NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INCOMPLETE INTELLIGENCE: IS THE INFORMATION SHARING ENVIRONMENT AN EFFECTIVE PLATFORM?

by

Jonathan H. Lewin

September 2012

Thesis Advisor:	Robert Simeral
Second Reader:	Christopher Bellavita

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 2012	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Incomplete Intelligence: Is the Information Sharing Environment an Effective Platform?	5. FUNDING NUMBERS
6. AUTHOR(S) Jonathan H. Lewin	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

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

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

13. ABSTRACT (maximum 200 words)

Gathering and analyzing suspicious activity is a core element in the prevention of crime and terrorism. The Information Sharing Environment (ISE) and the Suspicious Activity Reporting (SAR) program is an attempt to address this issue, but it creates human and systemic barriers to information access—the same barriers that existed prior to 9/11. The SAR program, through its process-related policies, limits critical information from entering the shared space for analysis. These limitations are two-fold: Information must be specifically prepared for submission by a human being who recognizes that a potential nexus to terrorism might exist and decides to act upon this recognition; and, once submitted, each data element must be individually vetted and approved by more human analysts. Removing the dual limitations of lack of complete operating picture (based upon the limited information made available for vetting) and dependence on human frailty will provide a more effective platform for the identification and mitigation of possible pre-terrorist incident indicators. This thesis provides an overview of the SAR program and compares and contrasts it with more mature platforms that better meet their objectives, and provides recommendations on how the ISE/ SAR enterprise can be improved.

14. SUBJECT TERMS Suspicious Activity Reporting, Information Sharing Environment, Fusion Center, Persistent Surveillance, Homeland Security, Intelligence Failure, Human Frailty, Police National Database, FinCEN, Financial Crimes Enforcement Network, Big Data, Common Operating Picture, Situational Awareness	15. NUMBER OF PAGES 91
	16. PRICE CODE

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

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

INCOMPLETE INTELLIGENCE: IS THE INFORMATION SHARING ENVIRONMENT AN EFFECTIVE PLATFORM?

Jonathan H. Lewin
Commander, Public Safety Information Technology,
City of Chicago, Department of Police, Chicago, IL
B.S., Southern Illinois University
M.A., Northwestern University

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 2012**

Author: Jonathan H. Lewin

Approved by: Robert Simeral
Thesis Advisor

Christopher Bellavita
Second Reader

Daniel Moran, PhD
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Gathering and analyzing suspicious activity is a core element in the prevention of crime and terrorism. The Information Sharing Environment (ISE) and the Suspicious Activity Reporting (SAR) program is an attempt to address this issue, but it creates human and systemic barriers to information access—the same barriers that existed prior to 9/11. The SAR program, through its process-related policies, limits critical information from entering the shared space for analysis. These limitations are two-fold: Information must be specifically prepared for submission by a human being who recognizes that a potential nexus to terrorism might exist and decides to act upon this recognition; and, once submitted, each data element must be individually vetted and approved by more human analysts. Removing the dual limitations of lack of complete operating picture (based upon the limited information made available for vetting) and dependence on human frailty will provide a more effective platform for the identification and mitigation of possible pre-terrorist incident indicators. This thesis provides an overview of the SAR program and compares and contrasts it with more mature platforms that better meet their objectives, and provides recommendations on how the ISE/ SAR enterprise can be improved.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CBRN	Chemical/Biological/Radiological/Nuclear
CIA	Central Intelligence Agency
CPIC	Crime Prevention and Information Center
CTR	Currency Transaction Reports
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FIN	Financial Intelligence Unit
FinCEN	Financial Crimes Enforcement Network
GCHQ	Government Communications Headquarters
GEOINT	Geospatial Intelligence
HUMINT	Human Intelligence
IACP	International Association of Chiefs of Police
INI	IMPACT Nominal Index
INT	Intelligence
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISE	Information Sharing Environment
ISR	Intelligence, Surveillance & Reconnaissance
MASINT	Measurement and Signals Intelligence
MIST	Multimodal Information Sharing Task Force
NCIC	National Crime Information Center
NOC	National Operations Center
NPIA	National Policing Improvement Agency
NSI	Nationwide Suspicious Activity Reporting Initiative
NYFD	New York Fire Department
NYPD	New York Police Department
OLAP	On Line Analytics Processing
OSINT	Open Source Intelligence
PDB	Presidential Daily Brief
PNC	Police National Computer
PND	Police National Database

SAR	Suspicious Activity Reporting
SIGINT	Signals Intelligence
SOCA	Serious Organized Crime Agency
UAV	Unmanned Aerial Vehicle

ACKNOWLEDGMENTS

I would like to thank my thesis committee members, Robert Simeral and Christopher Bellavita, for their encouragement, guidance, and inspiration during the course of the development of this project. This effort was inspired by the men and women of the Center for Homeland Defense and Security and was made possible by the generous time provided to me to complete the curriculum and thesis—both by my employer, the City of Chicago, and by my friends and family. It is not an exaggeration to say that my participation in the Masters in Security Studies program was the most rewarding learning experience of my life, and has motivated a re-focusing of my lifelong commitment to making people's lives better with an enhanced emphasis on the exploration of new ideas and an acknowledgement that there is almost always a better way.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. EXECUTIVE SUMMARY

The 9/11 Commission Report identified a key structural failure of the intelligence community, both before and after 9/11, as the organization of national intelligence around the "collection disciplines of home agencies," which makes it impossible to connect the dots due to a lack of integrated information (The 9/11 Commission Report, 2004, p. 408). Gathering and analyzing suspicious activity is a core element in the prevention of crime and terrorism. The efforts of the Information Sharing Environment (ISE) and the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) are an attempt to address this issue, but it creates human and systemic barriers to information access—the same barriers that existed prior to 9/11. The SAR program should be this nation's best effort to prevent another terrorist attack. It should be built upon a foundation that maximizes its potential for success. Best practices from all available sectors should be leveraged to ensure optimal functionality. Key characteristics from reference models that have achieved demonstrable success should be explored and implemented wherever feasible. By exploring how other models do things better, important lessons can be learned that can drive critical improvements to the SAR program.

This thesis demonstrates that, although it has the appropriate goals, the SAR program does not live up to its promise and cannot meet its desired outcomes. This platform did not prevent the Times Square bomber from almost succeeding, in fact, "…the fact that the U.S. was unable to stop this plot earlier, despite sufficient intelligence and knowledge that terrorists have been attempting these types of attacks since 9/11, is nothing to be celebrated" (McNeill, 2010, p. 1) and supports the notion that current information-sharing policies and programs have not yet realized their preventative goals for several reasons.

- The SAR program limits potentially critical information from entering the assessment environment, and this limited flow of information does not adequately encompass the range of information necessary to form the basis for identification of potential pre-terrorist incident indicators effectively.
- The SAR process requires that individual analysts at the agency level assess each piece of potentially critical information to determine whether or not a nexus to terrorism exists, before the information can be shared in the environment. This approach forms a critical point of failure, as the process relies upon the imagination of a single person recognizing the potential value of a piece of information before it can even be considered for further assessment, let alone enter the ISE for use by other follow-on analytics activities.

This thesis argues that the current ISE design limits key information critical to the identification of indicators of terrorist activity from entering the assessment space and does not allow advanced analytics to occur, and unless the design is modified, the efficacy of the platform will remain limited. To improve effectiveness, the ISE must address these shortcomings. More complete information must be provided, and human dependencies must be removed. Successful models in other disciplines and in other places can be used as references. The military's use of comprehensive, multi-mode situational awareness indicators is one such model, in which all available information is available for continuous assessment. The United Kingdom's Police National Database is another, in which a wide-ranging, inclusive, and non-limiting platform allows investigators to see all relevant information from across jurisdictional and geographic boundaries. FinCEN, the Financial Crimes Enforcement Network, is a comprehensive environment designed to identify illegal activity in the financial sector, which contains mandatory submissions from across the banking community. In all these cases, the limiting factor of a human being reviewing and vetting discrete elements of information without understanding potential relevance to situations of which they may not be aware is not present as a point of failure.

Big Data is an emerging computing concept that involves assessing vast amounts of information at scales not previously possible to identify patterns and trends and make connections across these massive amounts of data in ways that would not be possible without access to these large datasets and the tools necessary to exploit them (Dumbill, 2012, p. 37). Big Data describes the exploitation of massive amounts of information to identify patterns from which action can be taken (Brehm, 2012, p. 10). Exploring data analytics capabilities from various sectors, and examining the arena of Big Data and its potential to derive meaning from vast sets of information, will provide the potential for this environment to improve the signal-to-noise ratio that might otherwise exist given the large volume of unfiltered data elements that it comprises. For Big Data to be effective, three things are necessary: Volume (having access to extremely large sets of information), Velocity (the rate at which information enters the assessment space for analytics activities to occur), and Variety (a diverse range of information upon which to perform analytics).

Consider the following:

> A disastrous “bolt from the blue” attack kills thousands; enraged politicians and pundits point fingers; committees gravely recommend changes; a massive reorganization of the nation's security and intelligence organs follows. (Colby, 2007, p. 71)

This environment is the outcome of events that followed 9/11, December 7, 1941 at Pearl Harbor, October 1973 in Israel’s Yom Kippur War, the fall of British Singapore to Japan in 1942, and “even the Roman Senate’s reaction to the… irruption of Hannibal into the Italian peninsula” (Colby, 2007, p. 71). The ISE platform is the latest attempt to redress a modern, yet not unfamiliar, failure of intelligence. The system itself has inherent weaknesses and relies upon the intrinsically biased and potentially flawed capacity of a human analyst, who controls the gates of entry for any SAR submission into the assessment environment. The platform can and must be improved to increase its efficacy.

B. RESEARCH QUESTION

This thesis asks the question: *Is the Information Sharing Environment an effective platform?* To provide a useful answer, a working definition of *effective,* when used in this context, must be provided. To provide a basis for an answer, the intent of the environment itself suggests a useful reference. To avoid another catastrophic outcome, such as the terrorist attacks of September 11, such a model must be able to provide actionable, relevant, timely intelligence from its inputs. The outputs of the model must allow users of the platform to identify, understand, and act on warnings before another catastrophe occurs.

C. METHODOLOGY

This thesis examines the baseline problem space (the ISE) to explore the ideal characteristics that an effective model must encompass to address the problem within the framework of Big Data (the Police National Database, Persistent Surveillance, and the FinCEN), and compare and contrast key characteristics of the ISE with attributes of the reference systems. Chapter IV explains the concept of Big Data (evaluating vast amounts of information using tools to identify trends and patterns that would not be possible without advanced analytical capabilities).

