspectives to brainstorm the possibilities.
2. Make a list of significant evidence and arguments for and against each hypothesis.
3. Prepare a matrix with hypotheses across the top and evidence down the side. Analyze the “diagnosticity” of the evidence and arguments, i.e., identify the items that are most helpful in judging the relative likelihood of the hypotheses.
4. Refine the matrix. Reconsider the hypotheses and delete evidence and arguments that have no diagnostic value.
5. Draw tentative conclusions about the relative likelihood of each hypothesis. Proceed by trying to disprove the hypotheses rather than prove them.

[87] Heuer, "Psychology of Intelligence Analysis."

6. Analyze how sensitive your conclusion is to a few critical items of evidence. Consider the consequences for your analysis if that evidence is wrong, misleading, or subject to differing interpretation.

7. Report conclusions. Discuss the relative likelihood of all the hypotheses, not only the most likely ones.

8. Identify milestones for future observation that may indicate that events are taking a different course than expected.

The ACH method is fairly comprehensive and complements the "loop effect" that was discussed earlier. These methods can be used separately or together, which will greatly enhance analytical capabilities. New software such as Netmap is beginning to replace some of these methods, but there is sometimes the tendency to lose focus when using technology only so both these methods and computer applications should be used conjointly, which can be accomplished with DNIN. Both are useful when performing threat assessment and vulnerability analysis.

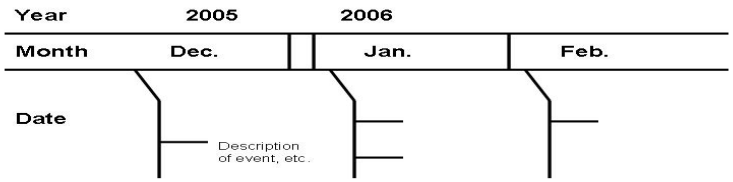


Figure 16. Mercer Method Event Chart.

C. PREDICTIVE TECHNIQUES

True intelligence analysis is always predictive. A single event can shape the future of a field of study, direction of research, or outcome of a problem. The goal is to be able to predict this event or scenario. For example, during the early age of computers, IBM approached Gary Kildall, President of Digital Research Intergalactic, to run

software on IBM's personal computers. On the date they were supposed to meet, Kildall decided to go flying in his new personal airplane. The meeting did not take place and IBM approached Bill Gates, head of Microsoft instead, Gates developed the DOS operating system for personal computers and thus changed/shaped the future of the computer industry. Another example is Henri Darcy who discovered how fluid flows through geologic media in his famous experiment in France in which he passed water through large cylinders of sand. He was able to accurately describe fluid flow in the vertical direction, but because the flow was confined in cylinders there was no outward movement and he failed to anticipate it. Thus, for transport in soils of hazardous materials, such as radioactive waste, the Darcy model could not accurately predict flow because the confined nature of Darcy's experiment failed to account for outward flux (divergence). L.A. Richards, a graduate student at Iowa State University, developed an equation called the Richard's equation that predicted this and changed the history of this field of science. It is this equation that developed the groundwork for storage of radioactive waste by the Department of Energy (DOE) at the Yucca Mountain Site in Nevada. Both of these events were the actions of individuals, and they were not truly predictable. However, the principles of causation should apply well to convergent phenomena, and prediction should be possible through proper analysis. The objective is to observe long-established patterns that have been used in science and organizational planning so that we are able to describe the past and present state of a target and make a qualified prediction about the future. Network theory, the operational principal of DNIN, is particularly applicable to this process.

An example is the Kalman Filter, which is a method of combining data to estimate an entity's current state and evaluating the forces acting on the entity to predict its future state.[88] The Kalman Filter methodology uses three predictive mechanisms: (1) extrapolation, (2) projection, and (3) forecasting. Each follows the approach of assessing forces that act on the entity. Essentially, an extrapolation assumes no change between present and future states; a projection assumes there is a change between these states, and

[88] James A Tindall, "Deconvolution of Plant Type(S) for Homeland Security Enforcement Using Remote Sensing on a UAV Collection Platform," *Homeland Security Affairs* II, no. 1 (2006).

a forecast assumes both change and an addition of new forces. The basic steps of the Kalman Filter method are as follows:

1. Estimate one past state and the present, i.e. a model. For example, a model of a terrorist organization.
2. Determine what forces acted on the entity to bring it to the present state.
3. Make a projection — estimate the changes in existing forces that are likely to occur.
4. Make a forecast — begin with the projection and identify new forces that may act on the entity then incorporate their effect.
5. Determine the likely future state of the entity based on an assessment of these forces.

Further, the Kalman Filter can be applied on a dual process for both analyzing intelligence and for identification of various parameters such as from surveillance and reconnaissance of the U.S. Mexico border or other targets, which is a major issue before DHS and congress.[89, 90]

In actuality a link analysis can be performed to develop the answers to these steps, but that is beyond the scope of this thesis. However, it demonstrates the necessity of analysis in the networked approach to intelligence sharing being discussed. A qualitative force analysis is the simplest approach to projection and forecasting, i.e., it is easiest to perform simply by answering the following questions:

1. What forces (technology, organizational structure, etc.) have affected the entity during the last several years (Al Qaeda would be a good entity to practice on)?
2. Which five or six forces have more impact than others?
3. What forces are expected to affect Al Qaeda over the next several years?
4. Which five or six forces are likely to have more impact than the others?
5. What are the main differences between questions 2 and 4?
6. What is implied by these differences for Al Qaeda?

---

89 Tindall, *Deconvolution of Plant Type(S) for Homeland Security Enforcement*.

90 Strohm, "Border Intelligence Plan Still in 'Early Stages,' Official Says."

Continuing with the example of Al Qaeda as a target for analysis, it is important to investigate the past and present state, determine a likely transition path from present to future, and determine the expected future state of Al Qaeda or another terrorist group such as Hezbollah. Center this process on Al Qaeda, i.e., the target. In this way it is target centric, and the actions of one organization will affect decisions of an opposing organization in terms of analysis, i.e., either by an LE or IC group. Thus, sharing becomes critical and is pulled into DNIN not only at the geographic and computer centric components, but the analysis phase as well, and will lead to a much better or likely actionable intelligence product. Further, an excellent method to use this approach with is to develop a scenario of a future Al Qaeda model, which would highlight large forces that shaped this future. It must be remembered that intelligence analysis must be predictive to be useful.

Digressing to the Kalman Filter method, extrapolation is one of the easiest mechanisms to perform, and the most conservative. Extrapolation extends a linear curve on a graph based on historical performance. An example would be a plot of the price per gallon of gasoline since the early 1960s. Continuing the plot into the future, what would the price be? Be aware that an extrapolation does not account for a change in forces that act on the price of gasoline. Therefore, extrapolation is usually accurate for the short term, assuming an accurate starting point and an understanding of the direction of movement. It is inaccurate for the long term because of narrow focus and because it negates dynamic forces, i.e., everything remains constant and does not change with time. Also, if the initial starting point for the extrapolation was inaccurate, the model it yields will also be inaccurate.

Projection is more reliable than extrapolation because it predicts a range of the future or likely future because projection assumes that past forces will change with time. There is a range of possible outcomes, and all should be carefully considered, i.e., analyzed. As an example, in the GWOT one could assume that the U.S. and its partners win, Al Qaeda wins, or there is a stalemate. What forces will act to influence who wins and why? Do any of the influencing events sway each other? Is it possible to assess the outcome of particular events directly, or is there a domino effect between events upon which the outcome depends? A particularly nice way to look at this is by using an

influence tree, which surprisingly follows fault-tree analysis that is used in network theory. Without illustrating the process or mathematical components, the influence tree approach to evaluation of possible outcomes is more convincing to customers than an unsupported analytic judgment about the prospects for who wins. Other processes that can be included are influence net models, correlation and regression, probability estimates (these can become fairly quantitative and deal with point and interval estimation and the use of Monte Carlo simulation), and sensitivity analysis. Even if a formal probability estimate is used or similar mechanisms, they generally have a strong subjective element that should be avoided if possible. Utilization of the influence tree and, therefore, network analysis principles will help avoid this subjectivity.

Projections based on forecasting usually work better than extrapolations for the long term. Generally, this is because new developments with time, which could not be foreseen by experts, have a disruptive effect on the outcome of the analysis; thus, forecasting can take these into account. A major objective of forecasting in intelligence is to define alternative futures of the target, Al Qaeda in this example, and not just the most likely future. The alternative futures are generally scenarios as discussed previously. Forecasting will provide the highest possible level of prediction to customers and will generally gain their confidence. As with network theory, a forecasting methodology requires analytic tools and principles and analysts who have a significant understanding of many technologies and disciplines — they must have the ability to think about issues in a nonlinear fashion. Why? Because forecasting is highly nonlinear; that is why it is generally better than extrapolation. Multidisciplinary individuals can pull together concepts from several technical fields and assess political, economic, technical, and social factors that influence the target. This breadth of understanding is recognition of the similarities of the principles from these fields and the underlying forces that make them work. However, forecasting is not an exact science; it is also based on a number of assumptions: (1) the future cannot be predicted only forecast; (2) forecasts will be misleading if they do not consider future developments in such areas as culture, technology, economics, institutional change and so forth; and (3) the most likely or alternative futures of the target are defined by human factors that include judgment, creativity, and imagination and are thus somewhat subjective. Further, forecasts are

judged on clarity, plausibility, credibility, relevance, urgency, advantage, and technical quality, which serve as filters for the information analytical process. If a given scenario cannot pass through these filters, it is rejected.

The use of DNIN on a national level, in which more relevant information can be garnered, will improve the intelligence analytical process because both are related to network theory and have a direct influence or domino effect on each other.

D. SHAPING FORCES AND ORGANIZATION ANALYSIS

Shaping forces and the analytical techniques that focus on the force and how it pertains to organizational structures are many. Generally, forces include economic, political, social, environmental, military, cultural, and religious. Each becomes important in its own right but is generally influenced by one or more of the other forces. For example, the U.S. IC settled on its basic organizational structure and decision-making process in the late 1940s and 1950s and patterned them after the dominant technology and business models of that era. The IC also followed the traditional hierarchal model of the military, and now, after more than 50 years, the IC and other intelligence groups find themselves in a radically different world that has been changed by technology and in which a horizontal networked environment proves more effective, logical, and efficient. However, the IC has remained at rest because of opposition to change and is thus a shaping force, one of the factors that helped cause intelligence failures leading to 9/11. Though most organizations resist change to a point, it is necessary at some place in time to begin shaping with the forces or become obsolete. That time has arrived within the IC, and it is now time to make the choice to remain in the organizational structure of the past or to move forward. John Arquilla and David Ronfeldt of RAND Corporation argued that, "Future conflicts will be fought more by networks than by hierarchies, and whoever masters the network form will gain major advantages." Networks and networking are two of the major shaping forces that are moving us toward change. If we resist this change, the U.S. and its partners will lose the GWOT. Thus, the goal would be to follow Newton's third law such that for a given amount of effort we can effect a small change in a larger system; the IC in this instance.

As there are shaping forces, so too there are counter forces, but not necessarily of the same nature. For example, a wise organization is not likely to play to its opponent's strengths but to its weaknesses. Al Qaeda is an excellent example in which they focus asymmetric attacks that are both unconventional and highly lethal. These same asymmetric counter forces exist in organizations and industries since they attempt to achieve cost asymmetry through defensive tactics that have a favorable cost differential between them and the adversarial organization. The reaction can be nothing short of asymmetrical. Even the U.S. military is using such countervailing forces in Afghanistan and Iraq because they realize that large-force measures of battalions that worked before no longer work well against an insurgency using asymmetric tactics. To involve shaping forces processes requires the investigation of contamination, synergy, strength, weakness, time delay, and a feedback process. However, this is a networked process, and governments and large organizations such as the IC have a disadvantage in this intervention because they observe one facet at any point in time, generally using a simplistic approach. The networked world we now live in is both dynamic and complex; remaining in such a functional state and disregarding the shaping forces that will steer an organization in a certain direction will result in catastrophe. This results because of slower feedback processes and a more cumbersome structure. The networked approach to regions and analysis will tend toward agility and, thus, a rapid reaction for planning, prevention and response.

1. Organizational Analysis

There are many ways to analyze an organization's structure, but there are three primary ways: (1) examine the size and capabilities; (2) assess the effectiveness of the structure; and (3) analyze the relationships among groups in the organizational hierarchy. Network theory is thus, particularly applicable. This is because of the ability of network theory to assess structural effectiveness. In effect, an organizational analysis is a network analysis that analyzes organizational structure because the latter does not sufficiently distinguish between members (nodes) and their relationships (links). When applied to the organization, this is generally referred to as social network analysis. There are distinct advantages. First, an analyst may be interested in comparing the network of trade in agricultural products to the network of trade in chemical manufacturing. A computer can

do this in a few minutes, and it may show relationships between chemicals that could be used for bioterror against agricultural production or display a similar network. Second, the formal methods for representing network data utilizing graphs and mathematics can suggest parameters that we may look for in the data that may not have occurred to us if we presented our data using verbal descriptions. Additionally, the node of most importance in the network can be identified, which can be a person, place, relationship, or other parameter. The analysis may also be able to yield why this node is most important.

Another organizational analysis concept is that of equivalence. For example, what if an individual such as Osama bin Laden were removed from the Al Qaeda network? The result would be dependent on bin Laden's centrality or uniqueness to Al Qaeda. Would he be missed or would someone else easily assume his leadership role, i.e., would he have an equivalent? In network terminology bin Laden would either have substitutability, stochastic equivalence, or role equivalence. That is, bin Laden could be interchanged with another individual if there is an identical relationship of some form. The stochastic equivalence, though more sophisticated, would apply if the probabilities of another individual linked to the network through any particular node were the same. Role equivalence implies that two individual play the same role in different organizations, even if they have no common acquaintances. Thus, what if bin Laden were captured or killed? Would equivalence make a difference in Al Qaeda in continuing the GWOT, or would some other group(s) take up the slack?

When analyzing a group or organization through network methodology, the analyst must be aware of the five principal types of networks:

1. Vertical – organized across a value chain.
2. Technology – alliances that allow maintaining technical superiority.
3. Development – an alliance focused on developing new products or processes.
4. Ownership – a dominant firm owns part or all of its suppliers. The DoD and specific members of the IC are a good example.
5. Political – focused on political or regulatory gains for members.

Variations of these principal network types are possible. For example, it is well known that religious and cultural ties in the Middle East can be the basis for a type of hybrid terrorist network, which is a form of radicalization.[91] This is why analytic capabilities are important from a network perspective. Another important issue is technology analysis within the network viewpoint, but this issue will not be discussed here.

E. SUMMARY

Intelligence analysis is a key factor of the DNIN system, which will address the following components in intelligence collection and analysis:

- The six keys to analysis of information — the computer system and relational databases can look at multi-dimensionality that will enhance analysis.
- Prevention through proper and timely analysis where LE can have the greatest impact, particularly in the area of civil liberties since LE conforms legally to this process. The DNIN will greatly assist in this role.
- Sharing workloads to reduce burdensome tasks of data collection.
- Expediting analysis — the DNIN system arms the analyst with an arsenal of databases, resources, and check lists to validate inferences, probabilities, and hypotheses.
- DNIN would utilize five of the most prevalent methods of intelligence analysis, which are well suited to network theory — link analysis, matrix Tables, timelines, event flow, and Heuer ACH. DNIN also has the capability to absorb others.
- Pooled intelligence within DNIN through proper analysis is likely to lead to more actionable intelligence.

[91] Allen, *Hearing of the Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee*.

- Shaping forces of networks will force change on the IC and LE groups. Resisting this change rather than embracing it will mean losing the GWOT. Counter forces such as asymmetric warfare can also be dealt with by using defensive tactics with a favorable cost differential.

The DNIN approach will tend toward agility by focusing on organizational analysis through examining size and capabilities, assessing effectiveness and structure, and analyzing the relationship(s) among groups in the organizational hierarchy. Agility is necessary if we are to counter unconventional enemies.

Another aspect critically important to intelligence analysis and sharing and why DNIN becomes so important is the loss of institutional knowledge that is beginning to befall the IC and that will increase during the next few years. This knowledge loss is due to the high retirement rates of well trained and skilled analysts — about 45 to 60 percent by 2011.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. OVERCOMING INTELLIGENCE-SHARING POLICY ISSUES

A. THE INTERAGENCY CONUNDRUM — CONTROVERSY OF INTELLIGENCE COLLECTION AND SHARING WITHIN CONUS

The real key to information sharing is to manage knowledge, not information because there is too much information, but not enough knowledge. After all, would not knowledge be actionable information? This statement is analogous to "all intelligence is information, but not all information is intelligence."[92] Therefore, knowledge management and not information is the key to effective intelligence sharing.

Throughout the manufacturing boom in the U.S., teams of personnel in factories and businesses worked together to complete tasks. As times have changed and technology has advanced, the information- and knowledge-based enterprises of today require greater levels of sharing and a more intimate, higher level of interpersonal skills among personnel. Ensuring the free flow of information within an organization and across a multi-agency culture requires not only a personnel adaptation, but a technological adaptation as well. The technical abilities are present to share information throughout agencies, but one must ask if an agency official needs access or should be perusing "military-order-of-battle information" in his or her search for intelligence. Obviously, the answer would be no; thus, as the geographic regions for intelligence sharing evolve, there should also be a common computer or virtual collaboration space set up into which all agencies and groups involved in intelligence sharing can place data and from which data can be extracted. Naturally, the DHS IA would be the logical place for this system to be established. In this manner, the need-to-know would be replaced with need-to-share that was highlighted in the 9/11 Commission Reports. After all, within the IC, it is the method and source of the intelligence that is most important. These would never need to be shared with other agencies unless directed by authority to do so. For the general intelligence officer, analyst, or LE personnel, the only desire is the information that may be pertinent to them, e.g., are we going to be attacked, what is the likely method, and when. These personnel do not care about how or where the

[92] Loch K. Johnson and James J. Wirtz, *Strategic Intelligence: Windows into a Secret World: An Anthology* (Los Angeles: Roxbury Publishing Group, 2004).

information was obtained. As early as 2002, perhaps sooner, information clearing houses have been discussed. One in particular, called the Intelligence Community System for Information Sharing (ICSIS) was discussed if the DHS agency was actually created.[93] The proposed system would provide controlled interfaces that will allow the IC to automate the process of stripping out from classified documents top-secret sources and methods of intelligence collection, as well as automating the sharing of that intelligence with analysts and officials with "secret" or lower security clearances. Such a system, to work properly in a network-strengthened IC would need to have an access point at each of the regional intelligence-sharing centers depicted in Figure 2. This system is also similar to the Regional Information Sharing System Network used by state and local criminal intelligence groups.[94]

B. REGIONAL STRUCTURES WITHIN AGENCIES

Most U.S Government agencies operate on a regional basis, e.g., they have offices within various regions within CONUS under which a varied number of states operate. This enables that agency to more easily coordinate Federal operations outside of Washington, D.C., on a reduced scale, synchronizes programs, enhances management flow, and otherwise helps the government keep abreast of agency issues within CONUS. This regionalized structure is just as important as interagency coordination and cooperation. The difficult part of regionalization is that each agency, including components of the U.S. military, has not only different regions, but different-sized regions, some of which may cross borders within a state rather state boundary lines. These structures may make sense to the specific agency, but the disparity among regions significantly inhibits interagency coordination so that any advantages gained by specific agencies from their unique structure are offset by the great disadvantage to coordinating and unifying the broader national interagency effort.[95]

---

[93] Dan Verton, "U.S. Intelligence Community Faces Info-Sharing Overhaul," *Computerworld*, 2002; available from http://www.computerworld.com/securitytopics/security/0,10801,74053,00.html. [cited March 20 2006].

[94] Ibid., 3.

[95] Bunil B. Desai, "Solving the Interagency Puzzle," *Policy Review* 1 (2005).

For greater effectiveness, it is now time for the IC and those related with it to convert to a unified regional structure just as the military did when they adopted a "unified command plan" in 1946 after WWII. This new regionalized structure should follow the same pattern as the military (one command per region, joint command headquarters composed of personnel from each agency involved, and final authority for the director/commander of the regional headquarters). The uniqueness of having personnel staff the regional office from all over the region is that all agencies would represent themselves, but that a culture of sharing would be developed through that new group, as has been explained previously. Further, the agency or group owning DNIN would be in closer contact with stakeholders of each region and if a stakeholder such as the U.S. Coast Guard wanted to make one contact call to convey information, the process would be greatly simplified. For the most effective planning and conduct of policy of operations, it is imperative that each region have clear lines of authority and geographic boundaries if possible. The latter is no different that an LE officer going out of his or her jurisdiction. Once he or she realizes they are about to do so, they can quickly pass the baton to an LE colleague who does have the authority so that they have, in effect, carried out a joint operation. Therefore, it is easily observable that aligning a variety of regional structures into a single regional structure would foster a unity of effort. Desai points out that, had the DoD, State Department, CIA, and other agencies had a single interagency regional structure in 1994, the genocide in Rwanda could have been prevented.[96] In about 100 days, an estimated 800,000 people, mostly Tutsis, were murdered.[97] This was a high price to pay for lack of drawing a few lines of regionalization in the sand. Not only did lack of unified regionalization cause a lack of operational functionality, it significantly, in this case, decreased world opinion of the United States. In regard of Homeland Security, it may be necessary to create sub regions for various agencies for congruity. If there is to be a national policy against terrorism, how can it be effectively conducted given the difference in regional structures between all the varied agencies? Unifying the DNIN regional structure, as proposed in Figure 4, would enhance unity of effort at the state and regional levels and, more importantly, the national level. The need

[96] Desai, "Solving the Interagency Puzzle."

[97] Available from http://en.wikipedia.org/wiki/Rwandan_Genocide. [cited May 1, 2006].

derives from the necessity to "connect the dots" from multiple individuals and locations within and without CONUS. There must be a regionalized network that fights for the U.S. against terrorism, not a disparate network that succeeds only in creating complex sharing issues. The state fusion centers may fit into this latter group that, although having clear goals, are not yet linked on a national or regional basis in most instances and therefore, lack the sharing capacity desired by DHS.[98] Ultimately, people and ideas will matter most for consensus.

C. INTEGRATED OPERATIONS — INTELLIGENCE AUTHORITY AND OVERSIGHT — STEPS FOR MAKING INTELLIGENCE SHARING WORK

Intelligence sharing within CONUS is plagued with discontinuity, turf wars, poor cooperation, and other factors. Essential steps that must be taken to improve intelligence and information sharing are:

- Implementation of a mutual operations doctrine.
- Relinquishing control for the sharing process to a single authority.
- Development of a regional structure.
- Developing personnel policies that will foster cooperation.

There are 16 primary intelligence agencies in the U.S. IC. Despite the fact that the entire IC (www.intelligence.gov) depicts cohesiveness, cooperation among IC members is less than desired, which was highlighted in the 9/11 Commission Report; a systemic problem was widely acknowledged. Compounding this problem are other diverse elements within intelligence including: economic, diplomatic, corporate, and law enforcement (LE). This volatile mix creates an interagency conundrum (riddle), about the best method to share intelligence. While it can be argued that sharing intelligence relates to policy and civil liberties issues, the real reasons can be condensed to authority and oversight agencies and cultures. To focus on one individual agency as the root problem is a mistake.

---

[98] Allen, *Hearing of the Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee*.

Due to blame levied on the FBI as a result of 9/11, it has been attempting to transform itself into an agency that can prevent terrorist acts rather than react to them as crimes. In late 2004 the FBI reorganized part of its agency creating a National Security Branch (NSB) under direction of the Deputy Director. Within the NSD is the Directorate of Intelligence. The purpose of this reorganization, i.e., the creation of the Directorate of Intelligence, was to drive and coordinate intelligence work across the FBI and the U.S. IC, build a cadre of well-qualified analysts, establish a dedicated intelligence element in every FBI field office, and increase intelligence production and the development of counter-terrorism sources. Many feel this reorganization is just reshuffling and that the FBI remains ineffective in capturing terrorists, especially since only one person was prosecuted involving the 9/11 attacks. Despite spending millions on reorganization of the FBI little has changed, they remain as ineffective at sharing intelligence as before, which is supposed to be the lead DI agency's role. An elitist prevailing attitude denies those in other agencies who have great ideas from expressing them and contributing to the problem. It is the authors and others opinion that the currently operated state fusion centers are following along this same path although there is more promise of sharing among LE groups. This also fosters the premise of the need-to-know versus need-to-share. If one is outside the agency, there exists less likelihood of a personal relationship and therefore, no sharing. The conundrum between culture and sharing is therefore manifest.

Agency cultures are characterized by different goals, policies, varied sets of values and other characteristics such as decision-making methods, leadership style, and communication policies, all of which contribute to problematic cooperation and integrated operations. Can differing cultures and separate agencies cooperate, coordinate, and be successful in accomplishing specific tasks and goals? Yes. A good example is the U.S. military. Despite differing cultures, in times of crises they are able to coordinate complex tasks to achieve mission goals and objectives. Desert Storm is a good example, which involved not only U.S. troops, but troops from various countries as well. This cooperative/joint attitude is exactly what we need in fighting the Global War on Terror (GWOT).

It is unlikely that marginalizing individual agency cultures would be successful in intelligence sharing. Instead, a strong interagency culture should provide the foundational basis for cooperation. There are four factors that encumber a shift from an agency to an interagency culture and from adequately sharing intelligence. These include a lack of doctrine, lack of a single authority (who's in charge), a regional structure that would allow for more timely and efficient sharing of data, and people policies, i.e., personnel who really do the job. This will be further explained in Chapter V.

1. Mutual Operations Doctrine

The Goldwater-Nichols Reorganization Act of 1986 (GNRA) mandated development of policies and doctrines for coordination between branches of the military; it became known as the "joint doctrine" and has become very successful. Operation Desert Storm was considered a work of art in military circles, so great were the cooperation, collaboration, and effectiveness, which included joint international forces operating under a single authority. Clearly, joint doctrine serves as a good example for development of a similar national doctrine/policy for HS and intelligence sharing among agencies. Such a doctrine must be flexible enough to evolve and change in regard to technological advances and strategic concepts, but should not change based on personal preferences due to political office rotations or individual agency culture. This implies that a networking approach such as DNIN would be preferred.

A number of Presidential Directives (PDD) has attempted to improve failures in interagency cooperation, specifically PDD 25 and PDD 56, which discuss managing peace-keeping forces and complex incident operations. Any interagency mutual doctrine should emphasize all elements of national power (LE, the IC in general, and economics) and recognize all parties (military, LE and others) to prevent diminished capabilities and promote unity. A mutual interagency doctrine must also avoid dominance by an individual agency — examples would be the FBI and CIA who dominate domestic and international intelligence and exemplify the lack of mutual trust and sharing. An example is the FBI Joint Terrorism Task Force (JTTF) that is virtually owned by the FBI although many other agencies and groups contribute to the process. The single agency control of this sharing entity undermines its effectiveness. Finally, a mutual interagency doctrine

should attempt a vertical integration of intelligence from the local LE level up through the national level to include the international arena, since most threats may likely be initiated abroad.

2. Single Authority

A single authority is more respected than multiple heads, less confusing, and usually has better grasp of doctrinal development and responsibility. The creation of DHS was a good step, bringing 22 agencies under its auspices; if managed properly, this will enhance coordination of each agency's role and its effect on HS. Prior to establishment of DHS, the President and Congress established the Homeland Security Council (HSC). Then, in September 2003 and March 2004, an "all hazards" Initial Response Plan and National Incident Management System (NIMS) plan was published. Both of these plans attempted to improve interagency coordination, but there remains a dilemma, of which hurricane Katrina was an example. The National Security Act of 1947 established the National Security Council (NSC) with authority for coordinating interagency efforts, but not interagency doctrine; its role is to manage the process. The NSC is not independent of the process, but involved in it, which creates significant problems. Only the HSC has influence over interagency coordination through the HSPDI and Homeland Security Act of 2002. With the development of the DHS IA we have, for all intents and purposes, a domestic intelligence (DI) agency, the new IA, established initially as the IAIP after 9/11 to enhance intelligence collection and sharing among LE groups and the IC agencies in CONUS. The Homeland Security Act of 2002 established IAIP within the DHS to provide intelligence integration and to merge into one organization the capability to identify and assess future terrorist threats. Immediately after the IAIP was established, President Bush (January 28, 2003, State of the Union) created the Terrorist Threat Integration Center (TTIC) as a single source of collection and analysis of all terrorism intelligence, which has evolved into the National Counter-terrorism Center (NCTC).[99] Within months, the terrorist screening center (TSC) that disseminates terrorist watch list information, was formed; managed by the Director of the FBI, TSC also works with NCTC. The TSC and NCTC are located in a joint facility; tragically, the IAIP, despite Congressional mandate to carry out its intelligence duties, is not located with these groups. After four years, the IAIP

[99]John Scott Redd, "Statement to the United States Senate" (Washington, D.C.: Government Printing Office, 2005).

(Information Analysis and Infrastructure Protection) has been separated and IA has become the Office of Intelligence Analysis within DHS, which has appointed a Chief Intelligence Officer, Mr. Charles Allen, reporting directly to Secretary Chertoff.[100] Allen is responsible for coordinating with the domestic Intelligence Community and providing guidance on HS specific issues. A specific agency needs to be named to promote information sharing and dissemination of DI throughout all levels of government as well as budgetary oversight. Could DHS IA assume this new this role? While it may not be the perfect choice, a single collection hub, i.e., single authority, is necessary if we are to achieve effective intelligence sharing. Also, that hub likely should not be an LE agency but an intelligence agency since they, in the opinion of many, are better trained to collect and analyze intelligence information. Thus, if not DHS IA, what agency/organization could pull mutual doctrine together?

3. Regional Structure

Due to the scope and scale of intelligence collection within the U.S., discussion of a regional structure is important. Whether or not information is collected within a regional framework (especially when involving LE), will determine the overall effectiveness of intelligence-sharing goals. Adequate intelligence sharing within the U.S. will require the incorporation of the 800,000 police officers representing 18,000 agencies and 27,000 FBI agents, only 11,400 of whom are in CONUS, as well as many other personnel from various agencies and the IC. Due to scale and scope, a national program will not work without regionalization of the process, i.e., regional centers. While JRIES and RISS operate on a regional basis, these programs are narrowly focused and utilize a piecemeal approach, i.e., they are not national in scope nor do they have the network strength for the regional operations to become a dedicated national network. Further, their IT components are not compatible with other groups or fusion centers. As another example and in contrast, MI5 works with only 56 agencies utilizing about 2,000 personnel and, while it is effective, the land area of the UK is about 245,000 sq km (about the size of Oregon) compared to 9 M sq km for the U.S, i.e., 37 times greater. Thus, the UK would be more comparable to a region within the U.S. such as that served by JRIES, RISS, or HSIN. There are simply too many agencies and personnel involved within the

[100] DHS Staff, "Press Room: Biographies," Department of Homeland Security, 2005; available from http://www.dhs.gov/dhspublic/display?theme=84&content=4935. [cited February 4, 2006].

U.S. not to regionalize. The military model — one command for each region under the authority of the regional commander who may be from any branch of service — is effective. Thus, within DNIN the regional director could be DHS, FBI, or from another agency as appropriate. Aligning all regional structures into a single regional structure would promote efficiency and enable better planning and performance of operations, intelligence would be from a similar reference base, would facilitate interregional cooperation among the various participants, would work better from a national incident response framework, and would reduce the management load on a national scale by reducing the number of individuals through appointment of regional leaders who would have the necessary link to the national level. This structure would also be able to recruit significant LE resources for a variety of problems outside intelligence collection.

4. People Policies

Interagency cooperation requires that culture be nurtured, in cooperative terms, within each agency. The GNRA has already set a precedent by implementing personnel policies to ensure development of military officers from various branches who would form a core of experts for operations within a joint culture. Regionally, staff duties would be to the interagency, not to individual agencies, which would enhance multi-agency trust and sharing. Positions would be filled by personnel with many and varied experiences, an á la carte board of experts. A renewed focus on personnel policy within a regionalized structure would diminish this long-term problem as close personal relationships develop with time.

To effectively achieve intelligence sharing we need to ensure a national and international strategic approach in addition to improving cooperation between the IC and LE. To accomplish this we must:

- Develop a mutual operations doctrine.
- Appoint of a single authority for national command and oversight.
- Regionalize intelligence-gathering efforts to reduce management and duplication problems, and become more efficient.

- Develop good personnel policies in regard to cultural change and bias and development of relationships through these policies that foster trust by dissolving specific single cultures in exchange for promoting an interagency culture.

D. CIVIL LIBERTIES AND DISSEMINATION ISSUES IN INFORMATION SHARING

The recent wiretaps linked to NSA under direction of the President caused quite a stir in the American populace. Are we to believe that liberty and security are in opposition to one another? Can we forfeit national security and still survive economically in the linked global world and win the war on terrorism, or do we have to forfeit civil liberties to fight this war? These are the questions that face the intelligence agencies within the U.S. despite whether the CIA or another agency is allowed to collect domestic intelligence; these issues will not go away. The question then becomes how to we deal with them?