This thesis identifies components of an effective model and contrasts how these differ from the ISE. Persistent Surveillance provides one such model, which is used primarily in a military intelligence context to describe the integration of data largely from sensors and systems, such as satellites, motion detectors, and UAVs (Unmanned Aerial Vehicles), to allow analysts to “rapidly search, correlate, fuse and visualize” across large datasets (Kimmons, 2008). The Police National Database is the United Kingdom’s attempt to integrate a wide range of police databases together to form an information-sharing platform. FinCEN is an outgrowth of the 1970 Bank Secrecy Act and provides perhaps the most mature, robust reference system for comparison—a system designed to assess vast amounts of data to detect indicators of financial fraud and potential terrorist

funding activities. Between 2002 and 2011, FinCEN has supported 378 requests related to terrorist financing and 1,148 related to money laundering activities from local, state and federal law enforcement agencies, with 15,741 persons of interest identified in these requests (Financial Crimes Enforcement Network Annual Report 2011, 2011, p. 51). FinCEN was able to share valuable information with international financial fraud units following the Madrid bombings and the United Kingdom's 2006 discovery of a terrorist plot involving trans-Atlantic commercial airliners, which resulted in "relevant information" involving suspects (Werner, 2006, p. 12).

Chapter II provides background on the Information Sharing Environment and describes how the events of September 11, 2001 represented a failure of the intelligence community to "connect the dots."

Chapter III gives a brief literature review, which notes the general lack of performance metrics or efficacy evaluations of the ISE itself. Little research exists on how the program has performed so far, except for a single report identifying the number of SAR entries for the period 2010–2011. Ample literature exists on how the intelligence fusion process itself should work, as well as some additional literature evaluating the ISE in the context of this framework. Research on the limits of human imagination and its role in intelligence failures is identified, along with work in the area of human frailty.

Chapter IV describes the models that will serve as references for comparison to the ISE: the use of business intelligence and Big Data, the Police National Database in the United Kingdom, the concept of Persistent Surveillance in the military space, and the FinCEN. Since a distinct lack of defined metrics for success with respect to the ISE occurs, some potential metrics are proposed, including the number of criminal terrorist investigations initiated, the number of terrorists identified, terrorists arrested, terrorist cells identified, terrorist plots identified, terrorist plots prevented, and so forth. Key characteristics of effective models are described, and the ISE is evaluated using each of these measures (spoiler: it fails). The ISE is evaluated using a Business Intelligence maturity

model, in which it scores at the low end of both the Business Value and Complexity scales (i.e., it is an immature model). Several illustrative tables are included. One compares the ISE with the Police National Database, and another utilizes the three performance measures of Big Data (volume, velocity, and variety) and compares the ISE with FinCEN. Weaknesses of the ISE are discussed in more depth, including its lack of information and its dependency on people, which leads to a discussion of human frailty.

Chapter V compares and contrasts key characteristics of the ISE with reference models including the Police National Database, the military's use of persistent surveillance, and FinCEN. In key performance areas, these reference models are more mature in their ability to meet desired outcomes. Tables are presented that allow these models to be compared with the ISE. Potential metrics for assessment of the ISE are proposed within the framework of its defined objectives.

Chapter VI presents a conclusion. The ISE is not an effective platform, if effectiveness is defined as meeting the charge of *The 9/11 Commission Report* and the *Intelligence Reform and Terrorism Prevention Act of 2004.* Recommendations are provided, which may be summarized as follows. The ISE needs to become more like the reference models discussed in this thesis—the Police National Database, FinCEN, the military's concept of Persistent Surveillance—and single points of failure need to be reduced or eliminated (removal of human dependencies). Barriers include legal, policy, privacy, and cost issues. To overcome these barriers, a bottom-up approach that uses technology itself to build in appropriate privacy controls and depends upon local and regional fusion centers is proposed, which will help overcome privacy concerns, as a diversification of control and decentralization will occur. This "system of systems" is described as the multi-ISE; a series of databases managed at the local agency level that forms a comprehensive, multi-mode platform that meets privacy and policy guidelines and removes key barriers to efficacy present in the current system design.

II. BACKGROUND

A. DEVELOPMENT OF INFORMATION SHARING ENVIRONMENT (ISE)

The terrorist attacks of September 11, 2001 were the first significant foreign attacks on United States soil in almost 200 years—since the War of 1812, and represented a stunning failure of the intelligence community to "interpret, analyze, and share" information that might have provided pre-incident indicators, or early warnings, prior to the attacks themselves (Chambliss, 2005). *The 9/11 Commission Report* describes a crescendo of intelligence indicators in the months prior to the attacks, with Central Intelligence Agency (CIA) director George Tenet describing the system in the intelligence world as "blinking red," and suggesting that it could "not get any worse" (The 9/11 Commission Report, 2004, p. 259).

Mark Lowenthal suggests that the various post-mortems describing intelligence failures of 9/11 agree on several key points (Lowenthal, 2008, pp. 303–315).

- The intelligence community failed to share information quickly or widely enough, and that stovepipes defined a lack of sharing across agency boundaries, such as the Federal Bureau of Investigation (FBI) and the CIA, partially due to restrictions that prohibited the sharing of such information unless a "need to know" existed and partially resulting from institutional arrogance and a failure of these agencies to get along.
- A "failure to warn," existed, which was characterized by intelligence agencies having information but failing to use it to generate a warning that might have prevented the attacks. A Presidential Daily Brief (PDB) of August 6, 2001, 36 days prior to September 11, is often cited as an example, although it did not specifically mention planes targeting the World Trade Center.
- The famous failure to connect the dots, in which information was available but was not connected. Lowenthal disagrees with the oversimplification of this term, and compares it literally to child's play; a situation in which a child is presented with numbered dots to

> connect, and is easily able to connect them because they are numbered and because exactly enough dots are available to form the desired picture—no more and no less.

What is important for purposes of this section's discussion is not whether or not it was in fact easy to connect the dots, but that the failures described above led directly to the development of the ISE and an attempt to remedy them. The following section describes the environment.

B. DESCRIPTION OF INFORMATION SHARING ENVIRONMENT

The ISE is sponsored and funded by the Office of the Program Manager of the Information Sharing Environment, established under the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). This environment is designed as a "low risk approach for testing and evaluating ISE policies, business processes, capabilities, architectures, and standards by sponsoring efforts that implement and evaluate solutions to operational needs in a relatively controlled environment" (Nationwide Suspicious Activity Reporting Initiative Concept of Operations, 2011, sec. 5.1).

1. Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)

In December 2008, the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Concept of Operations was published and described the suspicious activity reporting information gathering, processing, analytics, and production cycle (Final Report: Information Sharing Environment Suspicious Activity Reporting Evaluation Environment, 2010, p. 13). This process is depicted in Figure 1 (Final Report: Information Sharing Environment Suspicious Activity Reporting Evaluation Environment, 2010, p. 14).

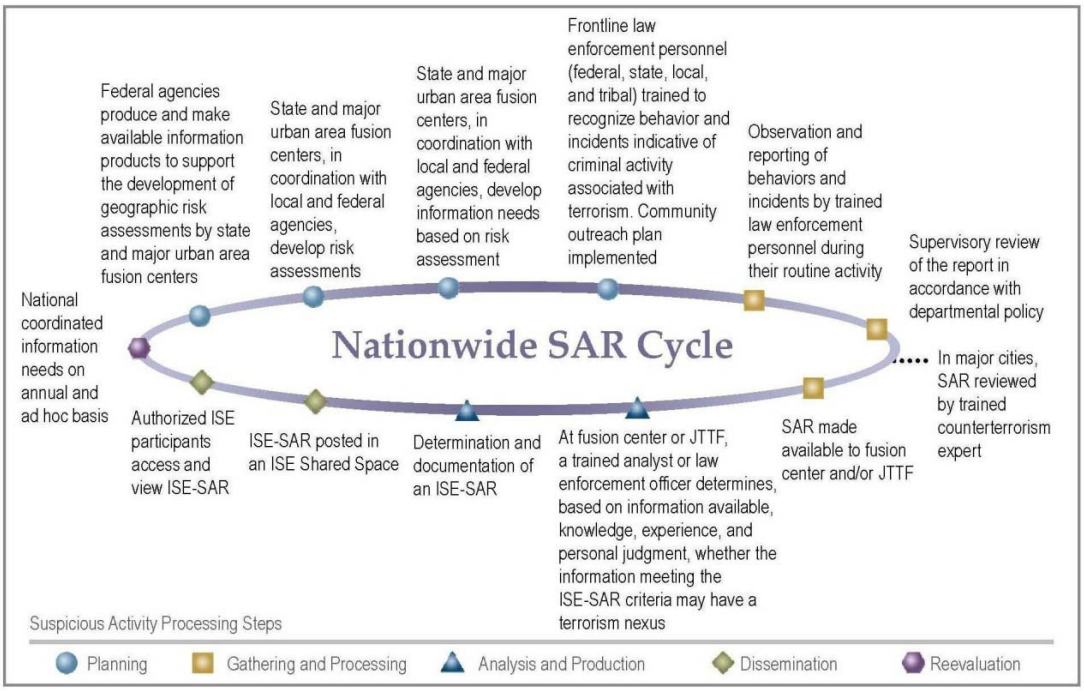

Figure 1. Nationwide SAR Cycle

As noted above, front-line personnel at federal, state, and local law enforcement agencies receive training to recognize and identify behavior and incidents indicative of criminal activity associated with terrorism and a trained expert then reviews this information to confirm a possible nexus to terrorism. To share information with external agencies in the ISE platform, a law enforcement officer must determine that suspicious activity that might have a possible connection to terrorism has been identified. That information must then be submitted to the state or local fusion center. An intelligence analyst must review it to determine if it meets the criteria for sharing. Presuming the analyst makes the determination that the activity meets the criteria for submission; it is entered into the information-sharing environment and can then be accessed by human analysts for possible connection with other intelligence information (Bjelopera, 2010, p. 8).

Figure 2 is a representation of the current process (which is “Single Mode,” or reliant upon only one input source), and the preferred environment (which is “Multi Mode,” or reliant upon a comprehensive set of input indicators).