Since 9/11 there has been an increase in general security measures for borders, critical infrastructure, and other issues, which many feel is justified. There has been a federalization of airport security by turning authority for that transportation segment over to the Transportation Security Administration, created after 9/11 within the Department of Homeland Security. There have been other changes as well, and psychologically we may feel safer as a Nation, but have these actions made us safer? In fact, good intelligence will ultimately filter down to our abilities with HUMINT. Whether we have a system such as discussed previously or whether our intelligence-collection efforts remain the same, HUMINT will be the most effective weapon against the GWOT. This brings us back to the fundamental problem of personal liberty versus state responsibility. Every person has a moral and ethical code, the law has ethical and legal codes, and agencies are pitted against these codes whenever they perform intelligence functions. And yet, it is these constructs that allow us to maintain order. Should there be a compromise? For example, the U.S. Government allows the individual the right to free speech, freedom to assemble, freedom to worship, freedom of expression, and other freedoms. In other countries such as Afghanistan, particularly under the brutal rule of the

Taliban, and in Iran, the citizens have no such freedoms. Thus, the citizen cannot challenge government control over personal liberty.

It is the responsibility of the state to ensure its existence but also to protect the citizens. Thus far, the Constitution has helped the U.S. maintain that delicate balance of personal liberty versus state responsibility. However, this has required proactive measures which have been within the law through our governing system. A good example of this is taxation. The "Boston Tea Party" was launched because of the levy of a 6 percent tax, but today our taxes are much greater. The Government has found how far they can push and have done so to the extent the citizens have not rebelled. Will the exorbitant costs in lives and dollars in Iraq, Afghanistan, and against the GWOT as we continue to ramp up security cause U.S. citizens to rebel? It is interesting to note that the U.S. Constitution or Bill of Rights does not guarantee personal liberty, but guarantees tools to assert and practice our beliefs as we see fit about personal liberty. In other words, within the U.S., sovereignty resides in the people, who act through the organs established by the Constitution.[101] The guarantees to protect personal liberties include Amendments 1, 2, 4, and 5. The framers of the Constitution understood individual rights versus government/state power, as is evidenced by these amendments. This allows for differences of opinion as well as conflict to coexist. This can be evidenced by the polar-charged issues within our society that include civil rights, abortion, and gun control. Through time, diversity has led to compromise for the good of all.

We are now faced with a new enemy who does not acknowledge laws, compromise, or liberties. This new enemy, terrorism, seeks to destroy all democracies, specifically the U.S., through use of asymmetric methods. As a result of this threat, 9/11 being the primary catalyst, the Patriot Act was passed. A great many individuals and local and state governments oppose this act, believing it infringes on personal liberties.[102] However, without security, democracy cannot exist. Thus, there must be a

---

[101] *Chisholm v. Georgia, 2 Dall 419, 471; McCullock v. Maryland, 4 Wheat 316, 404, 405; Yick Yo Hopkins, Supreme Court of the United States 118 U.S. 356, 370.*

[102] John Nichols, "Ten Against Patriot Act Reauthorization," *Yahoo News*, March 3, 2006; available from http://news.yahoo.com/s/thenation/20060303/cm_thenation/165474;_ylt=A86.I0baSwhEWe4AjQ_9wxIF;ylu=X3oDMTB;MHVqMTQ4BHN1ywN5bn1YmNhdA--. [cited March 3, 2006].

fine balance, at least in a democracy, between individual liberties and the power of the state and its survival. Generally, every person in the U.S. would not be infringed upon. For example, we have already categorized many as suspected terrorists, unlawful combatants, non-citizens, enemy combatants, and known terrorists. As such, these people are not guaranteed the same rights and privileges as those who are citizens of the country, if for no other reason than by definition. So, are the citizens of the U.S. or the state willing to infringe on the liberties of these labeled individuals and/or the countries from which they originate?

While many believe that all people within the U.S. should be protected through the civil laws and rights reasonable through constitutional process, this belief is in error. Why? It is because the Constitution only guarantees these rights to the "citizens" of the United States. Therefore, labeled individuals are not protected by the law against what many may perceive as unwarranted wiretaps or other surveillance. As an example, would U.S. citizens have an issue with the surveillance of a person planning another 9/11-style attack and who would be a labeled individual within U.S., but were residing in their own country? The answer is a resounding no. Thus, if it is okay to gather intelligence on that person in their own country, U.S. law should not protect them within CONUS or anywhere else. The main reasons are that the individual is not a citizen and thus has no rights extended to them through the U.S. Constitution and are within a labeled group that may be planning harm against the U.S. and affect national security. All of the hijackers in the 9/11 attacks used U.S. personal liberty laws against us and caused the deaths of over 3,000 individuals and billions of dollars in damage. Should we let this happen again? The answer is absolutely not.

It is interesting to note that individuals balk so much about the wire taps against those known to be adversarial toward the U.S. and the democracy it represents, i.e., the voice of people. Yet, these same individuals fill out credit card applications, use grocery store cards to swipe for savings, use gas cards, purchase cards of a wide variety, fill out questionnaires for trips, apply for all types of credit and knowledge, and all the while are giving up free information. Each time the individual does this, multiple times per day on average, this information is stored in myriad databases within the U.S. and can be purchased by any individual or government agency for a very small fee. An example is

www.intelligentinvestigations.com. One in particular is used specifically by LE groups. Therefore, to balance civil liberties, the law is clear that those who are in the U.S. and labeled as above, especially illegal immigrants and non-citizens, are not protected by the Constitution and are thus subject to intelligence-gathering methodology without the strict requirements as applied to citizens, which would have to follow legal means unless the individual can be shown to fall within the labeled group. The Patriot Act should make this clear, but does not. Also, because DNIN leverages the resources of LE agencies nationwide, who work within a strict legal framework, many civil liberty issues in regard to DI collection will be solved.

E. SUMMARY

To effectively achieve intelligence sharing we need to ensure a national and international strategic approach in addition to improving poor cooperation between the IC and LE. To accomplish this we must:

- Develop a mutual operations doctrine.
- Appoint of a single authority/board for national command and oversight (DHS IA).
- Regionalize intelligence gathering efforts to integrate intelligence collection and analysis, reduce management and duplication problems, and become more efficient. An, also to be closer to stakeholders for cooperation and collaboration purposes.
- Develop good personnel policies in regard to cultural change and bias and development of relationships through these policies that foster trust by dissolving specific single cultures in exchange for promoting an interagency culture.
- Address civil liberty issues, many of which will be addressed by incorporation of LE into the intelligence process since they already adhere to civil liberty guidelines and processes within the law.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. PSYCHOLOGICAL BARRIERS AND INCENTIVES TO SHARING INFORMATION

Earlier, the terrorist attacks of 9/11 and the case of WMDs in Iraq were mentioned as failures, of the U.S. IC. Assuming that these instances were indeed failures why did they occur? Was the failure due to not sharing information, or were other issues involved in the sharing process that contributed to the results? Ultimately it would appear that psychology, both of the group and the individual, has a great deal to do with the problems of sharing information or intelligence. However, even when information is ordered shared by law, problems may remain. For example, Congresswoman Jane Harman and Congressman Saxby Chambliss introduced legislation, called the Homeland Security Information Sharing Act, to direct Federal intelligence agencies to share information about possible terrorist attacks with the Nation's governors, mayors, LE personnel, and first responders; the bill was passed in 2002.[103] Despite passage of this bill, little has changed in regard to sharing information. Why?

A. HERDING, INCENTIVE AND FALSE POSITIVE/NEGATIVE PROBLEMS

An intelligence group or agency shares the same type of trade-offs as any organization or corporation. While an organizational hierarchy enables the aggregation of information, each bit of information that is deemed important is gradually passed up the organizational ladder, and if the information is exceptional and optimal, matching of problems to expertise termed "management by exception" will occur.[104] Thus, the hierarchy enables expert knowledge to be reserved for situations in which it is especially valuable. Large organizations enable constraints to be circumvented so that more intelligence data can be gathered and a greater variety of expertise can be used in data compilation and evaluation than in small groups. With greater resources one can trowl more broadly and not set restrictive upfront criteria for what is valuable data, which

[103] Philippe Reines, "Harman & Chambliss Introduce Homeland Security Intelligence Sharing Legislation," U.S. House of Representatives: Permanent Select Committee on Intelligence, 2002; available from http://intelligence.house.gov/CaseStudies.aspx?Section=84. [cited December 14, 2005].

[104] Luis Garicano, "Hierarchies and the Organization of Knowledge in Production," *Journal of Political Economy* 108, no.5 (2000).

happens with small groups with less funding. However, there are at least three sets of problems associated with the hierarchy of a large group. These problems exhibit themselves as, first, herding or "group think" that typically takes places at the analysis stage and in which the accumulated information and conclusions develop a momentum so strong they cannot be challenged, even if they are not correct. Second, erroneous conclusions can result if a pattern is missed because different pieces of information are not shared, which was the major cause in the failure to anticipate the 9/11 attacks. Third, agencies can be poorly designed to achieve the desired goal. For example, the FBI is supposed to be able to solve crimes and also collect domestic intelligence. The problem is that the FBI is designed to solve crimes. Because the organizational structure requirements for the two tasks are different, the FBI does not perform DI collection very well.

As has been demonstrated, the link or relationship between two nodes (people or organizations) is a key aspect of the strength of a network. Thus, who talks to whom and who passes along intelligence to whom is in direct proportion to the strength of a link between two nodes or entities. This becomes a trust issue that is the foundation of personal psyche. Because of hierarchy, however, the stages by which a particular piece of information moves from its origin to the point at which it is combined with other information for analysis is usually unknown to the analyst. Is the information a distinct piece that has been corroborated, or is the same piece of information being passed along via different channels? In the case of the Iraq WMDs the intelligence agencies relied heavily on intelligence supplied by exiles from Iraq. Most of the reports contained similar findings and appeared to be corroborated. Later it was learned that, rather than being distinct pieces of information from independent sources, the reports likely originated from one source, the Iraqi National Congress.[105, 106] Did the fear of going against the momentum of the reports, without corroborating them, drive analysts to a false conclusion? Most data concerning the issue of Iraq's possession of biological WMDs originated from an Iraqi defector, which became known as the infamous

[105] Jim Dwyer, "Defectors: Reports on Iraq Arms Were Embellished, Exile Asserts," *New York Times*, July 9, 2004.

[106] Glees and Davies, *Butler's Dilemma*.

"Curveball" case, the name given to this defector who claimed to have worked in Iraq's bioweapons program and who reported similar information several times to different sources.[107]

The problem of herding arises when an individual decides that a body of public information outweighs personal, contradictory information.[108] An example would be three individuals who can observe each other going to movie A or movie B. Individual 1 chooses A at random and although individual 2 believes each movie is equal also chooses A since individual 1 chose A. Individual 3 now has three pieces of information, the actions of 1 and 2, as well as his own opinion. Because there appears to be substantial evidence that movie A is better, individual 3 may choose to view it as well. Why? Herding occurred because each individual rationally weighed the evidence received and that appeared to be based on separate judgments against first-hand information; thus, the individual acted accordingly. Given the case, it is clear how herding can lead to a situation in which everyone is wrong, i.e., a poor consensus. Therefore, a herding problem can arise when intelligence analysts confront a consensus judgment based on many sources because the judgment may be based on the same single source that may have been communicated to the analyst through several channels. Psychologically, the analyst is weighing one data point against what appears to be several others that appear to be corroborated and thus will bow to peers pressure and agree with the general consensus, even if he may feel he is wrong.[109] A possible way to reduce the risk of herding, especially in a computer network or on paper, is the attachment of an encrypted tag to each information source. Actually, this should be required as a standard operating procedure (SOP).

Career incentives can also encourage herding, especially when the employee's career depends on evaluations by his superiors. The psychological pressure to please the superior can lead to the "yes man" phenomenon and also not to update prior beliefs,

[107] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, "Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction" (Washington, D.C.: Government Printing Office, 2005).

[108] Abhijit V.Banerjee, "A Simple Model of Herd Behavior," *Quarterly Journal of Economics* 107, no. 3 (1992).

[109] Peter M. DeMarzo, Dimitri Vayanos, and Jeffrey Zweibel, "Persuasion Bias, Social Influence and Unidimensional Opinions," *Quarterly Journal of Economics* 118, no. 3 (2003).

which could make the analyst appear unreliable — an acknowledgement of error.[110] In effect, the analyst herds with his own prior judgments. Generally, the more experienced the analyst or manager and the longer time on the job, the more likely this is to occur. Another incentive factor in intelligence sharing is that the analyst may take the easy path and adopt the opinion of co-workers. Like the old adage, "if you cannot beat them, join them," there is a psychological comfort in the safety of numbers, i.e., a reduction of fear of criticism. Actually, this would not be uncommon since if accurate information is difficult to recognize as being accurate, there will be difficulty designing a system of rewards for producing accurate information. A general approach to resolve this incentive is to ensure that career rewards depend on performance by evaluation, i.e., merit based, and that the biases of superiors are known by the subordinates. Even then, subjectivity will be unavoidable. The problems discussed are weaknesses of a hierarchal organization. Centralization of an intelligence system is likely to exacerbate the "yes man" problem by creating a tighter hierarchy.[111] In contrast, in a system in which there are many bosses and many sources of information, such as a multi-agency, intelligence-gathering network, even if the subordinate echoes the views of his superior, there will still exist many different views. The weakness herein would be the identification of the ultimate superiors. However, even through decentralization, superiors will have an incentive, i.e., the psychological fear of peer pressure, to conform their advice to policymaker preconceptions. As an example, before the Iraqi war, the IC knew that policymakers were convinced that Iraq possessed WMDs. However, the DOE did not concur with policymaker's belief because they had relied on a separate piece of evidence, but eventually DOE caved to the consensus view concerning Iraq's WMD capabilities, a position that "made sense politically, but not substantively."[112] Thus, we see that psychologically, the fear of going against the group or consensus may be too high a price to pay, at least for the individual or agency, not withstanding the long-term effects in this case to the people of the U.S. Top-down systems pressures to generate conclusions that

---

[110] Canice Prendergast, "A Theory of 'Yes Men'," *American Economic Review* 83, no. 4 (1993).

[111] Daniel E. Murphy, *What Stalin Knew: The Enigma of Barbarossa* (New Haven: Yale University Press, 2005).

[112] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.

fit existing or planned policy, it is the conclusions that are modified to fit the political agendas and the data can be discarded.

Looser, less centralized organizations filter out fewer ideas and thus produce a more diverse set of options for the leaders of the organization to choose from. When the environment is unstable, the organization should be decentralized in order to maximize the likelihood that many fresh new ideas will be produced, for that will make it easier for the organization to adapt to a changing environment. For intelligence organizations, particularly counter-terrorism intelligence, a loosely knit, decentralized structure of multiple agencies is likely to be optimal. The information environment is unstable, and since many intelligence leads and clues become dead ends, the few accurate clues are scarce and therefore valuable. Generally, when good ideas are scarce, a decentralized structure is preferable as more ideas will get through the filters that are so typical in large, hierarchal organizations.[113] Also, in intelligence work the cost of false negatives, i.e., not pursuing a lead and failing to aver a terrorist act such as 9/11, is likely to be considerably higher than the cost of false positives, e.g. pursuing a lead that turns out to be a false alarm. The 1973 surprise attack by Syria and Egypt that began the Yom Kippur war is an example in which a centralized intelligence approach failed; 9/11 is another example. In the months preceding the Iraqi war a number of low-level CIA officers in the Directorate of Operations expressed doubts about the accuracy of Curveball's information. Superiors disagreed due to fear of being out of sync with policymaker's views and the information was presented in a filtered, unified view that did not reveal the diversity of opinion at the lower levels.[114]

In a decentralized organization there arises a trade-off between false positives and false negatives. If too many warnings are given, much like the homeland security color-coded threat warning system, it is like the "boy who cried wolf" and little attention is given to the alert. Thus to minimize the number and cost of false positives or alarms, the standard for warnings must be raised, which requires a more centralized structure to filter out false alarms. If, because of past failures such as 9/11, agents become "trigger happy,"

[113] Raaj Kumar Sah and Joseph E. Stiglitz, "The Architecture of Economic Systems: Hierarchies and Polyarchies," *American Economic Review* 76, no. 4 (1986).

[114] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.

then less filtering occurs and information tends to be less accurate. This can be buffered in a networked process through critical analysis at a regional center before passing the intelligence forward.

B. INCENTIVES FOR SHARING INFORMATION

The lack of prompt and full sharing of intelligence within the IC, and between Federal, state, and local government levels, has been blamed for the failures of 9/11 and the Iraq WMDs. Generally, members of an organization often have disincentives to share information. The fear of lack of opportunities to climb the promotion ladder, loss of job, or disapproval of one's superiors serve as strong psychological fear barriers to go against the grain and to share information. Competition between employees for both pay and promotion for a fixed number of career-level slots creates an atmosphere of non-sharing. There may be good incentives in terms of performance, but a lack of sharing and even sabotage of one employee by another is common by concealing information or providing false information.[115] Employees may squander resources on activities that influence superiors' decisions in order to manipulate the perception of their performance or gain favor of superiors.[116] A good example is the presidential daily brief that has become "the" platform through which intelligence agencies seek to better themselves in competition with each other. The following statement illustrates this well: "The daily reports seemed to be 'selling' intelligence — in order to keep its customers, or at least the First Customer, interested."[117] Influence activities, such as a turf war in which agencies shift resources from productive activities to influence activities is an extreme example of this.[118] A turf war between the FBI and the CIA was at the heart of the failure to track 9/11 terrorists as they entered and moved about the U.S.[119] Since 9/11, not much has

---

[115] Edward P. Lazear, "Pay Equality and Industrial Politics," *Journal of Political Economy* 97, no. 3 (1989).

[116] Paul Milgrom and John Roberts, "Bargaining Costs, Influence Costs and the Organization of Economic Activity," in *Perspectives on Positive Political Economy*, ed. James E. Alt and Kenneth A. Shepsle (Cambridge: Cambridge University Press, 1990).

[117] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.

[118] Stergios Skaperdas, "Cooperation, Conflict, and Power in the Absence of Property Rights," *American Economic Review* 82, no. 4 (1992).

[119] *9/11 Commission Report*, 263.

changed; officials at the CIA's Counter-terrorism Center claim that "they have difficulty tracking and obtaining information about terrorist cases after they hand them off to the FBI."[120]

Another reason why members of an organization may not share intelligence is because they do not want to lose the rents derived from their control of the resulting knowledge. For example, a law enforcement agent who has information that may lead to an arrest is usually not willing to pass the information along to another officer or agency because by doing so, the reward of the arrest for him or her will be lost, even though it may be the right thing to do from a social perspective. The fear of losing the reward and gaining advancement outweighs the spirit of doing what may be perceived to be more correct, i.e., sharing the information.[121] However, a reward based on quantity of information shared causes information quality to suffer. Psychologically, the incentive to share should be stated such that "value" of information is more important; therefore, seeking something of greater value presents a mental challenge that most are willing to accept, and the individual agent will go to great lengths to find the best information. It is a natural competition, and incentives based on this concept retain and even increase information quality. Of course, it is generally difficult to determine just how important a piece of information may initially be, but utilizing an "encrypted tag" system as discussed earlier will allow tracking where and how the collected information is referenced in other reports. Academics use such a system for promotion criteria by tracking the number of "hits" of a particular written article, i.e., how many times that article is referenced by peers.

The best method of providing incentives for information sharing is to place those who have the information to be shared in close proximity with others that have related responsibilities. An example of this is the National Counter Terrorism Center (NCTC) where representatives from various agencies sit side by side. Psychologically, this creates an atmosphere of teamwork, and those who perceive others to be on the "same team" are more likely to share, feeling automatically that the others have a need to know.

---

[120] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 469.

[121] Luis Garicano and Tano Santos, "Referrals," *American Economic Review* 94, no. 3 (2004).

This is an excellent way to align individual and organizational incentives and reduce officer or agent conflict.[122] Further, when placed in a team situation, a feeling of needing to assist team members is developed, as well as mutual trust. In the case of intelligence, agents will typically care more deeply about their mission in these situations and may place a higher priority on sharing intelligence data.

There are various ways to accomplish trust in information sharing communities. Methods such as swift trust, institutional trust, and others are prevalent and well known. However, transactive memory theory is perhaps more easily applied and understood. Transactive memory theory is based on the idea that individual members can serve as external memory aids to each other.[123] Members are able to benefit from each other's knowledge and expertise if they develop a good, shared understanding of individual expertise in the group/unit — who knows what. A transactive memory system is built on the distinction between internal and external memory encoding. Often, individuals encode new knowledge internally, in their own memory. However, even more often individuals encode or use knowledge encoded externally (in diaries, in books, or even in other people's memory). In these cases, the individual internally encodes the label (subject) of the knowledge as well as its location but not the knowledge itself. Transactive memory systems are built on this view of individuals playing the role of external memory for other individuals who, in turn, encode meta-memories (i.e., memories about the memories of others). Wegner proposed that two types of meta-memories are maintained in people's minds — information about the subjects of knowledge of each member (i.e., areas of expertise) and information about the locations of the knowledge.[124] Knowledge is encoded, stored, and retrieved from the collective memory through various transactions between individuals, based on their meta-memories.

---

[122] George A. Akerlof and Rachel E. Kranton, "Identity and the Economics of Organizations," *Journal of Economic Perspectives* 19, no. 1 (2005).

[123] D.M. Wegner, "Transactive Memory: A Contemporary Analysis of the Group Mind," in *Theories of Group Behavior*, ed. B. Mullen and G.R. Goethals (New York: Springer-Verlag, 1986).

[124] T.G. Wegner and D.M. Wegner, "Transactive Memory," in *The Blackwell Encyclopedia of Social Psychology*, ed. A.S.R. Manstead and M. Hewstone (Oxford: Blackwell, 1995).

Findings of both field and laboratory research indicate that transactive memory can serve as a facilitator of group performance, where groups whose members are aware of the knowledge and expertise of other group members perform better than groups whose members do not possess such knowledge. Transactive memory systems enable groups to better utilize the knowledge that their members possess, and to reach higher levels of performance than they would have reached without such a system.[125] Members of small groups, who are co-located, can initially use surface information to infer rough estimates of "who knows what" and can then reach greater accuracy in the attribution of expertise to other group members through common experiences.[126] This will enhance information sharing.

It can be argued that centralization will improve information sharing, but as we have observed from the cases presented, the common centralization of either the CIA or FBI has not achieved this goal. Generally, a single agency will tend to have a common code to share, but with the team as illustrated above, that same code has a chance of being stronger due to a common goal. While the single agency may have a common code, compatible data networks, uniform access criteria, and other common practices, these same attributes can be accomplished by a network by developing the same tools for sharing, and as an overall team the strength of the relationships is strengthened as illustrated in Chapter III. This is a clear example where centralization has failed and argues for a network of multiple agencies with a common goal so that psychological barriers based on need to know can be converted to a need to share. That example is the FBI who, in the eight years following the 1993 truck bombing of the World Trade Center, tried without success to develop an effective domestic intelligence capability. On two separate occasions, it adopted strategic plans that it failed to implement. The 9/11 Commission found that the FBI had failed both to collect adequate intelligence data and to combine the raw, disaggregated data into accurate knowledge of terrorist threats. The causes of these failures included resistance and obstacles from local field offices, failure to obtain additional resources asked for from Congress, reliance of analysts on personal

[125] DHS Staff, "Press Room: Biographies."

[126] D. Nevo and Y. Wand, "Organizational Memory Information Systems: A Transactive Memory Approach," *Decision Support Systems* 39, no. 4 (2005).

relationships from field agents (these relationships were weak), lack of a single database into which field offices could send information to headquarters that prevented aggregation and sharing, and lack of human resource development.[127]

C. THE PSYCHOLOGY OF INFORMATION — WHY WE DON'T SHARE

Generally, intelligence is a simple process, but sharing it seems to have become complicated. It is not technology that causes the primary problems in sharing, but human nature and culture. Within the information process there are three basic steps. First, there is the data — collecting it or assembling the facts. Second, there is information, the step where meaning is attempted to be gleaned from the data. Third, we put form to the information phase to obtain knowledge; hence the term knowledge management. There are two applications for knowledge: either an organization is in the "sense-making" business such as science and arts or, as with the majority of many organizations, there is the "application" business where information is used to improve the lives of others. This is particularly true of the intelligence community, which gathers information to protect against threats and attacks. Technologies such as the advent of packet switching, XML, and other advances have progressed to the point where most organizations cannot keep pace with the advancements. Thus, the technology is like a gun, which typically has the ability to shoot much more accurately than the person shooting it. In this sense technology cannot be blamed for our inability to share. That inability then must stem from personal and shared culture.

Let us examine some of the reasons why sharing of information is often impeded. These reasons stem from our mental or psychological processes based on perceptions, feelings of trust, the right thing to do, and so forth. These reasons include, but are not limited to: (1) Many personnel do not want to deliver information their superiors do not wish to hear, i.e., bad news, especially if there is no plan in place or process to deal with it. Information is best absorbed by superiors if that information fits their preconceived opinions and is related to what policy makers also desire. Presenting such information does not usually coincide with upward mobility and promotion. (2) Within hierarchies, information is generously shared on a peer-to-peer basis, but is shared grudgingly either

[127] *9/11 Commission Report*, 76-78.

upward or downward in the organization. Reports to superiors are viewed generally as having little value to the person who prepares it. Information that flows downward in most organizations is usually on a need-to-know basis and, as is well known, water-cooler conversations and the office grapevine will usually spread information faster than the boss. (3) Acceptance and internalization of information depends on the individual's mental model. For example, after a presentation or information is shared, unless what is divulged fits the individual's personal perceptions or reinforces what he or she already believes, the tendency to share that information is reduced, i.e., because it does not conform to what is generally believed or does not fall in line with policy. (4) Accountability for bad information can be severe. Most are averse to sharing information orally, but especially in written form if that information is misused and is tracked back since he or she will be held directly accountable. (5) Generally, an individual is very reluctant to admit what they do not know or understand. In hierarchal organizations this is particularly true the higher up the pecking order one goes. This leads to what is termed "groupthink" in which those higher up tend to consult with other higher ups, particularly if they do not have the skills to use the technology that subordinates are adept at. An appearance of weakness is present and thus presents a perceived barrier that, psychologically, the superior is unwilling to cross, i.e., to admit a weakness or deficiency. (6) Internal competition may prevent complete sharing. Organizations that have internal performance evaluation systems that pit one employee against another for limited rewards or promotion will succeed in promulgating peer-to-peer distrust and will push sharing outside the organization. (7) Determining useful from useless information is difficult for most and, psychologically, most are unlikely to share that which they do not understand because of the exerted pressure of appearance of ignorance. The primary reason for the inability to determine the difference of information type is due to the inability to process the volume of information garnered and general lack of imagination. Thus, stored data is generally underutilized while information provided "just in time" tends to be over-relied upon, i.e., it is simply easier to see its value within the context of an urgent problem. (8) The cost of data acquisition versus not knowing is generally underestimated. For example, hurricane Katrina, 9/11, the avian flu, and Iraq have all demonstrated that the lack of knowing can lead to catastrophic though preventable

results. (9) Personal culture is such that the individual desires those he or she likes to succeed, while those that are not liked are desired to fail. Thus, the more office politics there are, the greater the impedance to information flow, particularly if promotion, acceptance, and/or recognition are on the line. Psychologically, we all fear failure. (10) Rewards for sharing can produce short-term results through initial increases in contributions, but a reduction in quality of data.

D. HOW DO WE COMPENSATE FOR SHARING IMPEDANCE?

There are various methods that can be used to compensate for poorly sharing information and intelligence. These include the following: (1) Flatten the organization so that it is no longer a hierarchy. This will transfer decision-making authority and place collectors and analysts on a more even playing field. (2) Change reward systems to recognize the group rather than the individual contribution, i.e., make it a team effort—small military units, SWAT teams, and law enforcement branches are good examples of this. (3) Eliminate reward and performance evaluation processes that encourage individuals to hoard, manipulate, or fight over credit for information and ideas or that interfere with collaboration. (4) Develop mechanisms to anonymously communicate "bad news" or information that does not fit the preconceived notion of the superior or policy maker. (5) Provide personnel with informal places to meet and exchange information with peers since they are much more inclined to share with peers than with those up or down the hierarchy. (6) Develop and use social network maps to determine key knowledge connectors and information transfer bottlenecks. This will address the issue of rewards that usually do not work well for long and also will encourage those to address this issue who have the most valuable knowledge and least time to share it. (7) Develop better filters for information and better ways of organizing, indexing, sorting, and archiving it for later retrieval to differentiate between useful and useless information. 8) Expand risk management programs to assess the costs of acquiring information and of not knowing.

Knowledge management and transfer have become significantly more important as society moves forward. To be effective in sharing information and to achieve successful knowledge management, the psychological fear of numerous points in the

process must be overcome. Knowledge transfer has always been a challenge for organizations. Its importance has grown for three reasons. First, knowledge appears to be an increasing proportion of many organizations' total assets, as well as the individual. Second, organizations have moved away from hierarchal methods of control toward more decentralized organizational structures and increased employee involvement, which has increased fear of failure in some instances.[128] Third, advances in information technology have created new means of knowledge transfer, itself a source of intimidation to many. Knowledge transfer is only valuable when it is integrated into a set of policies for knowledge generation and capture, which is particularly useful in intelligence.

Far more ideas exist than good ideas, but like the question in a class, which the individual is encouraged to ask because "no question is a stupid question," many fail to put forth the good idea for fear of non-acceptance. Because of the prevalence of ideas, organizations must evaluate new ideas and determine whether they have worked in the past, are likely to work now, and where they may be applicable. Personnel must have the capability, incentives, and structures to perform the necessary tasks related to information. Possession of the right tools will of itself reduce the fear of sharing information that may not be corroborative or perceived as being of little importance. In principle, more information is better than less. Conjointly, too much information creates overload. The Internet is a classic example, where no individual can read even a fraction of what is there. The key to disseminating knowledge is that people receive it that can use it and those who disseminate it gain confidence that it is "good" information. In an ideal world, if people knew the right thing to do, they would do it. Such a world does not exist. Complex theories have been developed as to why, even after knowledge has been transmitted to the right people, that it may not have been transferred to the organization. The FBI and CIA examples are clear illustrations of this. These theories fall into the categories of inadequate capability, poor incentives, poorly trained personnel, and inadequate structures such as rigid operating procedures that are difficult to update.

To effectively generate new ideas, personnel need to be trained in problem solving, including an ability to think "outside the box," a term that is much overused. A

[128] David I. Levine, *Reinventing the Workplace: How Business and Employees Can Both Win* (Washington, D.C.: Brookings Institution, 1995).

typical program includes how to identify problems, prioritize, analyze root causes, identify possible counter-measures, implement the solution, and check whether the solution actually works. Such personnel, better prepared, have great confidence and less fear of sharing. As an analogy, a well-skilled martial artist walks down the street with a friend; he sees two men that may appear to be a threat, but given his skill knows how to both perceive the situation and deal with it, while the friend does not. The reaction in the martial artists mind is analysis and problem-solving, "what if" scenarios while that of the untrained is an inward fear and panic due to possible consequences. All are based on psychology of differentiating between perception and intent and one's state of preparedness. Training will reduce fear of sharing and increase productivity. Both superiors and personnel must be trained to evaluate new ideas and not be threatened to share them. Just as importantly, they must be trained in systematically understanding what evidence should be convincing. An example would include the difference between correlation and causality and the problems of small samples since basic concepts are often difficult to apply in practice. Training personnel to both disseminate and adopt new ideas may revolve around making them aware of where in the organization their ideas may be useful and from where ideas may arrive. Given the current state of the IC in regard to loss of analysts through attrition, training analysts will become a priority. Charles Allen has mentioned that such training needs to be accelerated and the author agrees. Although analyst training is beyond the scope of this thesis, training large numbers of analysts can be done quickly and efficiently with current technological capabilities.

To create an environment that encourages the generation of new ideas, managers should consider the following policies: incentives for groups instead of just for individuals, duties that include experimentation with ideas and concepts, permitting such ideas that are well conceived but may fail, and giving credit to employees who generate new ideas while at the same time encouraging others. Personnel are most likely to spend energy sharing what they know if they are in a single workplace with group incentives, i.e., a network of multiple agency personnel. Thus, extra incentives can be helpful when personnel are in different units without necessarily common objectives. An example of this is Buckman Laboratories (see www.buckman.com) where everyone sees who

answers problems on the open bulletin boards. Those who contribute to solving company problems in public are praised while those who do not become conspicuous. This creates a better atmosphere of unity and cooperation as those who share frequently take others into confidence and further open discussions and sharing of all kinds of ideas.

Other components to promote sharing include structures and technology. The most important structural component that encourages creativity or idea generation is often providing time to experiment and tinker. Formal personnel involvement structures such as brainstorming, suggestion programs, quality circles, and self-directing teams support both creating and sharing information. People need the power and responsibility to make improvements. This breaks down the fear of sharing with peers and heightens the anticipation of possible "good" recognition, both of which are key parts of one's psychological framework. Technology can help with the dissemination of ideas by making it easier to target appropriate recipients such as a group defined formally by a common product such as a specific analyst type, a group formed by management, or an ad hoc group formed by personnel in the form of an email list or other membership.

The keys to sharing are to capture the existing knowledge from within and outside the organization and to adopt those ideas that are relevant. Training, incentives, structures and technology can all improve sharing because they become the tools to reduce the fear, sometimes individually preconceived, of failure or embarrassment. Good and actionable intelligence should not be about who is right, but about what is right. Only through overcoming fear of sharing and breaking down barriers to it will effective intelligence sharing come about. Further, an increase in agent numbers will mean little if the sharing culture does not change.