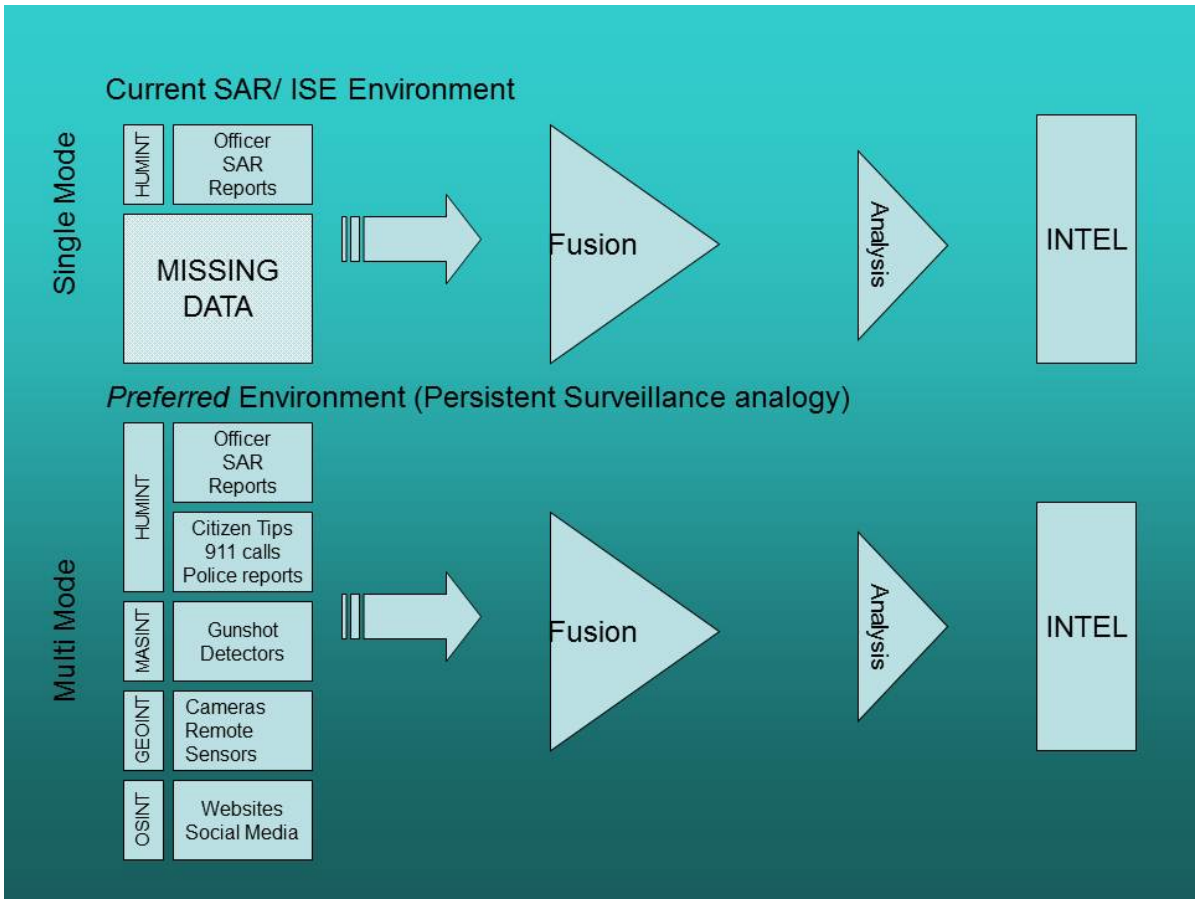

Figure 2. Current vs. Preferred ISE/SAR Environment

The general steps in the intelligence process are as follows.

1. Requirements
2. Collection
3. Processing and exploitation (“fusion”)
4. Analysis and production
5. Dissemination
6. Consumption
7. Feedback

The SAR program depends upon two limitations that create a problem of human frailty. One is that a human being must become aware of “suspicious activity” and decide that it is suspicious and needs to be reported and then report the activity. The second is that a human being at a fusion center must review the reported activity and determine that this activity has a nexus to terrorism and thus should be pushed to the (ISE for review and analysis. Consequently, , human frailty limits the effectiveness of the platform.

An effective model will remove human frailty at one or both of these stages. For example, more information available to the second-level fusion center reviewer would create a more comprehensive “common operating picture,” available in the form of analytical data aggregation products, such as maps, dashboards, and other visualization and inquiry tools, and would solve the problem of depending upon a human being to determine that a single, possibly discrete component of information rises to the level of suspicious activity that needs to be documented. In this alternative approach, the fusion center analyst would have access to real-time or near real-time information from source systems (such as incident reports, arrest reports, calls for service, and documentation of suspicious activity stops) from which to assess information by using analytics tools to perform more effective analysis.

Another alternative solution would involve providing common operating picture information from across multiple jurisdictions to a national fusion center, in which analytics could occur across a wider range of potential indicators to identify patterns of activity that might be crossing jurisdictional boundaries and would otherwise be undetectable. Criteria to judge existing policies might include a number of investigations initiated based upon SAR submissions (potentially with a review of their outcomes) and an assessment of how existing policies would have worked to identify earlier terrorist plots (i.e., 9/11 or previous World Trade Center bombing or foiled plots. As a recent (December 2011) Congressional Research Service report suggests, it is difficult to determine whether or not the SAR program is successful. Are the number of SARs

produced/shared relevant metrics, how can one determine if the SARs produced and shared are meaningful, and how can one determine if the correct connections are being made across reports (Bjelopera, 2010, p. 17). Characteristics of the SAR program are compared and contrasted with characteristics of more effective models.

The purpose of the ISE is to provide the "right information to the right people in time to prevent terrorist attacks" by providing access to the necessary information from the multiple and often disparate systems at the local, federal, and state levels (Paul, 2010, p. 36). To achieve this goal, the SAR process follows the traditional intelligence cycle: (1) requirements, (2) collection, (3) processing and exploitation, (4) analysis and production, (5) dissemination, (6) consumption, and (7) feedback (Lowenthal, 2009, p. 66). The initial process challenge is in the collection phase, in which a lack of control and consistency exists in the quality and type of information being collected and submitted into the environment. Under the current SAR protocol, this thesis argues that requirements process is too restrictive to allow for the volume of information to enter the assessment space.

2. Submission Characteristics

A SAR submission might be useful in two ways. One is the "direct" approach, in which a specific report itself is a clear indication of a terrorist threat, and this indication is apparent to each reviewer at each stage in the process: The collector (i.e., the police officer), the processor (i.e., the system collecting and transmitting the information), the analyst, and the process for proper dissemination. In this ideal approach, the system works as designed. Unfortunately, this happens very rarely. For example, in 2009–2010, the FBI reported that 3,400 SAR submissions were entered into the system (FBI—Connecting Dots with EGuardian, 2008), with only 56 of them (2%) meriting an investigation (Straw, 2010).

The “direct” approach further presumes that the law enforcement officer and the analyst have the foresight to determine that one piece of information, at the time it is identified and analyzed, might have a nexus to terrorism—or, to quote the National Strategy for Combating Terrorism from the Bush Administration, that “…[i]nformation acquired for one purpose, or under one set of authorities, might provide unique insights when combined… with seemingly unrelated information from other sources” (NSIS—Introduction and Overview, 2011). Presuming these participants have such foresight, the entity responsible for dissemination must also come to the realization that the information is important enough to be distributed, and then must distribute it to the right recipients, all of which must happen in the correct sequence and with the proper timing to prevent an event or events from occurring.

The second way a SAR submission might be useful provides insight into the great potential of the system: The “indirect” approach occurs when data analytics is used to identify unusual occurrences in baseline data automatically. For this to work, the system must have access to a “huge, relatively consistent, and comprehensive [dataset] to ensure robust analysis” (Steiner, 2010). In the intelligence community, this problem is known as “noise versus signals” or “wheat versus chaff,” which is the notion that the important information is often buried within a large amount of “noise” (Lowenthal, 2009, p. 72).

3. Desired Outcome

The formal, stated goal of the ISE is to comply with IRTPA, which requires the President to establish an ISE “for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties,” and which provides a very broad mandate with the following requirements, as quoted directly from the Act itself (Intelligence Reform and Terrorist Prevention Act of 2004, 2004):

(2) ATTRIBUTES.—The President shall… ensure that the ISE provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. The President shall, to the greatest extent practicable, ensure that the ISE provides the functional equivalent of, or otherwise supports, a decentralized, distributed, and coordinated environment

that—

(A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;

(B) ensures direct and continuous online electronic access to information;

(C) facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations and operations;

(D) builds upon existing systems capabilities currently in use across the Government;

E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;

(F) facilitates the sharing of information at and across all levels of security;

(G) provides directory services, or the functional equivalent, for locating people and information;

(H) incorporates protections for individuals' privacy and civil liberties; and

(I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls…

(4) TERRORISM INFORMATION.—The term ‘‘terrorism information’’ means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

(A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals

involved in transnational terrorism;

(B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;

(C) communications of or by such groups or individuals;

or

(D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

The latest (2011) ISE Annual Report to Congress reiterates the objectives as outlined in the Act and highlights recent emphasis on work in the area of developing a governance structure to establish standards for data sharing, create baseline capabilities for fusion centers, and enhance information sharing across public and private sectors. It also presents a broad definition of the ISE itself as “infrastructure and capabilities,” which extends the parameters of the environment and includes many such capabilities not directly accessible from the ISE assessment space, a notion that is reinforced by several examples given of potential use cases, one of which involves a police officer using the National Crime Information Center (NCIC) to conduct a query, the results of which direct the officer to contact the Terrorist Screening Center to assess a potential match against the terrorist watch list; while another example depicts an intelligence analyst utilizing the Library of National Intelligence to develop new intelligence

products (ISE Annual Report to the Congress, 2011, p. 3). Not all these systems are part of an integrated, searchable database, as the first example notes, an officer has to utilize one system (NCIC) and then is referred to another.

C. CHAPTER SUMMARY

This chapter provided background on the development of the ISE, which was recommended following the intelligence failures that preceded 9/11. These failures related to a failure on the part of the intelligence community to share information with each other, a failure to warn, or act upon information that these agencies possessed; and the famous failure to "connect the dots" across available data points. The ISE and SAR NSI were described, along with an overview of the seven-step intelligence cycle (requirements, collection, processing and exploitation, analysis and production, dissemination, consumption, and feedback). The SAR NSI's exposure to human frailty was identified as a barrier to the program's effectiveness. An effective model must remove this human weakness where possible. Instead of limiting information from entering the assessment environment, fusion center analysts need access to a wider range of indicators than just SAR submissions. When examining the seven-step intelligence process, the current SAR protocol is too restrictive in the requirements process.

III. LITERATURE REVIEW

A. BACKGROUND

The first topical literature describes the ISE itself and provides a rationale and basis for its development, and discusses a key information source for the ISE, Suspicious Activity Reports (SAR). The foundational document for the ISE is probably *The 9/11 Commission Report,* which framed the failures that led to 9/11. It identified a key structural failure of the intelligence community, both before and after 9/11, as the organization of national intelligence around the “collection disciplines of home agencies,” which makes it impossible to connect the dots due to lack of integrated information (The 9/11 Commission Report, 2004, p. 408). Therefore, this report is the key motivation for the development of the ISE.