E. SUMMARY

Overcoming psychological barriers to sharing will require:

- Avoiding herding or group think through incentives and promoting independent thinking and basing analysis on verifiable, multiple sources.
- Investigating career incentives and adopting policies to avoid consensus.

- Promoting a less centralized organization that will provide more diverse options, i.e., to promote fresh ideas, which have been proven to come from a wide variety of individuals regardless of age.
- Providing incentives for sharing information by placing those who have information to be shared into close proximity with others who have related responsibilities, i.e., a regional center with multi-agency personnel as in DNIN.
- Examination of rents derived from control of specific knowledge — we are one team.
- Integrating knowledge transfer into policy for knowledge generation and capture.
- Ensuring personnel are better trained in problem-solving processes.

Other processes that will break down psychological sharing barriers include compensation for information sharing impedance by flattening the organization; changing the reward system to recognize the group rather than the individual; eliminating of reward/promotion processes that encourage hoarding, manipulation, or credit for information; the ability to anonymously communicate bad news; determining key knowledge connectors and bottlenecks; developing better indexing, sorting, and data archiving methods; and expanding risk-management programs to assess cost of not knowing.

VIII. STRATEGIC PLAN FOR THE DEDICATED NATIONAL INTELLIGENCE NETWORK (DNIN)

A. HISTORY AND OVERVIEW

For many years there have been complaints about sharing intelligence between the two main stakeholders, the intelligence communities (IC) and law enforcement (LE). Reports about the events leading up to 9/11 highlight this issue, specifically regarding the CIA and FBI. New York City government felt that sharing was so bad between the Federal IC members, especially the FBI, that they formed their own intelligence group, sent officers overseas to collect intelligence, and have refused to share that intelligence with the FBI since the latter had refused many times in the past to share intelligence with New York City, citing a need-to-know position. The rationale for the NYPD's transformation after September 11th had two distinct facets. On the one hand, expanding its mission to include terrorism prevention made obvious sense. On the other, there was a strong feeling that Federal agencies had let down New York City, and the city could no longer count on the Feds for its protection.[129] Since the 9/11 attack on the World Trade Center, intelligence reforms within the U.S. have become key political and operational issues and forced agencies such as the FBI to reform and reorganize in response.[130] The FBI and CIA were singled out for intelligence failures due to events leading to the attacks — the most blatant criticisms were that there was a lack of intelligence sharing between the agencies and follow through issues were a problem, as well as focus on factors such as "who" versus "where."[131] Undoubtedly, if the CIA and FBI had been working with a networked sharing model, the outcomes could have been different. But, this criticism of intelligence sharing goes deeper than these two agencies; it prevails between the IC and LE agencies across the U.S., as well as the fact that neither of these agencies or any single agency involved in information sharing can hope to have the capabilities to share the large volumes of information that are collected on a national scope. Thus, a network, DNIN, is proposed to deal with both the scope/scale and volume of collected information.

[129] William Finnegan, "How Is the N.Y.P.D. Defending the City?" *New Yorker*, July 25, 2005; available from http://www.newyorker.com/fact/content/articles/050725fa_fact2. [cited April 12, 2006].

[130] Bowers, "How FBI Is Remaking Intelligence Functions."

[131] *9/11 Commission Report*.

A network-centric collection is the only way feasible for collecting the desired intelligence; but despite the vehicle, there will be both problems and advantages, as outlined below.

B. MISSION STATEMENT

A primary reason for existence of a DNIN would be its mission to the citizens it serves. Much like LE and the IC, the DNIN's mission must serve to promote the safety of the communities, states, and regions it serves. As an example, the Seattle Police Department lists its mission as preventing crime, enforcing the law, and supporting public safety.[132] Very similar mission statements can be found for the cities of New York, Los Angeles, Washington, D.C. and Los Angeles Sheriff's Department.[133] There is an interesting difference between the Washington, D.C. Police Department mission and others in that it specifically includes preventing crime and fear of crime, including terrorism, which may have been added after the 9/11 attacks. However, although LE agencies across the country collect intelligence of various kinds, especially through informants, which would be considered HUMINT, intelligence is not mentioned in any of their mission statements. Perhaps this is because the police inherently believe that collected intelligence is simply a component of their work, which would preclude the necessity of singling it out. In contrast, the CIA's mission statement, as a leading member of the IC, is collecting intelligence that matters, providing relevant, timely, and objective all-source analysis, and conducting covert actions.[134] The CIA focuses on overseas operations and foreign intelligence. Although they do cooperate with IC groups within the U.S., their primary focus is collecting information, analyzing it, and conducting covert operations at the direction of the President.

There are several attempts at local scales to gather intelligence and share it among LE agencies. Examples include the intelligence fusion centers in Virginia, Phoenix,

---

[132] The mission statement of the Seattle Police Department is listed on its Website at http://www.cityofseattle.net/police [cited May 1, 2006].

[133] These mission statements are found on the respective Websites of these police departments: http://www.nyc.gov/html/nypd; http://www.lapdonline.org; http://mpdc.dc.gov; and http://www.lasd.org [cited May 1, 2006].

[134] Source of mission statement is the CIA's Website at http://www.cia.gov [cited January 15, 2006].

Atlanta, the TEW (Terrorist Early Warning) group (which is part of the Los Angeles Police Department), and the intelligence and counter terrorism division of the NYPD. However, these remain at the local level and do nothing for homeland security and domestic intelligence collection nationwide. There remains a gap between LE and the IC in regard to intelligence that affects homeland security.

The intelligence-sharing network, DNIN, could have the following suggested mission:

DNIN is the eyes and ears for protection of the homeland to thwart and protect against acts of terrorism and other heinous crimes on U.S. soil. We accomplish this mission by:

- *Conducting authorized collection efforts that comply with judicial procedures and due process.*
- *Collecting and fusing intelligence from all sources.*
- *Providing credible, reliable, corroborative information on a need-to-share basis.*
- *Utilizing this information on a nationwide basis to preempt and prevent threats from organized gangs, terrorists, and other criminal activities.*

This mission statement serves to fuse LE and IC activities into a joined role. Intelligence is collected in a timely manner and disseminated on a need-to-share basis by LE, which can then be shared with members of the IC who may be able to add/corroborate with pertinent information from other sources without revealing source or method of collection. Further, LE will utilize this intelligence to enhance their own departmental missions and knowledge; but more importantly, since LE has arrest powers using basic probable cause, they can arrest and detain suspects when IC members cannot. If a system such as DNIN had been in effect concerning Mohammed Atta, who had been detained several times by the police, the enhanced intelligence would likely have resulted in Atta's arrest and the 9/11 outcome may have been different. The dots just could not be connected between LE, the IC, and all the existing intelligence that was not shared.

1. Fundamental Issues

"How can we collect information on a regional scale that becomes national in scope and disseminate information that is scrubbed along the way, that is credible, and that is reliable?" The general goal is to overcome resistance, typical constraints, and drawbacks involved in information sharing among agencies so that information flows in a constant stream to those who need it. The primary problems of traditional intelligence sharing are listed below, followed by the advantages of a networked collection and need-to-share approach. The fundamental challenge is to overcome the distrust and suspicion embedded in both organizations.

a. Problems

- Scale – Regional to National
- Cost
- Stovepiping
- Need-to-Know Attitude
- Specific Agency Culture
- Job Security

b. Advantages

- Credible, Reliable, and Corroborative Information
- Scrubbed Information
- Need-to-Share Attitude
- Memorandum of Understanding (MOU) Agreements
- Reputation
- Relationship Building

A comparison of the traditional versus networked method of intelligence sharing is illustrated in Figure 17. It will be noted that the networked method follows a

"Blue Ocean Strategy" whereas the traditional method follows a "Red Ocean Strategy."[135]

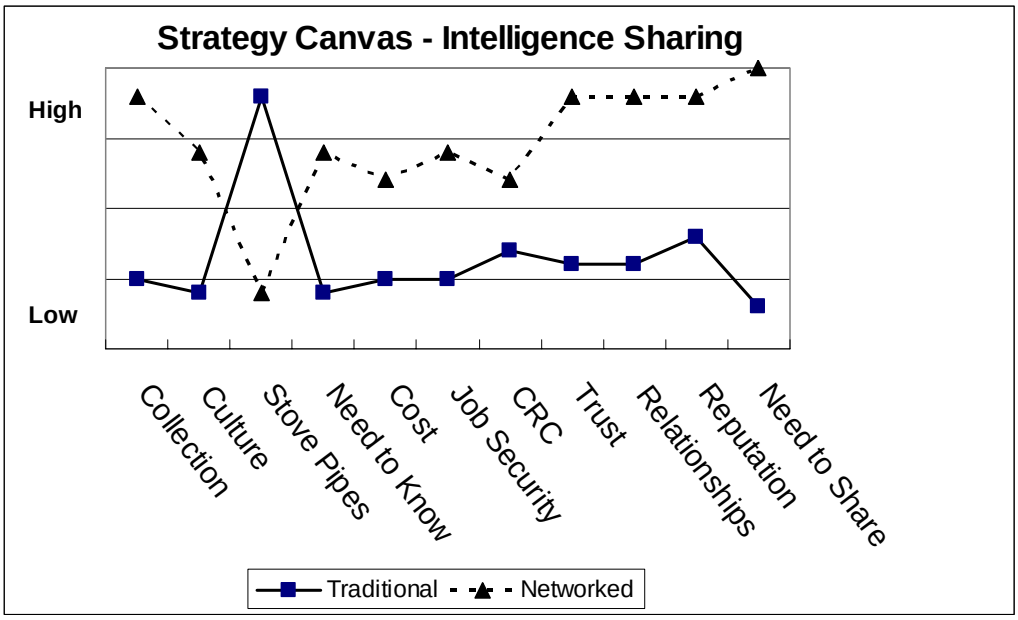


Figure 17. Traditional versus Networked Intelligence-Sharing Comparison.

The categories of difference are as follows: **collection** (more enhanced via DNIN than traditional methods); **culture** (multi-agency and much improved via network compared to traditional, i.e., friction of culture is reduced in DNIN); **stovepipes** (virtually eliminated in DNIN due to cultural shift and need-to-share attitude); **need-to-know** (traditional method operates strictly on need-to-know that is not conducive to the DNIN theory, which is based on need-to-share and is thus rated much lower in intelligence sharing in traditional method); **cost** (DNIN will require input funds compared to existing traditional system, but will show much greater returns on investment); **job security** (personnel in traditional system feel they must maintain status quo to keep jobs versus personnel in the DNIN in which networking and relationships would reduce fear of job security and thus increase perception that job security exists); **CRC** (credible, reliable and corroborative information) is enhanced in DNIN since the need-to-share attitude and relationships are much stronger than in traditional system); **trust** (working closely

[135] W. Chan Kim and Renee Mauborgne, *Blue Ocean Strategy: How to Create Uncontested Market Space and Make the Competition Irrelevant* (Boston: Harvard Business School Publishing Corporation, 2005).

together with a common goal, although from different agencies builds stronger trust factors than isolationist/elitist attitude of traditional system thus, the mutual trust factor is greatly improved); **relationships** (relationships become stronger in networked atmosphere and resulting in enhanced sharing) — an example is the JTTF, although little improvement has been made or at least has not spread nationally; **reputation** (within a networked sharing system it is perceived highly likely that agencies will be more forthcoming and not want to bear the brunt of the "agency" that held out in event of a scenario similar to 9/11 — cooperation will foster enhanced reputation); **need-to-share** (the development of DNIN is purely based on need-to-share intelligence, eliminating many barriers compared to the DoD-based need-to-know attitude that the IC operates under thus, information sharing is greatly enhanced).

The method of this stakeholder analysis involves building a regional to national intelligence-sharing network within the U.S., across barriers in which law enforcement (LE) are the main collectors of that intelligence. Further, the difference is due to the fact that LE will be the group collecting about 80 percent of the intelligence on a national scale. A recent example of this occurred in late 2005 when the City of New York went on heightened alert because of some gathered intelligence, which although not scrubbed as the IC community would have done, appeared credible.[136] The IC stressed not to go on the alert since the intelligence was not scrubbed, but the police, who were the major players and were operating on the need-to-share attitude, decided to err on the side of caution and deployed for high alert despite the desires of the IC, who were only a context setter in this case.

2. Goals

The priorities of DNIN are simple: to collect credible, reliable, and corroborative information that can be shared on a national basis to help thwart threats from all sources and also to reestablish the lost trust in Federal agencies by LE. The need to develop and share information and intelligence across all levels of government has significantly

[136] Leigh Sales, "Subway Warning: New York on High Alert," *ABC News*, 2005; available from http://www.abc.net.au/am/content/2005/s1477734.htm. [cited April 10, 2006].

changed since 9/11. The need to identify, prevent, monitor, and respond to terrorist threats, criminal activities, and all hazards is a significant challenge for the IC, LE, and private sector communities.

All IC members and LE desire credible, reliable, corroborative, and scrubbed intelligence and thus, have similar goals. However, due to 9/11 there is a lack of trust in the U.S. Government, which hurricane Katrina further exacerbated.[137] "How can the government or other agencies get that trust back?" There must be a 'buy in' for lack of better terminology, of the IC with LE. For example, LE continually passes information up then, nothing is returned in the process due to the need-to-know mindset. As has been seen, the FBI and CIA have had serious damage done to their reputations for the perceived failures that led up to 9/11. Consequently, there are two parameters that will have a drastic effect on the buy in for the American public. First, there is the reputation factor, and second, a job security factor. Examples of the first include the failures of the FBI, which has a poor reputation at present for perceived failure. Another is Colin Powell's passing along flawed information about Iraq's WMD capabilities, which was passed to him by IC sources, but which were wrong.[138] This resulted in damaging the CIA image and others in the IC. There is also the example of the Atlanta Olympic bombings in which the wrong man was initially arrested.[139] This caused damage to reputations as well. Coupled with media reporting the damage was maximized, and the desired good reputation is not easily recovered. In regard to job security, no one wishes to be the next failed FEMA director. Instead, one would hope to be a Rudi Giuliani who, interesting to note, was not well liked leading up to 9/11, but became one head that was well liked and trusted after the events took place. One would also not desire to be Mayor Nagan of New Orleans after hurricane Katrina devastated the area. Yet, there are good examples in these areas as well. A particular shining example in the IC is the good intelligence collected and shared during the Cuban Missile Crises in 1961, which may

---

[137] Borgna Brunner, *Hurricane Katrina: A Disaster and Its Catastrophic Aftermath* (Information Please, Pearson Education, 2005); available from http://www.infoplease.com/spot/hurricanekatrina.html. [cited April 9, 2006].

[138] Mike Wallace, "Colin Powell on 'Fox News Sunday'," *Fox News*, 2004; available from http://www.foxnews.com/story/0,2933,114159,00.html. [cited April 9, 2006].

[139] Ron Ostrow, "Case Study: Richard Jewell and the Olympic Bombing," *Journalism.org*,; available from http://www.journalism.org/resources/education/case_studies/jewell.asp. [cited April l 9, 2006].

have averted war between Russia and the U.S.[140] The value added by utilizing DNIN will help rebuild relationships between LE and the IC and allow for more efficient and rapid intelligence sharing that will protect the U.S.

While DNIN would not be a new business, it would dramatically extend current collection capabilities. So what? These capabilities would not just include a small increase. It is estimated that intelligence collection within the U.S. would increase a hundredfold. If DNIN is not addressed, another 9/11 would be more likely to occur. Evidence that supports this was the information obtained on September 10, 2001, that could have stopped the attacks but was not able to be shared quickly enough.[141]

3. Specific Approach

The traditional method for collecting intelligence, pre- and post-9/11, has been through various methods practiced by the IC, which is based on a reactive approach. The practices of LE have also been reactive. To be effective in collecting and sharing terrorism and anti-terrorism-related intelligence depends on CRC about the enemy, whether a terrorist, a criminal, or even a natural hazard/disaster. The obvious goal would be to provide information to identify immediate and long-term threats and the identity of person(s) involved in terrorism-related or criminal activities to implement prevention (risk-based), response, and consequence management. The traditional alternative of the IC and "the wall" between the IC and LE will not accomplish this task. The alternatives are the utilization of fusion centers across the country in various municipalities and states, which have for the most part remained isolated to a local or state basis, due to sharing as well as technology platform problems. In contrast, utilization of the DNIN can be scaled from a regional to national scope and will overcome these problems. The 9/11 attacks highlighted exactly how the traditional and local-based fusion approach failed and how it will do so again if we do not move to a national network of intelligence collection. The DNIN, coupled with data from over 800,000 LE officers, would be the front line of defense against terrorist and criminal activities and assisting in disaster mitigation. This network would dramatically improve information and intelligence sharing.

---

[140] National Security Agency, *NSA and the Cuban Missile Crisis*; available from http://www.nsa.gov/publications/publi00033.cfm. [cited April 9, 2006].

[141] *9/11 Commission Report*.

4. Environmental Scan

A variety of factors exist that will enhance implementation of DNIN. Those factors (not inclusive) include political will, "buy-in" of Federal government and IC, legal issues (specifically in regard to civil liberties), public reaction to intelligence collection (the recent wire taps performed by NSA are an example), community makeup, geography and culture (will collection processes be perceived as profiling?), whether or not it is an election year, and if another 9/11 type attack occurs. The following strengths, weaknesses, opportunities, and threats (SWOT) analysis provides an overview of DNIN and provides a direction to identify the necessary steps for a strategic plan. These also complement current DHS IA priorities very well.

a. Strengths

- Significantly enhances data collected
- Fosters cooperation, sharing, relationships, and trust
- National in scope
- More likely to detect threat and to prevent via more immediate action
- Reduces stovepipes
- Prevention based
- Operates on need-to-share attitude
- Improves job security

b. Weaknesses

- Cost
- Large scope
- Potential legal issues
- Buy-in from other participants

c. Opportunities

- Capitalizes on ability to amalgamate diverse data from various sources
- Ability to attract large pool of participants (LE)

- Intertwined with public's desire to be safe and perception that terrorist activities will happen
- Intertwined with local, state, tribal, and Federal LE agencies' collection abilities and HS goals

d. Threats

- IC
- Political demeanor
- Policy issues
- Database misalignment

5. Input – Output – Outcome

Long-standing barriers have existed among LE agencies, the IC, public safety, and the private sector for years. The need to prevent terrorist and criminal activities and to prevent and respond to national crises is a priority, especially since 9/11. DNIN represents an efficient intelligence-sharing network that can rapidly share information on a national basis. Successful intelligence collection must focus on outcomes, which begins with where we wish to go; for DNIN, this is improved intelligence collection on a national scale. The specific goals/outcomes for DNIN would be those listed in the mission statement above, but which can be further simplified into various components. The alternative means of obtaining the desired outcome is to obtain the outputs. The actions (activities) necessary to achieve the various outputs must be considered (as listed below). A measurement of the inputs would yield the dollar amount necessary to achieve the outcomes. If the actions to get to an output that leads to an outcome are too costly, then another output that leads to the same outcome can be considered. For many projects, especially one on the scope and scale of DNIN, a major reason behind the struggle of implementation is because, while the entity can control inputs (invest x $), actions (planning and construction of an intelligence-collection center), and to some degree outputs (enhance collection as an example), it cannot control the outcomes (illustrated in Figure 18). The outcomes to which DNIN is supposed to contribute include increased data collection, improved cooperation and information flow, and a more rapid response. The mission must justify the outcomes of any organization and the

reason for the investment of public/private dollars. In the case of DNIN, the outcomes are significant and therefore, warrant the investment.

The International Police Organization (Interpol) is an excellent example of how improving collection capacities can affect terrorism efforts and the apprehension of terrorists, drug traffickers, and other criminals. Interpol demonstrates how networking with its 184 member countries can fight crime. Although Interpol rarely makes headlines, in the last half-decade it has frequently been the puppet master behind some stunning feats of international law enforcement. Last year alone (2005), Interpol's efforts led to 3,500 arrests, including the capture of one of the world's most wanted war criminals and assailants in the Madrid train bombings and London subway attacks.[142] Interpol was created during World War I and is probably better known for chasing art thieves, but as it happens, Interpol is well suited to counter-terrorism work.

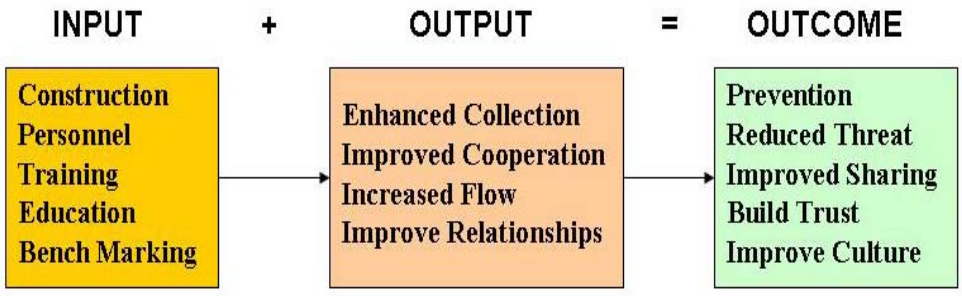


Figure 18. Illustration of inputs, outputs, and outcomes.

Interpol does not have secret agents, and it cannot make arrests; it is and always has been an investigative support network that collects, analyzes, and disseminates information to law-enforcement personnel in its member countries.[143] During the past 5 years, Interpol has gotten better at connecting the dots. In 2002 it introduced a high-tech global police communications system (call I-24/7), which lets member countries instantly send alerts about terrorists, missing person, and various threats around the globe and

142 Rebecca Ulam Weiner, "To Protect and Serve the World,"*Boston Globe*, February 12, 2006; available from http://www.boston.com/news/globe/ideas/articles/2006/02/12/to_protect_and_serve_the_world/. [cited April 19, 2006].

143 Ibid., 2.

provides access to databases containing millions of criminal records, DNS profiles, fingerprints, and intelligence reports. Advances in technology have driven this process significantly, and the U.S. Government has been influenced and impressed enough to back a 50-percent increase in Interpol's budget for the last 5 years.[144] As an example, in December 2005, this system helped end a four-year manhunt for one of the world's most wanted war criminals, the former Croatian Army General Ante Gotovina, who was captured at a luxury resort in the Canary Islands. The database continues to grow as each of the 184 member countries continually adds new data. The arrest of Gotovina is a tribute to this network of world police. Additionally, Interpol created a Fusion Task Force in 2002 to identify active terrorists groups, share information and intelligence, provide analytical support, and enhance response to terrorist and criminal threats. Input into this registry from member countries during the last five years has increased 400 percent.[145] The goal is similar for DNIN, to incorporate data from all IC and LE groups nationwide to grow a comprehensive intelligence database.

Although it is difficult to extrapolate these numbers to DNIN and the 18,000 LE agencies within CONUS, the development of DNIN and effects in the sharing process should be nothing less than phenomenal in comparison to Interpol. Why? First, because DNIN is region to region, and a national database should be more easily accessible; thus, the structural differences between members of Interpol in terms of criminal justice procedures would be greatly minimized. Second, systemic differences in culture and differing rules of criminal procedure utilized by multiple countries, which DNIN would not encounter to any moderate degree, would enhance success. Third, cultural differences that influence policy, prevention, and enforcement priorities should be similar within the U.S. and, therefore, DNIN and should help to foster better success, likely at least threefold or more above the success Interpol has enjoyed. Further, in a strategic sense, the influence of organizations would be greatly enhanced in the police and public security sector, and the repatriation of personnel from the regional centers of DNIN and

144 Weiner, "To Protect and Serve the World."

145 Ronald K. Noble, "Speech by Interpol Secretary General Ronald K. Noble" (paper presented at the Americas Regional Workshop on Preventing Bioterrorism; Santiago Chile, July 10, 2006); available from http://www.interpol.int/Public/ICPO/speeches/SGBioterrorism20060710.asp. [cited May 1, 2006].

.

the knowledge they have gained would improve the cosmopolitanization in key areas of their respective organizations and between other LE groups.

6. Specific Action Plan

The planning for terrorist attacks and other criminal activities spans countries, regions, and states. Fighting such a network will require the same level of effort and cooperation among LE and intelligence agencies, which is becoming more significant with the rise in scale and sophistication of the adversary. The principal roles and responsibilities of DNIN would therefore be:

- Collection and dissemination of pertinent intelligence and information from the local to regional to national scale.
- Analytical support.
- Terrorist and organized crime[146] identification, monitoring, and threat assessment.
- Solicitation of input/output parameters and data storage for a national criminal/terrorist database.
- Development of new strategies/initiatives to continually improve the process and enhance capacity of member agencies to address terrorist and other threats.

Because terrorist and criminal groups have far-reaching activities and are inextricably linked via technology, DNIN members would investigate attacks, organizational hierarchies, training, financing, methods, motives, and other parameters.

7. Budget

The budget exhibited in Table 2 is based upon conversations with personnel at various state intelligence fusion centers throughout the U.S., including, but not limited to, the Virginia State Police Fusion Center, Arizona Fusion Center, LA TEW (Terrorist Early Warning), and Georgia Fusion Center. The costs and staffing to run these facilities were extrapolated to a regional scope based upon economies of scale and the authors personal management experience as a Vice President and also as a Chief Technology Officer. Initially it was estimated that costs for a regional center would be approximately

[146] Organized crime in this instance refers to drug smugglers and human traffickers across the border, and related groups.

$10 million. Because of economic situations and personnel staffing, building costs are based on leasing rather than new construction, which makes it easier to select a location, obtain the best leasing rates, and focus on areas that may not be directly in an urban population center. Because intelligence is a sensitive issue, Internet technology is based on best practices for a secure operating environment; therefore, connection from center to center and to a regional hub is via a point-to-point connection and access to the Internet from all regional centers is through the central hub (ideally located in Washington, D.C.).

The budget is based on a conservative estimate. Figures are from national averages for software site license agreements, salaries based upon state and Federal pay scales, as well as private sector rates. Building costs for lease are based on an average of five of the regional center geographic locations (New York was excluded because lease space was more than twice the average of the other center locations, which include Los Angeles, Denver, Dallas, Chicago, and Atlanta). The price for the SCIF (Sensitive Compartmented Information Facility) is based upon a real proposal for a 20 x 20 x 8 foot room that can be retrofitted to any leased or newly constructed building, is Tempest rated, and can be moved elsewhere if the facility relocates. Actual costs are significantly less than initially estimated cost. The cost for a central hub that the regional centers would be connected to is $23.4 million including personnel, equipment, and building costs. Considering one potential funding scenario, there are approximately 3,000 police agencies in each of the six regions. A contribution of about $3,400 from each agency or municipality would fund each regional center. An additional $10,000 from each of the 18,000 police agencies across the U.S. would be required to fund the central hub. Although this funding scenario is unlikely, the relatively small funding contribution from each participating agency demonstrates how small the cost would be if spread across participants (this would be comparable to a cooperative). The contribution of currently assigned personnel to the centers from various agencies would significantly reduce center staffing costs. These Figures are relatively small compared to the derived benefits.

8. Implementation (Leadership and Dissent)

- Driving the Plan
- Pilot Initiative – Build on Existing Types
- Consider the Alternatives

The 9/11 attacks were declared the fault of poor intelligence due to lack of sharing key information. In the five years since the attacks little has changed in the way of sharing. The NCTC was established to share information throughout the U.S., but it is composed of Federal agencies and their representatives. Despite the lack of LE cooperation with the IC overall, it is the information collected by LE that should drive this process because they are the greatest collectors of the needed information. The IC, since it collects intelligence primarily from overseas, will likely add little to the overall intelligence collected within the U.S. and will deal with both terrorism and other crimes. Therefore, it is the need for the information that must drive the plan, especially since no one agency is large enough or has enough personnel to collect, manage, analyze, and disseminate the collected intelligence.

Table 2. Regional Intelligence Center Annual Budget (includes LE component costs, not IC costs such as transaction space and so forth).

Item	Number	Cost
Personnel		
Analysts	48	3,628,800
Agents	15	756,000
Administrative	9	396,900
Clearances	72	720,000
Equipment		
Desks	72	82,800
Chairs	72	21,600
Phone	72	14,400
Fax	4	4,400
Sec Fax	4	27980
Computers	72	71,928
Software		43,800
IT		3,500,000
Building		
SCIF	1	93,500
Lease	20000[1]	392,000
Energy	27000[2]	324,000
Phone Services	40[3]	1,000
Miscellaneous		150,000
TOTAL		**10,230,988**

[1]Space listed as total square feet.
[2]These are based on national average of $1.35 per square foot for electricity and gas.
[3]Basic monthly fee – does not include long distance, which is included in miscellaneous.

An example of a pilot initiative would be the Arizona or Georgia intelligence "fusion" centers and perhaps the Los Angeles Police Department TEW. The Arizona and Georgia fusion centers were established after the 9/11 attacks. However, the TEW was actually created in 1996 due to monetary problems and because of the need to share information within an LE venue that could have an impact on fighting crime through pooling valuable resources. DNIN would actually be an extension of these concepts, but on a much larger scale and more dynamic with greater capabilities. The general goal is to create a regional interdisciplinary group in which local, state, and Federal agencies work together to share information and combine resources and to enhance the ability to identify and respond to terrorist threats. Ideally, this interagency approach would allow early response and enforcement by strengthening communication between agencies and facilitating a sharing culture. The result would be a strong and effective network with the ability to identify information that may indicate impending terrorist or other criminal activity, make appropriate notifications and recommendations, and aid in the planning and efficient allocation of resources. As an analogy, it would function much like a large group of first responders to a very large disaster with a central command and control that could quickly and efficiently communicate the need for specific resources to specific events, on the fly as it were.

The alternative to DNIN is to continue the current procedures of sharing information and intelligence between the IC and LE with the same old complaints and results. These complaints have not changed since 9/11 with the main one being the failure of the IC to share information and LE citing a need-to-know. However, because LE will collect most of the information in the DNIN model, it would make sense to empower that entity to share on a wider basis. Doing so would create a need-to-share attitude and would essentially eliminate the cause of non-sharing with the federal groups since the greatest amount of information could be classified as law-enforcement sensitive rather than of a classified type. Enforcement, crime prevention, and terrorism prevention are interrelated. Consequently, if we are to avoid another 9/11-scale tragedy, we must opt for a better system that is networked and capable of delivering information in a timely manner to those who need it most.

The intelligence failures that led to 9/11 have plagued intelligence and law enforcement agencies since the attacks and long before them. Despite attempts to reform, especially by the FBI, little progress has been made in sharing information across the Nation, which should be a cause for grave concern given the sophistication and capabilities of terrorist groups such as Al Qaeda. Sharing problems have caused police departments such as NYPD and LAPD to deploy their own operatives within the U.S. and overseas because they do not want to count on the national IC to provide results. A networked-centric collection is the only way feasible for collecting the desired intelligence and sharing it among all agencies. The sole purpose of DNIN would be to collect, analyze, and share this information from over 800,000 LE personnel and 18,000 police departments within CONUS and thus dramatically extend collection capabilities an estimated hundredfold beyond what currently exists. The strengths and opportunities of DNIN outweigh the weaknesses and can overcome the threats by protecting the homeland against terrorist attack, organized criminal activity, and other crimes or other hazards. This is especially true since utilizing mostly LE intelligence across the Nation, in conjunction with other gathered intelligence, threats from the IC, collection policy issues, and database problems, would be more easily overcome.

The comparison of traditional methods of intelligence collection versus the networked approach of DNIN (Figure 17) illustrates the strong position and benefits of the latter. Using Interpol as a benchmark DNIN would likely outperform that organization by several fold, which is significant since Interpol has become very efficient at connecting the dots and fostering cooperation among LE agencies in 184 member countries. As a result, Interpol has made significant impacts on counter-terrorism, and it is believed that DNIN would parallel this, except at a higher capacity. DNIN would collect and disseminate pertinent intelligence from the local/regional/national scale, provide analytical support, identify terrorist groups, solicit data for input into a unified database, and develop new strategies to enhance the capacity of member agencies to address terrorist and other threats.

The two primary factors that would prevent DNIN from becoming operational would be the cost of the network and the leadership. However, fusion centers such as those in Arizona and Georgia and also the TEW in Los Angeles have met with some

success, and while budgeting problems have arisen, the successes gained have overcome many funding issues. Leadership of the network will be critical; it must be forward thinking and progressive, looking at what can be done rather that what has been done. As for "buy in" by the IC, that may not be necessary since the DNIN would be primarily LE and therefore, under different authority and jurisdiction, and with the powers of arrest. It is envisioned that the IC will come to DNIN and ask for their intelligence, which the FBI is now doing with NYPD's mini-CIA group — ironic how sharing between the latter two groups has shifted. Ultimately, the power of the DNIN should be able to overcome these issues and play a prominent role in intelligence collection and sharing within the U.S.

C. SUMMARY

The strategy of DNIN is to overcome the problems generally associated with intelligence sharing as listed below and replacing these problems with the advantages.

1. Problems

- Scale – National
- Cost
- Stovepiping
- Need-to-Know Attitude
- Specific Agency Culture
- Job Security

2. Advantages

- Credible, Reliable, and Corroborative Information
- Scrubbed Information
- Need-to-Share Attitude
- Memorandum of Understanding (MOU) Agreements
- Reputation
- Relationship Building

The principal roles and responsibilities of DNIN would therefore be to:

- Collect and disseminate pertinent intelligence and information from the local to regional to national scale.