Various publications describe the goals of the ISE and provide an overview and assessment of implementation efforts to date (Final Report: Information Sharing Environment Suspicious Activity Reporting Evaluation Environment, 2010, p. 13). A Concept of Operations document outlines sponsorship and funding of the ISE, which is administered through the Office of the Program Manager of the Information Sharing Environment, established under IRTPA. This environment is designed as a "low risk approach for testing and evaluating ISE policies, business processes, capabilities, architectures, and standards by sponsoring efforts that implement and evaluate solutions to operational needs in a relatively controlled environment" (Nationwide Suspicious Activity Reporting Initiative Concept of Operations, 2008, sec. 5.1). By definition, this document embraces the components and framework of the ISE and does not consider the possibility that the foundation itself might be built upon incorrect assumptions. What if the entire concept of operations itself is flawed?

In *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress,* Jerome P. Bjelopera of the Congressional Research Service provides additional background on the

intent in a report to Congress, in which he describes how the process is designed to work. Another report to Congress, this time from the Program Manager of the Information Sharing Environment, the *Information Sharing Environment Annual Report to Congress* (most recently from 2011) provides a good general background on the ISE and its state of readiness, at least as of the latest report in 2011. The report describes the purpose of the platform, to provide the "right information to the right people in time to prevent terrorist attacks" by providing access to the necessary information from the multiple and often disparate systems at the local, federal, and state levels (Paul, 2010, p. 36).

Mark Lowenthal's work on the intelligence community is widely respected and frames a central expert narrative. His work makes it easier to understand how the SAR process should work in the context of the intelligence cycle: (1) requirements, (2) collection, (3) processing and exploitation, (4) analysis and production, (5) dissemination, (6) consumption, and (7) feedback (Lowenthal, 2009, p. 66). According to Lowenthal, the initial process challenge is in the collection phase, in which a lack of control and consistency exists in the quality and type of information being collected and submitted into the environment.

Little research is available on how the SAR program has worked so far, with the exception of information published by the FBI. In 2009–2010, the FBI reported that 3,400 SAR submissions were entered into the system (FBI, 2008), with only 56 of them (2%) meriting an investigation (Straw, 2010). Additional literature review is necessary in this area. In 2011, the International Association of Chiefs of Police (IACP) conducted a meeting of local, state, and federal partner agencies to support a unified strategy in support of the SAR initiative. This strategy focuses on increasing public awareness of SAR reporting to law enforcement, SAR report generation by law enforcement, analysis by fusion centers and Joint Terrorism Task Forces, and appropriate investigations. The strategy also includes emphasizing training for frontline officer training on the need to identify and report indicators of suspicious activity (Nationwide SAR Initiative, n.d.a.). An Activity Overview describing the Department of Homeland

Security/Department of Justice Technical Assistance Program for fusion centers places a heavy emphasis on training and enhancing critical thinking skills (DHS/DOJ Fusion Process Technical Assistance Program and Services Activity Overview, 2012). The 2011 Nationwide SAR Initiative Annual Report suggests an increase in the number of SAR submissions compared to previous years; over 17,000 as of March 2011, which supported 43,000 inquiries using a relatively simple search tool that supports user-generated inquiries as part of the environment (Nationwide SAR Initiative, n.d.b.). However, this report is silent on the number of investigations initiated because of these 17,000 submissions and does not make qualitative conclusions about their value, aside from reporting some anecdotal success stories.

James E. Steiner retired after 36 years with the Central Intelligence Agency. He worked in the area of national intelligence, and now teaches at the State University of New York at Albany. In an article in the *Homeland Security Affairs Journal*, he argues that for a SAR submission to be useful in an "indirect" way, the system must have access to large amounts of information to identify unusual occurrences in baseline activity (Steiner, 2010). This argument supports Lowenthal's notion that important information is often buried within a large amount of noise (Lowenthal, 2009, p. 72).

Lowenthal provides background on the intelligence process. According to his work, at the stage of initial collection, information is not yet intelligence. Rather, it is a component of the collection phase that is then analyzed and results in intelligence. Nestor Duarte, an intelligence professional from the FBI and graduate of the Naval Postgraduate School, provides research insights into the foundation of prevention and the requirement to collect a wide range of information concerning people who have not yet committed terrorist acts, in a well-researched thesis (Duarte, 2007, p. 17).

Part of the problem is that the ISE does not allow the full range of information to be assessed. The notion of Persistent Surveillance as it exists in the military world is discussed by Lieutenant General and Deputy Chief of Staff of

the United States Army John Kimmons in a journal article describing the integration of indicators from a wide range of sensors and systems (Kimmons, 2008) and Major David W. Pendall (also of the U.S. Army) in another article presenting a description of this continuous collection and assessment process.

The failures of human decision making, or human frailty, is also explored. Significant challenges occur when relying upon this human process to make the correct determination that a piece of information should be shared. In the 2008 Mumbai attacks, fishermen reported the arrival of the terrorists to local police, who did not act upon or share the information. According to reports cited in a RAND publication, the CIA and FBI did not share information that Khalid al-Midhar and Nawqa Alhazmi, two men with connections to terrorism, had entered the United States prior to 9/11 (Hollywood & Pope, 2009, p. 5). Perhaps, this lack of sharing information occurred because, at the time the information became available, its significance was not known.

In an article entitled, “Suspicious Activity Reports: Shifting the Analytical Paradigm,” Rafael Brinner (a Department of Homeland Security (DHS) Liaison Officer to the Northern California Regional Intelligence Center) discusses the risk of placing too much emphasis on SARs in the absence of better threat intelligence. The article also describes SARs as anecdotal information that the reporter deemed suspicious “on some level” (Brinner, 2011, p. 2), which is consistent with the notion that the ISE places too much reliance on SARs from which to connect the dots, and thus, these subjective reports receive artificially high levels of attention.

Researcher Gustavo Diaz, a fellow at the University of Madrid, presents a discussion paper in which he describes Michael Handel as a student of intelligence failure, who feels that the principal cause of such failure is the “limitations of human nature,” and most failures occur because decision makers fail to adapt their concepts to new information (Diaz, 2005). This human dependency must be removed. This review is expanded to explore more fully the notion of human failure, both in the intelligence space and in larger related

endeavors. Susan G. Hutchins (of the Naval Postgraduate School), Peter L. Pirolli, and Stuart K. Card (both of the Palo Alto Research Center) authored the chapter, “What Makes Intelligence Analysis Difficult?: A Cognitive Task Analysis” in *Expertise Out of Context: Proceedings of the Sixth International Conference on Naturalistic Decision Making.* In this chapter, they highlight the problems faced by intelligence analysts, who must sort through “enormous volumes of data” to combine seemingly unrelated events to develop intelligence, often under periods of intense pressure and time constraints (Hoffman, 2007, pp. 281–282).

Dr. Fathali Moghaddam describes the notion that humans are predisposed to certain ways of viewing the world, and these “constructs” impact the way information streams are processed (Moghaddam, 2001, pp. 29–31). In *What Makes Intelligence Analysis Difficult?: A Cognitive Task Analysis*, the authors conducted a study of the cognitive challenges associated with intelligence analysis, and identify a number that falls within the scope of human frailty (Hutchins, Pirollo, & Card, 2007, pp. 298–304). In *Black Swan*, Taleb discusses the “highly improbable consequential event” (Taleb, 2007, p. 18), and the difficulty humans have in identifying something that they do not expect to happen. Dan Ariely, the noted Israeli professor of psychology and behavioral economics, challenges the entire concept of human rationality in a compelling Ted Talk in which he discusses that sometimes when faced with too much complexity, humans simply do not do anything (Ariely, 2008).

An optimistic report entitled “Vision 2015: A Globally Networked and Integrated Intelligence Enterprise” describes a vision for what the ISE needs to become—that it should more closely align with the concept of persistent surveillance by removing the restrictions on information entry and adding appropriate technologies and capabilities to the environment to improve its potential effectiveness. The current ISE, by definition, requires that the evaluator determine the potential criticality of a piece of information within the framework of that person’s current understanding of the threat environment, which does not contemplate “weak signals” and indicators of new and emerging threats that will

require an ability to assess global risks and the use of a more interactive model that blurs the distinction between the information producer and the information user, as described in a “best case” visioning document from the Director of National Intelligence published in 2008 and still operative, which describes a vision for the year 2015. This vision will not be realized if the arguments in this literature review and subsequent thesis are correct (Vision 2015: A Globally Networked and Integrated Intelligence Enterprise, 2008, p. 9).

The use of business intelligence in the commercial arena, including prediction and analytics, in risk modeling (Bamberger, 2010), fraud detection (Malphrus, 2009), medical diagnostics (Wernick et al., 2010, pp. 25–38), sales and operations planning (Lapide, 2004), banking (Graves, 2011), and other fields is well documented. One directly relevant process is suspicious activity reports in the banking sector, in which machine models detect unknown patterns for fraudulent use of credit cards using real-time data for assessment (Widder et al., 2007).

Less literature is available in the role of data mining for counterterrorism, primarily because this segment is less mature than private sector uses of this capability. The Cato Institute concluded that data mining is not ideally suited to this problem (Jonas & Harper, 2006). Other work by Colonel Brett Weigle of the U.S. Army War College explores the possibility of using “prediction markets” to aggregate information from disparate sources to develop possible leading indicators towards future terrorist events (Weigle, 2007). Three years before 9/11, the CIA described data mining as “vital” to support the intelligence community’s ability to identify future threats as outlined in a *Jane’s Defense Weekly* journal article (Starr, 1998). An excellent summary document from the Congressional Research Service by the technology analyst Jeffrey Seifert outlines the role of data mining in homeland security, which describes some of its current uses in the anti-terrorism arena, as well as challenges in data quality and interoperability (Seifert, 2007).

An emerging area of Predictive Policing involves "…taking data from disparate sources" and using analysis techniques to predict and respond to outcomes based upon this data, as published by the National Institute of Justice (Pearsall, 2010). Chicago is one of a handful of U.S. cities to receive the second phase of a National Institute of Justice Predictive Policing grant, and initial and secondary grant application materials, along with anticipated early project results from the second phase of this project, is used to inform the development of this thesis (Chicago Using Predictive Analytics to Fight Crime, 2010). Some best practices in the use of law enforcement technology include Chicago's fusion center (the Crime Prevention and Information Center, or CPIC), which is described in various reports (Harris, 2008), and Chicago's early and current use of technology (Technology Update, 2007), beginning with an automated crime mapping platform developed in the early 1990s as documented in a National Institute of Justice Report (Rich, 1996).

A great wealth of industry reports exist from commercial research providers, such as Forrester, in which senior analyst James Kobielus conducted an evaluation of vendor-specific solutions and assessed trends in this space (Kobielus, 2010). Numerous workshop proceedings, presentation summaries, and industry reports provide an overview of best practices in the use of information indicators to make predictions.

A breadth of information on the reference models is discussed in Chapter IV, including the Police National Database that was mandated as a result of a non-terrorism related murder of two schoolgirls as described in report that acknowledged the failure of police systems to share information across jurisdictional boundaries (IMPACT Programme: Police National Database Privacy Impact Assessment Report, 2009, p. 6). Bruce Berkowitz describes the use of technology in facilitating the military's use of Persistent Surveillance. The FinCEN is well described in various official publications, and a wide range of performance data exists on the system (Financial Crimes Enforcement Network Annual Report 2011, 2011).

Big Data describes the exponential growth and availability of vast quantities of information, and a variety of industry research publications and the White House itself identify its potential to lead to innovation within organizations (Big Data, 2012). In March 2012, the White House announced a $200 million funding initiative designed to improve "…our ability to extract knowledge and insights from large and complex collections of digital data… to help solve some of our Nation's most pressing problems" (Executive Office of the President, 2012). This effort announced a series of grants to various agencies, ranging from the National Science Foundation to the Department of Energy to the Department of Defense: but no Department of Homeland Security nor Department of Justice projects were identified, unfortunately. When examining Big Data and Business Intelligence (which is critical to "connect the dots" if they are available in the assessment environment to connect), a wide range of models and descriptions of required characteristics for success is necessary, such as Eckerson's Spectrum of BI Technologies (Eckerson, 2012, p. 5) that presents a Value and Complexity Scale for scoring the maturity of various intelligence capabilities (as one might expect, the ISE scores very poorly on this scale). A journal article by Calvert Jones discusses the need to provide access to information from as many sources as possible (Jones, 2007, p. 385) and to have comprehensive data to avoid being caught off guard (Jones, 2007, p. 387). In a report on how to plan for Big Data (entitled, not surprisingly, "Planning for Big Data"), the components necessary for success are defined (Volume, Velocity, Varity) (Dumbill, 2012, p. 37).

Dr. Erik Dahl discusses a comprehensive analysis of 176 terrorist plots against the United States that have been thwarted, , with Human Intelligence identified as being utilized to stop 60% of these attacks (Dahl, 2011, p. 628). This assessment may seem counter to the narrative presented in this thesis, except for two things. First, 40% of the attacks were stopped using other mechanisms, such as signals intelligence, other law enforcement activity, public threats, and other means. Second, since no effective platform comprises all available

information from all sources that might allow for the concept of Big Data to work, it is impossible to determine whether or not such a model and the use of analytics across available data elements and used by fusion centers (if the data and tools had been available for use) might also have identified and thwarted these same attacks, perhaps even sooner, and perhaps, even more attacks might have been uncovered.

In *Terror and Consent*, Philip Bobbitt provides material that has relevance for this thesis, which includes discussions on the use of state power to ensure freedom and the notion that increases in such power does not necessarily equate to a diminishment of liberty, and in fact, may be necessary to ensure that it survives. He also describes a failed attempt at creating an analytics platform to identify pre-terrorist activities using data mining presented as exactly the wrong approach to take in the recommendations chapter of this thesis (Bobbitt, 2008).

B. CHAPTER SUMMARY

This chapter provided a literature review and described publications describing the ISE and providing a basis for its development. Little published information on the performance of the platform is available to date, although an increase in submission volume over the years occurs, although little assessment appears on the outcomes of these submissions (for example, how many may have resulted in referrals to other investigative agencies or to follow-up investigations being conducted). Publications describe the need for the program to have access to large amounts of information to establish unusual occurrences outside of the expected baseline of activity. In other words, it is hard to determine what is unusual if adequate indicators are not available to determine what is usual. The military's concept of persistent surveillance is reported, in which a variety of information is available to form a complete operational picture. Human frailty and its role in intelligence failure are highlighted in several publications. People just are not good at seeing things they do not expect to see, and are

predisposed to view the world with a distinct set of biases. The use of business intelligence and Big Data across numerous sectors is described. Reference models for comparison are outlined.

IV. REFERENCE MODELS FOR INFORMATION SHARING

This section focuses on what is possible with complete information. It explores the use of predictive analytics in numerous applications, including both the private and public sectors. This issue is important to investigate because it is central to providing a complete operating picture from which to perform proactive analytics activities to identify and prevent pre-terrorist incident indicators before they escalate to terrorism. The literature on the application of predictive analytics traces back to at least 1947 in the book *Cycles: The Science of Prediction* that describes the use of prediction in chemistry, nuclear physics, and economics (Dewey & Dakin, 1947, p. vii). A model utilized in the United Kingdom, the Police National Database (PND), is explored.

A. PRACTICAL MODELS

1. United Kingdom

The British intelligence system consists of three agencies: MI5/ Security Service for domestic activities and threats and national security (reporting to the Home Secretary), MI6/ Secret Intelligence Service for foreign activities and threats, and the Government Communications Headquarters (GCHQ) for signals intelligence, which is discussed in more detail shortly (both of these reporting to the Foreign Secretary). In addition, every police department in Britain has a dedicated unit known as Special Branch, which consists of specially trained officers directed by MI5 to gather information related to potential domestic terrorist activities (Burke, 2009, p. 35). In addition to specially-trained officers directly assigned to each police agency in Britain, every police department is able to communicate with MI5 utilizing a computer network, and a national platform known as the IMPACT Programme, similar to the Suspicious Activity Reporting process in the United States, facilitates information-sharing (Burke, 2009, p. 37).

IMPACT was initiated as a result of a non terrorism-related murder of two schoolgirls and the acknowledgement that a cross-jurisdictional investigation was hampered by an inability to exchange information effectively between the Cambridge and Humberside police departments that allowed the offender to get close to the children despite numerous prior sex crimes, as identified in a report by Sir Michael Bichard.. Published in 2004 and commissioned by the (then) Home Secretary, this report acknowledged that national information systems were accessible to all police departments, but concluded that no “firm plans” existed for the creation of a national, interoperable, intelligence-sharing system (or shared “IT system,” as the report calls it), and thus, prompted the development of such a system that is now part of the National Policing Improvement Agency (NPIA), launched in 2007 as part of the Home Office (IMPACT Programme: Police National Database—Privacy Impact Assessment Report, 2009, p. 6).

Although not yet complete, this system is a more comprehensive approach to facilitating information sharing across British police agencies. It consists of three key deliverables.

- IMPACT Nominal Index (INI), a reference system that allows agencies to identify which force is holding information related to an individual (delivered in 2005 and replaced by the Police National Database in 2011).
- Management of Police Information, a comprehensive guidance to ensure that information is relevant, accessible, and professionally managed (all forces were compliant by 2010).
- Police National Database, a single source of police information consisting of records from individual agency intelligence, crime, domestic abuse, child abuse, and custody business areas (operational in summer, 2011), allowing specially-trained and vetted users to identify “links and patterns” occurring at the local, regional, and national levels (Police National Database).

Despite the development of comprehensive guidelines for appropriate use, the system has faced criticism and raised privacy concerns. A Daily Mail article reports that one in four Britons will be recorded in the Police National Database,

which will be loaded with 15 million records of suspects, some victims, and criminals. The article quotes Daniel Hamilton, of Big Brother Watch: “It’s staggering to think that a quarter of the British population could be logged...” on the database (Greenwood, 2011).

The Police National Database is consistent with the need to have a complete operating picture from which to connect the dots. The system is specifically designed to overcome one of the inherent weaknesses of the U.S. SAR program: that an analyst must identify a possible nexus to terrorism for a discreet component of information before it is even flagged for potential sharing. A publication of the NPIA describes it this way, “Sometimes connections [across incidents] can be very weak, and [under the old system] we had to rely on other forces putting their markers on intelligence” (The PND: Making a Difference, 2010). Thus, the IMPACT Police National Database is specifically designed to overcome this inherent weakness of the U.S. SAR program.

2. Military Intelligence, Surveillance & Reconnaissance (ISR)

Consistent with the notion of a broad, unfiltered first-stage collection of information for analysis is the concept of Persistent Surveillance, a term used primarily in a military intelligence/ISR context and which refers to the integration of data largely from sensors and systems, such as satellites and motion detectors to allow analysts to “rapidly search, correlate, fuse and visualize” across large datasets (Kimmons, 2008). This concept is exactly what a fusion center should be doing, and is consistent with the concept of operations described in earlier sections (United States, 2005, p. 11), except that the fusion center depends upon the ISE that limits this breadth of information. To continue the military reference, this concept has three primary components (Pendall, 2005).

- Multimode, multidimensional and continuous collection across the entire operational environment.
- Near real-time data distribution with user-defined presentation formats (delivery).
- Horizontal integration of data and advanced, distributed analytics.

Although used in the military space, this term can also be used to inform the needs of the ISE. In fact, one could argue that Persistent Surveillance is almost fundamentally at odds with the current process that restricts information into the ISE. Instead of persistent surveillance, in which a broad base of unfiltered real-time information is immediately available to analysts and delivered to users, the SAR process requires that first responders (collectors) individually assess each potential component of information, before it can even be considered for analysis at the fusion center level.

Information that enters the fusion environment generally comes from the following sources (Berkowitz, 2008).

- Signals Intelligence (SIGINT), which often includes intercepts of electronic communication.
- Geospatial intelligence (GEOINT), which includes satellite imagery, pictures, sensors, and video.
- Measurement and Signals Intelligence (MASINT), which includes nuclear, acoustic, seismic, or spectral information.
- Human Intelligence (HUMINT), which comes from human beings; e.g., collectors and operative agents.
- Open Source Intelligence (OSINT), from public websites, media sources, and other unclassified events and reports.

Although some of these sources do not have a direct application to law enforcement data sources that are the suppliers to the ISE, most do. For example, GEOINT can be police surveillance camera imagery. MASINT can be gunshot detectors or Chemical/Biological/Radiological/Nuclear (CBRN) sensors. HUMINT would be the primary information sources from a police agency: 911 calls, incident reports, arrest reports, suspicious activity reports, gang incident data, curfew violation reports, vehicle crash reports, and others.