- Provide analytical support.
- Provide terrorist and organized crime identification,[147] monitoring, and threat assessment.
- Solicit input/output parameters and data storage for a national criminal/terrorist database.
- Development of new strategies/initiatives to continually improve the process and enhance capacity of member agencies to address terrorist and other threats.

Because of its networked approach, DNIN would be able to collect more than a hundredfold more intelligence than separate IC agencies and its operational network principles would allow for proper analysis and dissemination of this information, which would make significant progress in intelligence and information sharing within the U.S. and reduce the risk of future terrorist attacks.

[147] Organized crime in this instance refers to drug smugglers and human traffickers across the border, and related groups.

THIS PAGE INTENTIONALLY LEFT BLANK

IX. CONCLUSIONS

A. SUMMARY

Terrorists do not recognize borders therefore the flow of information and intelligence must not either. Additionally, terrorist planning, surveillance, movement and other activities will not all occur in one sector or discipline and because of our open democratic society, acts of terrorism will be more difficult to thwart. A dedicated national intelligence network can help fuse the necessary components to gather the needed intelligence to assist in prevention. The greatest challenge within the United States is achieving security and protecting civil liberties. In certain respects, the greatest threat to the American people is how government efforts will restrict them in pursuit of homeland security. The greatest threat for the government is not being able to connect the dots for that one large disaster such as 9/11. How does the government avert another attack of this nature? Within the U.S., two efforts are going on simultaneously regarding the war on terrorism. There is the LE component, which is more interested in building cases for prosecution and there is the intelligence effort who is more interested in gathering long-term data and following the trail to expose a larger network before capture is attempted. As has been illustrated, the intelligence services missed the 9/11 attack, causing a high price. The primary failure was due to intelligence sharing, which rests upon the lack of relationships among the agencies and their respective personnel, lack of trust, cultural differences, and other factors.

The same problems still exist in terms of sharing intelligence, but due to the large volumes of information, there is a critical need for LE and the IC to cooperate on a national scale. A small version of Britain's MI5 is insufficient for the U.S. due to the sheer scope of our intelligence collection problems, geographic areas, and the differing governmental structures between the two nations. To overcome this problem, the proposed Dedicated National Intelligence Network (DNIN) will allow collection from over 800,000 LE personnel to be joined on a regional to a national level in cooperation with local, state and Federal agencies and with the IC to gather the critical data needed to protect society not only against terrorists, but against all types of organized crime. The current existence of various state fusion centers and several other regional centers are not

sufficient to perform such a task due to poor integration within the IC, lack of a single governing authority, lack of training, and narrowly focused approach compared to the overall intelligence goals of DHS. They also do not share with each other very well due to mutual trust issues, but more importantly, incompatible IT platforms, software issues, and other preventable technical issues. However, such centers should and can be incorporated into DNIN.

The objective of this thesis was to provide a dedicated, national-scale networked approach for gathering and sharing intelligence within the U.S. and the allied methodologies to demonstrate its application and evaluation within this area. This thesis has demonstrated that, given its ability to identify, uncover, map, and measure the interrelationships within and between networks, the network approach offers an alternative approach and technique for information sharing, as well as having utility across a wide array of fields of interest. The network approach offers considerable flexibility and agility in terms of the amount of information collected, level of analysis, level of study, the focus on links (patterns), and the ability to detect hidden threats that are not readily obvious. In certain ways, the very strength of the network approach, i.e., versatility, flexibility, and multiplicity, can create problems in conceptualization and, therefore, limits in application. This thesis draws out some of the key network methodological and analytical components to provide a basic framework to address network-centric intelligence sharing. However, the DNIN will provide the key enabler that DHS Chief Intelligence Officer Mr. Allen spoke of in terms of a national collection and sharing architecture, improve the quality of intelligence analysis across DHS and participating agencies, increase overall intelligence production, promote integration of DHS intelligence, ensure the priorities of DHS within the IC, and increase analytic capabilities. Additionally, DNIN will further strategic goals for border, maritime, anti- and counter-terrorism, and other security and intelligence issues.

The question may also arise as to how current and future fusion centers can be incorporated into the DNIN. The DNIN will ensure compliance and standardization on a national scale, which fusion centers do not have. Although there are guidelines for fusion centers to follow, most are built based on stakeholder “buy in” and are thus, different in compliance standards and are not compatible with each other in many instances. As most

of these may be considered legacy systems, at least current fusion centers, connecting them to the network will be a complex undertaking in regards to budget, coordination, standards, training, and restoration of the network from old to new, but it can be accomplished. Assuming each fusion center has access to the Internet the major problem with incorporation is the intelligence and information within the fusion centers current database(s). Database compatibility has plagued many intelligence collection and dissemination efforts, which is why DNIN will have a compatible database that all users will access based upon security level. To incorporate a current fusion center will require that the center strip the data out of their database and send it to DNIN or, DNIN could extract the data (with permission) using a Web spider. This data will then become part of the larger data stream. Once the data from the fusion centers has been incorporated into the DNIN database, personnel at the center will always be able to access DNIN by connecting to any of the regional centers or the national center and retrieve whatever information they need and are cleared for (they should always be cleared for information they have forwarded to the center). Security can be performed in a variety of ways. A common method is termed 3-Factor ID that incorporates biometrics such as a finger print or iris scan, passwords, and a token fob (a physical key). In lay terms this is known as "something I know, something I have, and something I am" (a password, token fob, and finger print respectively). Thus, the process of incorporating a fusion center or any other intelligence facility is not as difficult as some would indicate, nor is security.

There are those who may consider such incorporation very difficult if not impossible, however, the U.S. Navy, prior to the advent of the Internet, ran a program called OSIS (Ocean Surveillance Information System. This system of intelligence collection and analysis had five to six centers that used teletypes and secure-line communications. OSIS worked exceptionally well because it had standards and followed specific compliance rules. The goal behind DNIN is to operate similarly, but with much increased technology.

It has been shown that society, on a global basis, has entered into an era of networks, and Al Qaeda was among the first to utilize network operational principles. It is therefore likely that the network concept will continue to have an increased impact across many areas of endeavor for either positive or negative purposes. Networking

principles are being brought into play to solve a wide array of social and public problems as well as to generate innovation and profitability. Network analysis, with its distinctive processes and focus on relationships between nodes (people, places, or groups/agencies), provides an appropriate mechanism with which to wage the war against terrorism and organized criminal activity within the United States. Rather than being based on trendy terminology, shallow methodologies and processes, or limited theory, the network approach presents new evaluation tools and processes for those charged with the formation, administration, and evaluation of networked groups that is grounded in science. Networking of intelligence sharing within the U.S. offers the potential for a comprehensive, integrative, interdisciplinary/multi-agency approach that enables analysts and administrators to formulate and work on problems using a common language, analytical framework, and theoretical basis. The DNIN will be agile like our enemies and thus, able to respond very quickly. It will also ensure the priority capabilities of DHS and other IC members for communications at any security level, ensure collaboration and analysis because of its ability to support, search, and interactively share with all participants, and ensure rapid information collection and analysis from a large variety of sources whether criminal or terrorist activity, critical infrastructure protection, mapping and imaging, OSINT, media studies and analysis, or others. Finally, DNIN will focus more resources on combating terrorism and criminal activities, leverage LE and other state, local, and tribal resources, and more importantly, perform secure, real-time collaboration, information sharing, and analysis on a national scale.

B. FINDINGS AND POLICY IMPLICATIONS

The 9/11 Commission argued for intelligence-sharing reform and for a single intelligence czar among its many recommendations so that one single agency does not have all the powers. Unfortunately, the commission did not specifically address the bloated bureaucracy of the 16 intelligence agencies and the cultural differences between them and also the LE groups throughout the U.S. What is needed is not more intelligence bureaucracy, but a streamlining and perhaps privatization of intelligence collection and processing. Only through a network-centric approach, such as that presented, can intelligence information be streamlined and rapidly disseminated to those who need it.

The mere creation of newer intelligence agencies and officials ignores the basic and fundamental problems that include (1) timely collection and analysis; (2) recognition of that one tidbit of information in context with many other tidbits that becomes actionable; and (3) dissemination of critical information on a need-to-share rather than a need-to-know basis.

Any revamping of the U.S. IC must include a serious examination of the U.S. Congress's role in intelligence failures. After all, no organization can be any better than those giving it guidance — this includes not only the President, but Congress as well. An example of this is the mandate given by Congress for the Department of Homeland Security's office of Information Analysis and Infrastructure Protection to collect domestic intelligence in the U.S. into one place. Almost at the same time, the President created what eventually became the NCTC of which DHS IAIP was not a part. While the IAIP has since been split in two parts, the major failure in this case is that Congress did not give DHS IAIP oversight authority to carry out its mission. Further, while the mechanism (IAIP) was created to help expedite sharing by Congress, it was immediately thwarted by the President through creation of the NCTC. Congress has refused to reorganize itself to provide better oversight of the executive branch's anti- and counter-terrorism activities. Further, while there are many components the comprise intelligence sharing and many reasons offered about why it does not work, there are three primary reasons that cause intelligence sharing failure. These include agency culture, security clearances, and ownership. This thesis has proposed that DHS IA take ownership of this network. They have the resources and the Congressional mandate. Additionally, they could also become a clearing house for security clearances on an IC-wide basis, which would greatly improve sharing among the IC and LE.

A networked approach for extracting actionable intelligence for the overwhelming volumes of information that is available is necessary. Counter-terrorism exercises are necessary between both the LE and IC entities because they are the only means, other than an actual attack, to uncover problems associated with prevention and response. While there have been exercises, each one has revealed recurring problems. The recurring problems are in communications, which is the key to effective response in preventing an attack or to the aftermath of either an attack or disaster. The two best

examples of this are the 9/11 attacks and hurricane Katrina, which struck New Orleans, Louisiana in the fall of 2005. In each case, government communications have had significant problems. This failure in communication represents the epitome of the continued lack of information sharing and explains to a large extent the problems with coordination among different governmental agencies and levels within them, particularly the CIA and FBI. The outcome has been lack of sharing, coordination, lack of unity of command, and the transfer of tactical and other critical information up and down the chain of command. Perhaps the real lesson learned is that bloated, ponderous government bureaucracies frustrate the rapid decisiveness and responsiveness necessary for intelligence analysis, information dissemination, and response to terrorist attacks and other hazards. Such a system cannot thwart the asymmetric warfare principles of terrorist and organized criminal groups. A network-centric approach, such as that outlined in this thesis, DNIN, can. However, regardless of the implementation, methodology, or process used to link agencies and share intelligence, ultimately, personnel are the key asset. The human factor is the most essential and cannot be replaced. The better trained the personnel are, the better the intelligence will be.

C. FUTURE RESEARCH ISSUES

Network approaches for sharing intelligence can grow in many areas of research, and there are several problems that will likely plague network analysis. One particular area is the construction of an accurate map of a criminal network, which the analyst must face. Three areas can cause problems with this construction. First, there will be the inevitability of missing nodes and links that will not be uncovered. Second, there is the difficulty of deciding who to include and who to exclude, what is termed fuzzy boundaries. Third, networks, whether terrorist, computer, energy, or other is dynamic and ever changing. The question becomes how to deal with this problem. Additional research issues should include a systematic, comparative analysis of the system representation of terrorist behaviors and their analogies to other complex systems for which network theory has successfully provided insights into system dynamics. Further, the development of a simulation model for terrorist group behaviors would be ideal, tested against case studies, for future predictions to help mitigate threats. Regardless of

the research in question, it should be remembered that simply removing the leader of a group will be of little value regardless of the strength of the relationship of the leader to the group. Another critical priority is how to train an adequate number of skilled intelligence analysts. This training is a worthy and compelling undertaking that will help ensure success of the IC. A blended learning approach utilizing network-based learning via the Internet, as well as in-class instructors and other technology can help reduce training costs and likely increase efficiency and perhaps economy of scale. However, training is beyond the scope of this thesis. The issue of security clearances also needs to be addressed. Because almost all IC agencies and LE use the DoD security-clearance model, the establishment of a clearing house to issue clearances should be studied in depth. Perhaps it would be advantageous for DHS IA to be that clearing house, which could be staffed by personnel from a variety of agencies much like the NCTC. In this manner input from all agencies would assist in developing guidelines that would satisfy all stakeholders so that those cleared could access information as needed. This would create a need-to-share rather than a need-to-know culture.

One final area should be considered for future research — good management practices. As with knowledge management, personnel management may be more critical since the network, in its simplest form, relies on the human factor. This is especially true due to the institutional knowledge drain (loss of experienced personnel due to retirement and unwillingness to serve in Washington, D.C. due to cost and other factors) that is befalling almost all agencies in the Federal government. An example of this would be the national search for the new FEMA director with extensive emergency-management experience due to failures exhibited by former Director Mike Brown during hurricane Katrina; the new Director, R. David Paulison, has 30 years of firefighting experience.[148] The DHS has not been guiltless in this area either, i.e., exhibiting poor management and hiring practices that fail to meet the necessary requirements and qualifications e.g., the new U.S. ICE Director, Julie Myers. During her nomination hearing, Sen. George V. Voinovich (R-Ohio) stated that Myers' résumé indicated she was not qualified for the

[148] CBS News, "Bush Nominates New Fema Director: President Taps Acting Director, R. David Paulison, a 30-Year Firefighter," *CBSNews.com*, April 6, 2006; available from http://www.cbsnews.com/stories/2006/04/06/katrina/main1480711.shtml. [cited July 23, 2006].

job.[149] Despite this public acknowledgement Myers won her appointment. The appointments for Paulison and Myers are in direct contrast — Paulison was chosen due to the catastrophic events of hurricane Katrina and because politicians were lambasted for disaster response during hurricane Katrina thus due to public and political pressure, an experienced candidate was sought (Paulison). Myers appointment appears to be politics as usual and exhibits further poor management and hiring judgment. It is likely that a catastrophic event affecting ICE will result in the same consequences that befell FEMA during hurricane Katrina. Hiring experienced professionals should be mandated. Current hiring practices that place inexperienced staffers in significant positions of authority (Myers as an example) does not progress the goals of homeland security nor does hiring "Hollywood Types" who utilize scenarios from the television series "24" for creativity. A lack of imagination still plaques HS decision makers. While we should be open and embrace diverse input from every stakeholder, there is no substitute for substantial or lifelong experience. Unlike corporate America, HS is not an industry where a mistake can be rectified easily. A poor decision within HS can have fatal and national security implications, which hurricane Katrina exemplifies. To many, especially the taxpaying citizen, as well as experienced DHS managers, these practices are laughable. Such practices will accomplish little for improving overall management and building a strong, cooperative, and collaborative coalition for intelligence or homeland security. This issue is highlighted by a recent discussion with a young, creative, HS staffer. As we discussed the issues regarding technology and the human component within HS, the staffer was baffled when asked how this technology could work with the discussed HS aspects. Further explanation to the staffer about various existing possibilities and solutions were replaced with a look of excitement. The discussion with the staffer revealed that inexperience and lack of maturity within HS can not be replaced by working long hours and/or serving in a position of responsibility for which formal experience is clearly lacking. The costs of living and working in Washington, D.C. does not outweigh the responsibility of DHS and other agencies to hire the experienced, the very best, and the brightest to fill critical management positions. Our lack of imagination was an impetus

[149] Dan Eggen and Spencer S. Hsu, "Immigration Nominee's Credentials Questioned," *WashingtonPost.com*, 2006; available from http://www.washingtonpost.com/wp-dyn/content/article/2005/09/19/AR2005091901930_pf.html. [cited July 23, 2006].

on the 9/11 attacks and response to hurricane Katrina. We reacted by creating a new tool for the GWOT, The Patriot Act. This new legislation streamlined procedures for LE to accomplish tasks that were not probable due to prior rules of conduct; perhaps the same should be investigated within Federal government management hiring policies. Simply stated, a new threat occupies our comfort zone and the rules of engagement must change. This would include modifying Federal agency hiring regulations to promote those who may not be within the grade level required by the current position, increased pay, other issues and the critical need for such positions. This is a very serious issue and should be considered for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

The 9/11 Commission Report. New York: W.W. Norton & Company, 2004.

Akerlof, George A., and Rachel E. Kranton. "Identity and the Economics of Organizations." *Journal of Economic Perspectives* 19, no. 1 (2005): 9-32.

Allen, Charles. *Hearing of the Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee of the House Homeland Security Committee Subject: Examining the Progress of the Chief Intelligence Officer*. 2006. In *Capitol Hill Hearing*, Federal News Service, http://www.fnsg.com.

———. "Written Statement before House Committee on Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment." Edited by Department of Homeland Security: House Permanent Select Committee on Intelligence Subcommittee on Terrorism/HUMINT Analysis, and Counterintelligence, 2005.

Angeli, A.J. De, I. Graham, and L. Coventry. "The Unfriendly User: Exploring Social Reactions to Chatterbots." Paper presented at the Proceedings of The International Conference on Affective Human Factors Design, London 2001.