This Persistent Surveillance concept is designed to address this key failure of the intelligence and law enforcement communities to integrate their available information, the "dots," if you will; to allow for their analysis, or "connection," thus the "connect the dots" metaphor. For this concept to be realized, the dots must be available. This "failure to disseminate… threat information" and lack of information-sharing between law enforcement and intelligence agencies and "*ambiguity inherent in attempting to assess hostile intent* [emphasis added]" were factors in missed opportunity to prevent the attacks of 9/11" (Ang & Luikart, 2003, p. 69). This concept is nothing new. Failures of intelligence occurred prior to 9/11 as well.

3. Financial Crimes Enforcement Network

Interestingly, a very similar information-sharing environment is focused on protecting the financial system from crime that has been in place for more than 20 years. Known as FinCEN, the FinCEN overcomes many of the fundamental problems with the ISE, and even utilizes its own version of the Suspicious Activity Report—also known by the same name as the ISE SAR, and designed to identify potential illegal activity. FinCEN receives vast amounts of financial transaction information, assesses these indicators for possible abnormal activity, shares information with international organizations, and disseminates data for law enforcement purposes (Financial Crimes Enforcement Network Annual Report 2011, 2011, p. 1). FinCEN receives the bulk of its information from two mandatory sources, Currency Transaction Reports (CTRs), which must be filed by financial institutions when transactions exceed $10,000.00 in value (either individually or in aggregate in the case of multiple transactions on behalf of the same person), and Suspicious Activity Reports when financial institutions "know, suspect, or have reason to suspect" illegal activity. These reports are mandatory, and all financial institutions must comply, with 14,826,316 Currency Transaction Reports filed, 1,446,273 SAR filings, and various additional reports and

submissions to the network; for a grand total of 17,124,020 total submissions in 2011 (Financial Crimes Enforcement Network Annual Report 2011, 2011, pp. 7–8).

Detailed reports of the number of reports are submitted to FinCEN, but little recent information on how many resulted in a follow-up investigation. In the 6-½ year period ending October 31, 2002, 940,000 financial SARs were generated in the United States, which resulted in 70,000 direct referrals to law enforcement agencies, although no specific information is available on how many of these actually generated investigations (Reuter & Truman, 2004, p. 107). This number is a 7.44% referral rate, if presuming that most of these resulted in some kind of follow-up investigation (a reasonable presumption since FinCEN reviewers found some reasonable basis for referring them to law enforcement in the first place), or more than three times the rate for ISE SAR investigative action (which was 2% in 2009–2010, from Section II-B of this thesis).

Similar financial crime reporting platforms exist in other nations. FinCEN is the Financial Intelligence Unit (FIN) for the United States. More than 100 nations participate in the Egmont Group, which derives its name from a 1995 meeting conducted at the Egmont Arenberg Palace in Brussels during which participants recognized the benefits of creating a network of international financial crime detection and reporting, and as such, standards were defined for participation (The Egmont Group of Financial Intelligence Units, n.d.). The United Kingdom is another participant in this group, whose Serious Organized Crime Agency (SOCA) is responsible for the collection and analysis of financial SARs in the country. Consistent with the completeness of the Police National Database, SOCA provides a more robust platform for information assessment than its U.S. counterpart, in which up to 30% of SARs in the United Kingdom “either led to a longer term investigation, or added substantially to an existing investigation” as reported in 2011 (The Impact of SARs in Reducing Crime, n.d.). This number is more than three times the number of follow-up referrals for the U.S. program and 15 times the number of follow-up referrals for the ISE SAR program (although

each measure is for a different performance period and reflects a different level of maturity for the various platforms, with ISE SAR probably the least mature if the referral metric discussed in this thesis is an accurate measure).

B. METRICS FOR SUCCESS

According to research by a leading business intelligence think shop, the top two leading survey responses from over 100 users who have implemented data analytics this technology across their business enterprise, include 1) meeting business goals and 2) model accuracy (Eckerson, 2007, p. 9). If these metrics are applied to the ISE, they might reasonably be expected to translate into allowing the environment to meet its objectives of facilitating the sharing of terrorism-related information better and for allowing this information to be used for the prevention of terrorist acts. If a goal of applying analytics to the ISE were to identify actionable intelligence from the data, metrics for success would reasonably include such elements as the following.

- The number of criminal terrorist investigations initiated.
- The number of criminal terrorists identified.
- The number of criminal terrorists arrested.
- The number of criminal terrorist cells identified.
- The number of connections across criminal terrorist organizations determined.
- The number of criminal terrorist plots identified.
- The number of criminal terrorist actions prevented.
- The number of inquiries and analysis activities performed by users of the environment.
- Self-surveys of perceived value and usefulness across users of the environment.

C. DESIRED OUTCOMES

The desired outcome of any effective model is the successful realization of its stated objectives. In the case of the ISE, the objective is, according to the 9/11

Commission Report and its recommendations, to connect the dots across data sources so that the events of 9/11 do not occur again and the next potential terrorist attack is identified and prevented before it occurs.

D. KEY CHARACTERISTICS OF EFFECTIVE MODELS

The examples of effective models described above share similar characteristics.

- Complete, comprehensive, persistent, real-time information from multi-mode sources.
- Analytical tools to identify relationships across data elements.
- Consistent training across jurisdictional lines.
- Horizontal, integrated data sharing.
- Lack of dependency upon human element vetting discrete components of information before they can be shared.

E. CHAPTER SUMMARY

This chapter identified the art of the possible by describing several reference models for comparison, including the Police National Database in the United Kingdom, the military's concept of persistent surveillance, and the FinCEN. All of these systems "get it right," or at least get it better than the ISE. Metrics for success for the ISE were explored, and included such measurement areas as the number of terrorist investigations initiated and the number of terrorists arrested. Key characteristics of the effective models described here are outlined. These models all have access to a greater range of information from multiple sources, analytical tools, consistent training, horizontal integrated data sharing, and a lack of dependency on single points of human frailty.

V. COMPARE AND CONTRAST

A. INFORMATION SHARING ENVIRONMENT COMPARISON

Eckerson describes maturity levels of Business Intelligence platforms as shown in Figure 3 (Eckerson, 2007, p. 5).

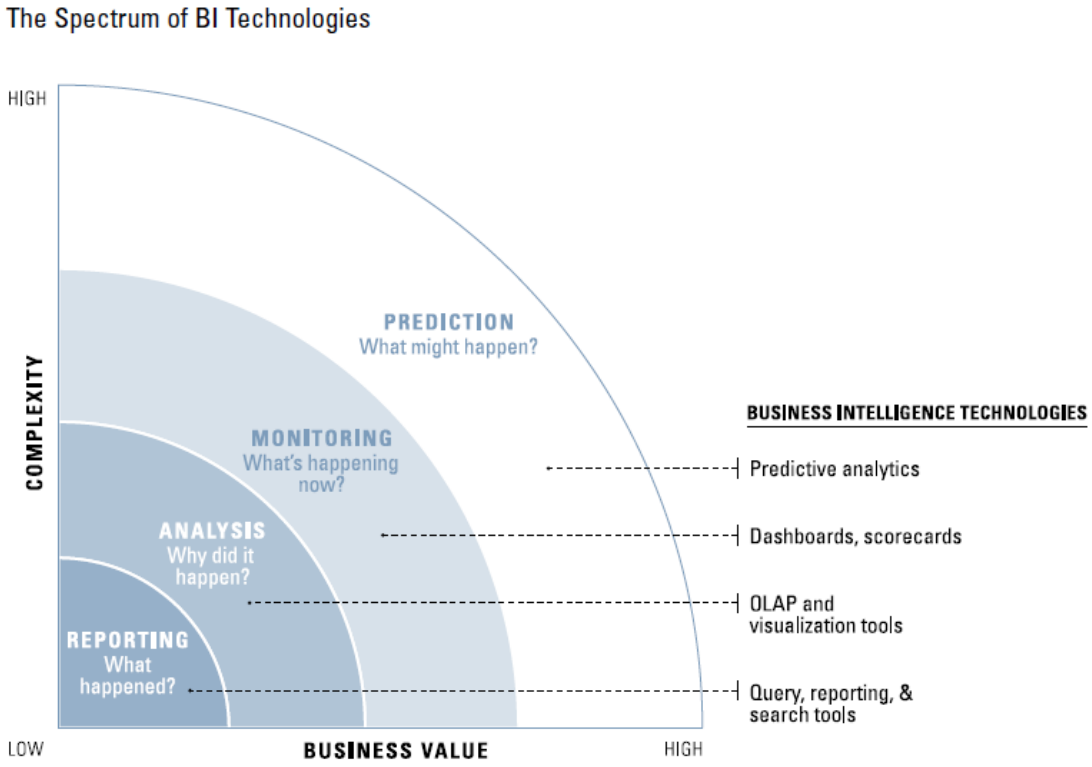

Figure 3. Spectrum of Business Intelligence

In this spectrum, the ISE is at the low end of both the Business Value and Complexity scales. It tracks what happened, and provides basic query, reporting, and search tools based upon the data it collects. It actually does a poor job at even this lowest-level task since, as discussed earlier, it does not even do a comprehensive job of collecting enough data elements to form a comprehensive picture of what has happened.

1. Limited Data

In the journal article entitled “Intelligence Reform: The Logic of Information Sharing,” Calvert Jones makes some relevant points. Information needs to be as sharable as possible and integrated from as many sources as possible (Jones, 2007, p. 385). Vast amounts of data are required to prevent “being caught off guard” by unexpected happenings (Jones, 2007, p. 387). As a basic framework for understanding activity, information is necessary to form a baseline of expected activity, so that unexpected activity can be detected. However, the ISE relies on a “conduit” metaphor for information sharing; ideas must be physically transferred from one person to another through a conduit (Jones, 2007, p. 389). In the case of the ISE, this metaphor means that the sender is the person completing a SAR, and the listener is the person analyzing it for potential actionable intelligence (of course, additional approval stages exist that could also be considered “listening” activities). Jones suggests that this process can quickly overwhelm the listener, which causes a loss of context and confusion from “information overload,” and that technology and analytics are needed to make sense of this information (Jones, 2007, pp. 396–398). This analytics component is missing from the ISE, and if it were present, it would not have access to the range of information Jones describes as necessary to detect unexpected behavior.