Armitage, Richard. "Intelligence Sharing and September 11 Attacks." U.S. Department of State. 2002. http://www.state.gov/s/d/former/armitage/remarks/2002/13566.htm.

Arquilla, John, and David F. Ronfeldt. *Advent of Netwar*. Washington, D.C.: RAND Corporation, 1996.

Baker, Stewart. "Wall Nuts: The Wall Between Intelligence and Law Enforcement Is Killing Us." Slate.com, 2003.

Banerjee, Abhijit V. "A Simple Model of Herd Behavior." *Quarterly Journal of Economics* 107, no. 3 (1992): 798-817.

BBC News. "Al-Qaeda 'Claims Madrid Bombings'." BBC News, 2004. http://www.news.bbc.co.uk/2/hi/europe/3509426.htm.

Bearden, Milt, and James Risen. *The Main Enemy: The inside Story of the CIA's Final Showdown with the KGB*. New York: Random House Publishing Group, 2003.

Berkowitz, Bruce D., and Allan E. Goodman. *Best Truth: Intelligence in the Information Age*. New Haven: Yale University Press, 2000.

Best, Richard. *The Intelligence Community and 9/11: Congressional Hearing and the Status of the Investigation*. Edited by Congressional Research Service. Washington, D.C.: National Printing Office, 2002.

Betts, Richard K. "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable." *World Politics* 31, no. 1 (1978): 61-89.

Bowers, Faye. "How FBI Is Remaking Intelligence Functions." *Christian Science Monitor*, 2004. http://www.csmonitor.com/2004/0519/p02s02-usju.html.

Brunner, Borgna. "Hurricane Katrina: A Disaster and Its Catastrophic Aftermath." Information Please, Pearson Education, 2005. http://www.infoplease.com/spot/hurricanekatrina.html.

Chaddock, Gail Russell. 2004. Was There Enough Intel to Act? The Christian Science Monitor, http://www.csmonitor.com/2004/0415/p01s03-uspo.html. (cited February 28, 2006).

Chisholm v. Georgia, 2 Dall 419, 471; McCullock v. Maryland, 4 Wheat 316, 404, 405; Yick Yo Hopkins, Supreme Court of the United States 118 U.S. 356, 370.

Colvin, Marie, Michael Smith, and Sarah Baxter. "Iran Suicide Bombers 'Ready to Hit Britain'."*London Times Online*, 2006. http://www.timesonline.co.uk/article/0,,2087-2136638,00.html.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*. Washington, D.C.: Government Printing Office, 2005.

Cooper, J., E. Nelson, and M. Ronczkowski. "Tactical/Investigative Analysis of Targeted Crimes." In *Advanced Crime Mapping Topics*, 31. Denver: National Law Enforcement and Corrections Technology Center, 2002.

Cutter, S. *Geographical Dimensions of Terrorism*. Edited by T.J. Wilbank. Abingdon, UK: Taylor & Francis, 2003.

Davis, Paul K., and Brian Michael Jenkins. *Deterrence and Influence in Counterterrorism: A Component in the War on Al Qaeda*. Washington, D.C.: RAND Corporation, 2002.

Dee, W.V. "Defense Contractors Must Change to Survive in the 1990s." *Aviation Week & Space Technology* 131, no. 3 (1997): 43-44.

DeMarzo, Peter M., Dimitri Vayanos, and Jeffrey Zweibel. "Persuasion Bias, Social Influence and Unidimensional Opinions." *Quarterly Journal of Economics* 118, no. 3 (2003): 909-68.

Desai, Bunil B. "Solving the Interagency Puzzle." *Policy Review* 2005, no. 1 (2005).

Dwyer, Jim. "Defectors: Reports on Iraq Arms Were Embellished, Exile Asserts." *New York Times*, July 9, 2004.

Eggen, Dan, and Spencer S. Hsu. "Immigration Nominee's Credentials Questioned." *WashingtonPost.com*, 2006. http://www.washingtonpost.com/wp-dyn/content/article/2005/09/19/AR2005091901930_pf.html.

Finnegan, William. "How Is the N.Y.P.D. Defending the City?" *New Yorker*, July 25, 2005. http://www.newyorker.com/fact/content/articles/050725fa_fact2.

Fox News. "Tehran Threatens West with Homicide Attacks." *FoxNews.com*, 2006. http://www.foxnews.com/printer_friendly_story/0,3566,191910,00.html.

Garicano, Luis. "Hierarchies and the Organization of Knowledge in Production." *Journal of Political Economy* 108, no. 5 (2000): 874-904.

Garicano, Luis, and Tano Santos. "Referrals." *American Economic Review* 94, no. 3 (2004): 499-525.

Glees, Anthony, and Philip H.J.Davies. *Butler's Dilemma*. BCISS Working Paper 1, The Social Affairs Unit, 2004. http://www.socialaffairsunit.org.uk/digipub.

Golbeck, Jennifer, Aaron Mannes, and James Hendler. "Semantic Web Technologies for Terrorist Network Analysis." In *Emergent Technologies and Enabling Policies for Counter Terrorism.* Piscataway, NJ: IEEE Press, 2005.

Gunaratna, Rohan. *Inside Al Qaeda: Global Network of Terror*. New York: Columbia University Press, 2002.

Heuer, Richard J., Jr.. *Psychology of Intelligence Analysis*. Langley, VA: Central Intelligence Agency, 1999.

Heymann, P.B. *Terrorism and America: A Commonsense Strategy for a Democratic Society*. Cambridge: MIT Press, 1998.

Jain, A.K., and R.C. Dubes. *Algorithms for Clustering Data*. Upper Saddle River, NJ: Prentice Hall, 1988.

Johnson, Loch K., and James J. Wirtz. *Strategic Intelligence: Windows into a Secret World: An Anthology*. Los Angeles: Roxbury Publishing Group, 2004.

Katzman, Kenneth. *Al Qaeda: Profile and Threat Assessment*. Congressional Research Service, 11. Washington, D.C.: Library of Congress, 2005.

Kennedy, L.W. and C.M. Lunn. *Developing a Foundation for Policy Relevant Terrorism Research in Criminology.* New Brunswick: Rutgers University, 2003.

Kim, W. Chan and Renee Mauborgne. *Blue Ocean Strategy: How to Create Uncontested Market Space and Make the Competition Irrelevant*. Boston: Harvard Business School Publishing Corporation, 2005.

Klerks, P. "The Network Paradigm Applied to Criminal Organisations: Theoretical Nitpicking or a Relevant Doctrine for Investigators? Recent Developments in the Netherlands." *Connections* 24, no. 3 (2001): 53-65.

Krebs, Valdis. "Connecting the Dots - Tracking Two Identified Terrorists." *Orgnet.com*, 2005. http://www.orgnet.com/prevent.html.

Lawrence, S. and C.L. Giles. "Accessibility of Information on the Web." *Nature* 400 (1999): 107-09.

Lazear, Edward P. "Pay Equality and Industrial Politics." *Journal of Political Economy* 97, no. 3 (1989): 561-80.

LeBoutillier, John. "Congress Let Us Down Too." *NewsMax*, September 24, 2001. http://www.newsmax.com/archives/articles/2001/9/24/83522.shtml.

Levine, David I. *Reinventing the Workplace: How Business and Employees Can Both Win*. Washington, D.C.: Brookings Institution, 1995.

Loudon, Kenneth C. and Jane T. Loudon. *Essentials of Management Information Systems: Managing the Digital Firm*. Sixth ed. Upper Saddle River: Pearson Prentice Hall, 2005.

McBryan, O. "Genvl and Www: Tools for Taming the Web." Paper presented at the Proceedings of the First International Conference on the World Wide Web, Geneva, Switzerland 1994.

Meyer, Herbert E. "Connecting the Dots." *National Review*, 2004. http://www.nationalreview.com/comment/meyer200404080954.asp.

Milgram, Stanley. "The Small World Problem." *Psychology Today* (1967): 60-67.

Milgrom, Paul and John Roberts. "Bargaining Costs, Influence Costs and the Organization of Economic Activity." In *Perspectives on Positive Political Economy*, edited by James E. Alt and Kenneth A. Shepsle. Cambridge: Cambridge University Press, 1990.

MSNBC. "Islamic Group Claims London Attack." MSNBC News, 2005. http://www.msnbc.msn.com/id/8496293/.

Murphy, Daniel E. *What Stalin Knew: The Enigma of Barbarossa*. New Haven: Yale University Press, 2005.

National Research Council. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. 339. Washington, D.C.: Government Printing Office, 2002.

National Security Agency. NSA and the Cuban Missile Crises. National Security Agency, http://www.nsa.gov/publications/publi00033.cfm. [cited April 9, 2006].

National Science Foundation. "Data Mining and Homeland Security Applications." Washington, D.C., 2003; available from www.bfrl.nist.gov/PSSIWG/presentations/Understanding_al_Qaeda_Networks.pdf. [cited July 26, 2006].

Nevo, D. and Y. Wand. "Organizational Memory Information Systems: A Transactive Memory Approach." *Decision Support Systems* 39, no. 4 (2005).

CBS News "Bush Nominates New Fema Director: President Taps Acting Director, R. David Paulison, a 30-Year Firefighter." *CBSNews.com*, April 6, 2006. http://www.cbsnews.com/stories/2006/04/06/katrina/main1480711.shtml.

Nichols, John. "Ten Against Patriot Act Reauthorization." *Yahoo News*, March 3, 2006. http://news.yahoo.com/s/thenation/20060303/cm_thenation/165474;_ylt=A86.I0baSwhEWe4AjQ_9wxIF;ylu=X3oDMTB;MHVqMTQ4BHN1ywN5bn1YmNhdA--.

Noble, Ronald K. "Speech by Interpol Secretary General Ronald K. Noble" (paper presented at the Americas Regional Workshop on Preventing Bioterrorism; Santiago Chile, July 10, 2006); available from http://www.interpol.int/Public/ICPO/speeches/SGBioterrorism20060710.asp. [cited May 1, 2006].

O'Connor, T. *Intelligence Gathering and Information*. Rocky Mount: North Carolina Wesleyan College, 2002. http://faculty.ncwc.edu/toconnor/392/spy/terrorism.htm.

Ostrow, Ron. "Case Study: Richard Jewell and the Olympic Bombing." *Journalism.org*, http://www.journalism.org/resources/education/case_studies/jewell.asp.

Pincus, Walter. "Negroponte Cites 'Innovations' in Integrating Intelligence." *WashingtonPost.com*, April 20, 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/04/20/AR2006042001785.html.

Posner, Gerard L. *Why America Slept: The Failure to Prevent 9/11*. New York: The Random House Publishing Group, 2003.

Prendergast, Canice. "A Theory of 'Yes Men'." *American Economic Review* 83, no. 4 (1993): 757-70.

Redd, John Scott. *Statement to the United States Senate*. Washington, D.C.: Government Printing Office, 2005.

Reines, Philippe. "Harman & Chambliss Introduce Homeland Security Intelligence Sharing Legislation." U.S. House of Representatives: Permanent Select Committee on Intelligence, 2002. http://intelligence.house.gov/CaseStudies.aspx?Section=84.

Rhodes, R.A.W. "Putting People Back into Networks." Paper presented at the Australasian Political Science Association 43rd Annual Conference, Brisbane, Australia, September 24-26, 2001.

Sageman, Mark. *Understanding Al Qaeda Networks*. Cambridge: Harvard University, 2005. www.bfrl.nist.gov/PSSIWG/presentations/Understanding_al_Qaeda_Networks.pdf.

———. *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press, 2004.

Sah, Raaj Kumar, and Joseph E. Stiglitz. "The Architecture of Economic Systems: Hierarchies and Polyarchies." *American Economic Review* 76, no. 4 (1986): 716-27.

Sales, Leigh. "Subway Warning: New York on High Alert." *ABC News*, 2005. http://www.abc.net.au/am/content/2005/s1477734.htm.

Selberg, E. and O. Etzioni. "Multi-Service Search and Comparison Using the Metacrawler." Paper presented at the Proceedings of the 4th International World-Wide Web Conference, Boston 1995.

Skaperdas, Stergios. "Cooperation, Conflict, and Power in the Absence of Property Rights." *American Economic Review* 82, no. 4 (1992): 720-39.

Sparrow, M.K. "Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects." *Social Networks* 13 (1991): 251-74.

Strohm, Chris. "Border Intelligence Plan Still in 'Early Stages,' Official Says." *Daily Briefing*, GovExec.com, June 6, 2006. http://www.govexec.com/dailyfed/0606/062806cdpm1.htm.

Terrorism Research Center. "About the Terrorism Research Center." Tampa, 2003.

Tindall, James A. "Deconvolution of Plant Type(S) for Homeland Security Enforcement Using Remote Sensing on a UAV Collection Platform." *Homeland Security Affairs* II, no. 1, Article 4.

USA Today. "Al-Qaeda in Iraq Names a New Leader." *USA Today*, June 12, 2006. http://www.usatoday.com/news/world/2006-06-12-zarqawi-successor_x.htm.

Tremayne, Mark. *Internet Newspapers: Making of a Mainstream Medium*. Austin: Lawrence Erlbaum Associates, 2004.

U.S. Department of Homeland Security. "Homeland Security Information Network to Expand Collaboration, Connectivity for States and Major Cities." *Press Room*, Department of Homeland Security website, 2004. http://www.dhs.gov/dhspublic/display?content=3350.

———. "Press Room: Biographies." Department of Homeland Security, 2004. http://www.dhs.gov/dhspublic/display?theme=84&content=4935.

U.S. Department of Justice. United States of America v. Zacharias Moussaoui.2001 http://www.usdoj.gov/ag/moussaouiindictment.htm.

U.S. Department of State. "Patterns of Global Terrorism." 2003. http://www.state.gov/s/ct/rls/pgtrpt/2003/c12153.htm

U.S. Navy. "Naval Intelligence Operations." *Naval Doctrine Publication 2: Naval Intelligence* (Annapolis: U.S. Navy, 1994).

Verton, Dan. "U.S. Intelligence Community Faces Info-Sharing Overhaul." Computerworld, 2002. http://www.computerworld.com/securitytopics/security/0,10801,74053,00.html.

Wallace, Mike. "Colin Powell on 'Fox News Sunday'." Fox News, 2004. http://www.foxnews.com/story/0,2933,114159,00.html.

Watanabe, F. "How to Succeed in the DI: Fifteen Axioms for Intelligence Analysts." *Studies in Intelligence* 1 (1997): no. 1; available from http://www.odci.gov/csi/studies/97unclass/axioms.html

Wegner, D.M. "Transactive Memory: A Contemporary Analysis of the Group Mind." In *Theories of Group Behavior*, edited by B. Mullen and G.R. Goethals. New York: Springer-Verlag, 1986.

Wegner, T.G., and D.M. Wegner. "Transactive Memory." In *The Blackwell Encyclopedia of Social Psychology*, edited by A.S.R. Manstead and M. Hewstone. Oxford: Blackwell, 1995.

Watts, Duncan J. *Small Worlds: The Dynamics of Networks between Order and Randomness*. Princeton: Princeton University Press, 1999.

Weiner, Rebecca Ulam. "To Protect and Serve the World." *Boston Globe*, February 12, 2006. http://www.boston.com/news/globe/ideas/articles/2006/02/12/to_protect_and_serve_the_world/.

Wikipedia. "Herman Hollerith." *Wikipedia, The Free Encyclopedia,* 2005. http://en.wikipedia.org/w/index.php?title=Herman_Hollerith&oldid=61950396

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Captain Robert Simeral
   Naval Postgraduate School
   Monterey, California

4. Richard Bergin
   Naval Postgraduate School
   Monterey, California

5. Chief Intelligence Officer
   Department of Homeland Security, Intelligence Analysis
   Washington, D.C.

6. Principal Deputy Assistant Secretary for Intelligence Analysis
   Department of Homeland Security, Intelligence Analysis
   Washington, D.C.

7. Principal Deputy Director of National Intelligence
   Office of the Director of National Intelligence
   Washington, D.C.

8. Assistant Deputy Director of National Intelligence for
   Homeland Security and Law Enforcement
   Washington, D.C.

9. Assistant Deputy Director of National Intelligence for Community Support
   Office of the Deputy Directory of National Intelligence for Analysis
   Washington, D.C.

10. Executive Assistant Director, National Security Branch
    Federal Bureau of Investigation
    Washington, D.C.

11. Deputy Secretary
    Department of Energy
    Washington, D.C.

12. Dean Anderson
U.S. DOI
Denver, Colorado

13. Assistant Director in Charge
Federal Bureau of Investigation
Los Angeles, California

14. Captain Michael Grossman
Los Angeles County Sheriff's Department
Los Angeles, California

15. Andrew A. Campbell
CI-CE-CT
Melbourne, Australia

16. Dean, Graduate School of International Studies
University of Denver
Denver, Colorado