As noted earlier, the 2011 ISE Annual Report to the Congress presents a broad definition of the ISE itself as “infrastructure and capabilities,” which extends the parameters of the environment and includes many capabilities that are not directly accessible from the ISE assessment space—a notion that is reinforced by several examples given of potential use cases, one of which involves a police officer using the NCIC, a national computer database of criminal justice information including wanted persons and criminal histories (Aftergood, ,2008), to conduct a query, the results of which direct the officer to contact the Terrorist Screening Center, a terrorist watch list containing information on known or suspected terrorists (Terrorist Screening Center, n.d.), to assess a potential

match. Another example depicts an intelligence analyst utilizing the Library of National Intelligence, a centralized automated “card catalog” containing a summary of all disseminated intelligence products maintained by the Office of the Director of National Intelligence and the CIA (Library of National Intelligence, n.d.) to develop new intelligence products (ISE Annual Report to the Congress, 2011, p. 3). Not all these systems are part of an integrated, searchable database, as the first example notes, an officer has to utilize one system (NCIC) and then is referred to another. Using this definition of a system, just about any anti-terrorist activity conducted by any local, state, or federal official accessing any system would fall within the parameters of the ISE, whether or not the system utilized is actually integrated with the ISE and available for data analytics and inquiries from this environment (i.e., without having to leave one system and access another).

2. Unlimited Data

At the other end of the scales of value and complexity exists the Predictive Policing framework, using the Chicago model as an example, in which information is collected and reported upon. On Line Analytics Processing (OLAP) and visualization tools, such as maps, allow users to ask and receive answers to questions of why things are happening, real-time dashboards allow users to ask what is happening now, and the prediction capability in development allows for projections about what might be likely to happen in the future. OLAP is a “multi-dimensional view of aggregate data” that allows advanced analytics to occur, and can be accessed by users throughout the Chicago Police Department on networked desktop and mobile computers to provide “one stop shopping” accessibility and analysis activities (Forsman, 1997). The Chicago model creates a single, integrated assessment space in which all available variables—the more the better, since any combination of obscure indicators could point to an emerging problem, trend, or pattern, or could form a prediction space—are available for analysis.

Big Data is a concept that involves the ability to process massive amounts of information at scales not possible with traditional computing techniques. It generally involves three components.

- Volume, or having access to extremely large sets of information. As this source suggests, if a forecasting model that considers 300 factors rather than six could be developed, a more accurate prediction could probably be generated.
- Velocity, or the rate at which data flows into a processing environment. In the retail space, this component could be access to real-time customer sales data that provides competitive advantage to those retailers who can assess it instantly and make projections about customer behavior. This term refers to the ability to process large streams of real-time information quickly.
- Variety, or the diverse nature of information from a wide range of sources that might not fall within defined structures. Examples include text from social networks, sensor data, image detection, and other semi-structured and unstructured information (Dumbill, 2012, p. 37).

The concept of Big Data requires that the manner in the value of information is though about, must change. Rather than a single piece of information being individually assessed for its potential value and being utilized only if it is relevant, Big Data takes the opposite view. With the amount of information potentially relevant for pattern identification, forecasting, and other analytics activities, it is not practical to assess individual components. Instead, each piece of information by itself may have low value, but the "potential for insight is great" if everything can be analyzed (Zikopoulos, 2012, p. 11). The current ISE SAR process is everything that Big Data is not. It fails to consider the potential value of a single piece of information in the larger context and only assigns value to that piece of information itself, rather than considering the value of larger sets of data that might form a more accurate assessment environment. When looking at volume, for example, only specific SAR submissions that have been manually identified, generated, submitted, approved, and shared will ever form the basis for future assessment. When examining velocity, a SAR must be

created by a human being after that human being becomes aware of an event that this person believes has a nexus to terrorism. Finally, when examining variety, the primary information type assessed in the ISE is a SAR.

B. DIFFERENCES AND SIMILARITIES

One useful reference model to compare and contrast with the ISE is the United Kingdom's PND or Police National Computer (PNC) as it is sometimes called since its objectives, users, data sources, and national cross-jurisdictional scope are most aligned. The PND is accessible by both MI5 and MI6, in addition to the police services (The Police National Computer (PNC), n.d.). Therefore, it is useful to provide a matrix comparing the two approaches, which is referred to in Table 1 as the U.S. approach and the U.K. approach.

Challenge	U.S. Approach	U.K. Approach	Comment
Lack of actionable intelligence means there is a lack of dots to connect	Information Sharing Environment (ISE) pushes selected, discrete pieces of information into a shared environment	Police National Database (PND) provides comprehensive, "all source" information to ensure all the dots are available, not only those that have been vetted	U.K. approach provides complete operating picture from which to draw connections, U.S. approach does not
Lack of ability to identify and assess pre-terrorist incident indicator information means dots cannot be connected	Fusion centers with varying protocols generally operated by states assess information, federal fusion centers assess available information	Trained Intelligence analysts embedded at each police agency and at the national level and reporting to the Home Office can assess all information from the PND	U.K. approach provides consistency and standards in training for intel analysts at each agency, U.S. approach is characterized by a lack of standards and no centralized oversight
Human Dependency	Agency analysts must decide that information rises to the level of nexus to terrorism before it can be shared with anyone in the ISE	The PND shares all information, without a "pre-vetting" process	The U.K. approach removes one of the barriers for information availability and thus eliminates a critical human dependency from the process

Table 1. U.S. vs. U.K. Approach

A second useful comparison is FinCEN, the financial network, which uses SAR reports as the ISE does, but also uses additional indicators, which in this example, are compared in the context of the components of Big Data described earlier.

Component	ISE SAR	FinCEN	Comment
Volume	Suspicious Activity Reports prepared manually by human analyst. 3,400 reports submitted in 2009-2010.	Currency Transaction Report, Suspicious Activity Report, various other reports generated automatically and by human analyst. 32,937,760 total submissions in 2009-2010.	FinCEN has appropriate volume to provide enough information to identify patterns, trends, and activities outside the baseline. ISE SAR relies on the traditional model of reviewing a single indicator for potential value without any contextual assessment.
Velocity	Suspicious Activity Reports generated after the fact, if a human being determines the need; and submitted only after preparation, approval, vetting, and submission to the Information Sharing Environment. Voluntary compliance with no penalties for failure to submit.	Currency Transaction Reports generated automatically by most financial institutions when certain criteria are met. Suspicious Activity Reports required to be generated when suspicious activity is identified. Mandatory compliance with penalties for failure to submit.	FinCEN has appropriate velocity to allow for detection of activity in near real-time. ISE SAR relies on a slow manual process as far from real-time as one can imagine.
Variety	Indicators are limited to a single component, the SAR.	Indicators include SARs and a variety of other sources including Currency Transaction Reports and reports of cash payments over $10,000, registration of money services businesses, reports of foreign bank accounts, and others.	FinCEN provides access to a variety of indicator data sources. ISE provides access to a single data source, the SAR.

Table 2. ISE/SAR vs. FinCEN

Both the PND and the FinCEN utilize approaches designed to increase volume, velocity, and variety of information available for analysis to identify potential indicators of criminal activity. Both these platforms reduce the role that human decision making plays in determining whether or not data enter the assessment environment by allowing complete situational awareness indicators to enter their respective evaluation spaces, and thus, reduce one potential point of failure and enhance the effectiveness of these platforms.

C. WEAKNESSES OF CURRENT MODEL

This section describes weaknesses of the ISE in the context of the reference models described earlier. When discussing weaknesses, it is useful to note that the working definition of the ISE used for comparison purposes in this thesis is not the definition included in the ISE Annual Report to the Congress, in which almost any system or database could be described as part of the ISE. Rather, it is the integrated, accessible, searchable platform for inquiry and analysis that forms the actual ISE data components, primarily SAR reports.

1. Lack of Information

Big Data relies upon vast quantities of information to detect patterns and trends and to support analytics activities. A lack of information limits the effectiveness of these assessment activities. In other words, the less dots that available, the less ways they can be analyzed for possible connection. In an analysis of terrorist plots identified from 1999 to 2009 published by the Institute for Homeland Security Solutions, 86 foiled or executed attacks against U.S. targets were evaluated using open-source intelligence. The ISE, through SAR reports, only indirectly allows for a large majority of clues from law enforcement agencies and the public. This analysis indicated that law enforcement is the first line of defense in detecting these plots, with information related to over 80% of the plots coming from criminal justice agencies, and the intelligence community providing initial clues in only 19% of the cases. Nearly one in five plots were

identified and stopped “accidentally” while law enforcement was investigating seemingly unrelated crimes (Strom et al., 2010, p. 19). This analysis is important, because the emphasis of the ISE is on the more traditionally defined “intelligence” information or that with an identifiable nexus to terrorism, which must be vetted by trained analysts and approved by supervisors before it can be shared. Law enforcement investigations are recursive processes, which depend upon the availability of a wide range of information to find associations across people, events, and assets. Investigative techniques are more mature than finding (or, to put it another way, collecting and reporting) the initial clues (Hollywood & Pope, 2009, p. 5).

a. Information Beyond SAR Submissions

It is more likely that information related to a terrorist threat will be identified from law enforcement sources than from intelligence sources, and that evidence of such a threat will be found in the “incidental contact with… police officers” (Bjelopera, 2010, p. 5) than with federal agents. It is not too much of a stretch, then, to presume that such information might come from a source not traditionally allowed for in the SAR report or the ISE, such as a 911 call or other documentation of a routine law enforcement interaction with a subject. It is further possible that the records related to such documentation will not be pushed into any shared space for analysis or possible connection to other sources to allow for a determination that such activity has a possible nexus to terrorism, especially when evaluated in the context of events and activity documented in other jurisdictions from other sources. The question of what is shared needs to be eliminated as a point of failure. Everything needs to be shared and made available for analysis. The conclusion chapter provides some possibilities for achieving this vision, which will not be easy and is not a short-term fix.

b. Disrupting Terrorist Plots

Dr. Erik Dahl has conducted an analysis of 176 terrorist plots against the United States over the last 25 years that have been thwarted, and describes the assessment dataset as the most comprehensive of its kind. According to this evaluation, most plots were not disrupted "when a highly skilled analyst detects subtle clues" that link disparate bits of data, but rather when intelligence and law enforcement entities identify detailed information relevant to specific plots, which is often developed by domestic agencies (Dahl, 2011, p. 622). However, Dahl acknowledges that it is difficult to assess precisely how many attacks may have been prevented, specifically because it is difficult to measure events that do not occur, and terrorists themselves may flood systems with deceptive information that might indicate false plots (Dahl, 2011, pp. 622–623). This assessment suggests that evaluating large volumes of information to "connect the dots" is not the solution to preventing terrorist attacks. In fact, externally thwarted domestic terrorism cases were thwarted based on the following information sources: human intelligence (60%), signals intelligence (10%), chance encounter (7%), other law enforcement activity (6%), overseas intelligence (6%), detainee interrogation (6%), and public threats (5%) (Dahl, 2011, p. 628).

Dahl's assessment strengthens the need to remove barriers present in the ISE. It is difficult to conclude that assessing available data would not have prevented the referenced potential attacks, since no environment available presents all possible indicators of behavior. In other words, if a robust, data-rich environment, with a complete operational picture, had been present (in other words, if all the "dots" had been available), it is possible that the plots identified might have been found using other information elements assessed in other ways. Perhaps in at least some of these cases, other indicators of suspicious behavior might have been reflected by measures not in the current environment. In fact, it is possible that more plots might have been identified, that these plots might have been identified sooner, or that more connections across

potential terrorist activities might also have been uncovered. Even if the argument that a majority of plots are uncovered based on human intelligence is accepted, current barriers to the ISE SAR process unnecessarily restrict even this form of intelligence from entering the evaluation space. Also, —the remaining 40% of non-human intelligence sources are potentially lacking from the evaluation environment altogether. Finally, as Dahl acknowledges, the universe of thwarted (or non-thwarted plots that might be in progress at this moment, for that matter) terrorist plots could be larger than 176, since it is impossible to assess all the plots that did not occur (i.e., proving a negative).

c. Scope of Information

A range of information collected at the law enforcement agency level does not meet the definition of nexus to terrorism by itself and does not have formal categorical descriptors in the SAR report, that together could have allowed these thwarted plots to be identified with methods other than (or enhanced by) human intelligence, which include such critical elements as 911 calls for service and reports of theft and other seemingly unrelated (to terrorism) crimes. Take the example of a series of calls to 911 concerning suspicious persons taking photographs of bridges. If these calls occur over a period of time, without connections made between them, it is unlikely that a single call would result in any kind of police report (Hollywood & Pope, 2009, p. 5), much less a SAR report. This scenario becomes even more compelling if the events were occurring across local jurisdictional boundaries.

The 2011 ISE Annual Report to Congress acknowledges the need for improved efforts to improve the scope of information available and to enhance analytics and aggregation capacity. It refers to the creation of a Multimodal Information Sharing Task Force (MIST) designed to foster information-sharing in a port environment, and to enhanced law enforcement information-sharing through N-Dex, the FBI's voluntary national data exchange system for police incident reports that will be an important addition to the ISE. Working groups

were also established to discuss interoperability standards and improved data aggregation, and analytics capabilities, and to partner with the private sector and foreign partners to identify critical sources of knowledge (ISE Annual Report to the Congress, 2011, pp. xiii–xvi). These efforts are in the working group assessment process.

2. Human Dependency

To share information with external agencies in the ISE platform, a law enforcement officer must determine that suspicious activity has been identified that might have a possible connection to terrorism. That information must then be submitted to the state or local fusion center, at which an intelligence analyst must review it to determine if it meets the criteria for sharing. Presuming the analyst makes the determination that the activity meets the criteria for submission; it is entered into the information-sharing environment and can then be accessed by human analysts for possible connection with other intelligence information (Bjelopera, 2010, p. 8). This information sharing presumes that both the law enforcement officer and the analyst have the foresight to determine that one piece of information, at the time it is identified and analyzed, might have a nexus to terrorism, or, to quote the National Strategy for Combatting Terrorism from the Bush Administration, that "…[i]nformation acquired for one purpose, or under one set of authorities, might provide unique insights when combined… with seemingly unrelated information from other sources" (NSIS—Introduction and Overview, n.d.).

a. Unknown Significance

Significant challenges arise when relying on this human process to make the correct determination that a piece of information should be shared. In the 2008 Mumbai attacks, fishermen reported the arrival of the terrorists to local police, who did not act upon or share the information. According to reports, the CIA and Federal FBI did not share information that Khalid al-Midhar and Nawqa

Alhazmi, two men with connections to terrorism, had entered the United States prior to 9/11 (Hollywood & Pope, 2009, p. 5). Perhaps this lack of information sharing occurred because, at the time the information became available, its significance was not known. This inability to recognize the significance of an observed activity can result in a failure to take appropriate action, such as sharing the observation with other agencies or acting upon it to prevent a terrorist act from occurring. One police officer responding to one call of suspicious activity, being unaware of the seemingly unrelated information from other sources, might not have enough background to make the connection that the activity this person has become aware of would make the connection, when examined in the context of information from other sources.

b. Inbuilt Schemas

Dr. Fathali Moghaddam describes the notion that humans are predisposed to make sense of sensory inputs through "inbuilt schemas" that "predispose us to synthesize the streams of information reaching us," and that "constructs," or "particular ways of viewing the world," tend to shape a view of the world and situations in which inadequate information exists (Moghaddam, 2001, pp. 29–31). Consistent with this identification of difficulty in assessing information without bias is the notion of tunnel vision. Intelligence analysts expect continuity and thus underestimate the possibility that change might occur, and therefore, fail to identify "low probability/high consequence" events, and this phenomenon is reinforced due to the long gaps between significant unusual occurrences, which cause both a "physical and psychological" impact of surprise attacks—a mindset known as "cognitive bias" (Rovner & Long, 2005 p. 623).

c. Cognitive Challenges

In *What Makes Intelligence Analysis Difficult?: A Cognitive Task Analysis*, the authors conducted a study of the cognitive challenges associated with the task of intelligence analysis, and identified a number of "cognitive

challenges" faced by the analyst that fall within the scope of human frailty, as summarized as follows (Hutchins, Pirollo, & Card, 2007, pp. 298–304).

- Time pressure. The requirement to produce reports for decision makers under stressful time constraints can cause "channel thinking" down a specific path, in which analysts are required to produce assessments without adequate time to develop background knowledge.
- Multiple sources of information. Analysts must merge together multiple types of information, each with its own set of factors that may impact interpretation; and the analyst may not have familiarity with these varying information types.
- Uncertainty. This notion relates to the cognitive bias described by Rovner and Long, and to Moghaddam's discussion of "constructs." A strong correlation exists between the "context in which data occurs and the perspective of the observer." When faced with great degrees of uncertainty, the capacity of the analyst to assess data based on context sensitivity will likely be diminished.
- High mental workload. Analysts are faced with continuous streams of incoming information, which must be evaluated, synthesized, and aggregated, which causes trade-offs to occur as these cognitive analytical tasks compete for attention with other requisite tasks.
- Potential for error. The high workload imposed on analysts increases the likelihood that errors may occur, including the possibility of tunnel vision discussed earlier, in which an analysis may be "skewed when analysts attempt to reduce their cognitive load by focusing on… data they understand" and ignoring information with which they have less familiarity or context.

D. LIMITS OF HUMAN NATURE

Michael Handel, a student of intelligence failure, feels that the principal cause of such failure is the "limitations of human nature," and most failures occur because decision makers fail to adapt their concepts to new information (Diaz, 2005). This human dependency must be removed. Unfortunately, the ISE system is exposed to these inherent weaknesses. The system itself is flawed at the most fundamental level because rather than control for the vulnerabilities characterized by Handel, it relies upon them.

In a relevant and stunning example of human failure, the limits of human nature essentially prevented the New York Police Department (NYPD) from sharing critical information concerning the imminent collapse of the North tower with the New York Fire Department (NYFD), and thus, the urgency of evacuating the tower was not properly conveyed to members of the fire service (Pfeifer, 2007, p. 208). Situational awareness was available to one agency and not another, despite the fact that both agencies were directly involved in the same situation and would both be impacted by the eventual outcome that this awareness suggested. As with the failure of the FBI and CIA to share information on 9/11 hijackers, and the failure of police to act on information supplied by fishermen in Mumbai, this situation was less a technical radio interoperability issue as it was a process issue, since commanders and personnel from both agencies were within close proximity of one another (Pfeifer, 2007, p. 211). Turf battles, organizational arrogance, group theory, and social identity issues defined the long-term alienation between these agencies, issues that existed between the agencies prior to 9/11 as a fundamental part of the system that defined interagency cooperation (or lack thereof), and that became even more apparent when that system was stressed with the critical input if a catastrophic event, leading, in this case, to a loss of life that perhaps could have been prevented if these systemic flaws had been addressed prior to the event. Whatever the motivation for failure to share information in these examples, they all involve human beings required to make decisions, who made the wrong ones. The time to fix these problems is not during an unplanned crisis, but prior to the crisis. If the system had been optimally functioning in advance, it might have produced a more desired outcome during the event.

Human limitations in imagination, stove-piping, institutional arrogance, and turf battles are the product of people, who themselves suffer from human frailty. Human error itself is embedded in the organizational processes that embody the error (Grabowski & Roberts, 1996, p. 2). Research suggests that simply focusing on fixing the superficial errors themselves does not address fundamental process

issues in the system and will not effectively solve the underlying problem (Edmondson, 1996, p. 9). The ISE process does not address these fundamental issues, since the system depends on human decision making to determine what information elements to share, and with whom. Pfeiffer argues the need for the use of a unified command system during emergency events (Pfeiffer, 2007, p. 213). This kind of system must be in place all the time, so that when an unplanned emergency occurs, the process is already in existence. The behavioral economist Dan Ariely suggests that when faced with too much complexity, humans take the easiest of the possible decision points, even if that decision point is to do nothing (Ariely, 2008). In the case of an analyst faced with a complex set of indicators that may or may not require the completion of a SAR submission, in this framework, the analyst may decide to take the path of least resistance and simply do nothing at all. The current ISE process requires the analyst to take deliberate action in the face of complexity.

E. MITIGATION OF HUMAN WEAKNESS

In the case of the ISE, the system itself needs to be designed in such a way as to mitigate human weaknesses that are an inherent part of any system that a human being designs. In many ways, the system is a reflection of the inherent flaws in all humans, and since it is possible to recognize this situation in advance, the opportunity exists to optimize the system before a critical event occurs, not after one has already happened, at which point, of course, it is too late.

> Events present themselves to us in a distorted way. Consider the nature of Information: of the millions, maybe even trillions, of small facts that prevail before an event occurs, only a few will turn out to be relevant later to your understanding of what happened [because your memory is limited and filtered]… (Taleb, 2007, p. 12).

> Categorizing always produces reduction in true complexity. It is a manifestation of the Black Swan generator… Any reduction of the world around us can have explosive consequences… (Taleb, 2007, p. 16).

The above quotes from *The Black Swan* discuss weaknesses in the human ability to process, interpret, recall, and classify information, which from a larger perspective, relate to the narrative of human frailty; which will be a key topic of this thesis. Taleb discusses the “highly improbable consequential event” (Taleb, 2007, p. 18), otherwise known as the Black Swan, as one that is unexpected and has consequential impact. The author would go a step further and suggest that any event that is unexpected, regardless of the consequence or perceived consequence, needs to be considered in the same category as a Black Swan. In other words, the author does not think it is the level of impact that matters as much as the level of surprise, because even an event that by itself might not have a significant impact, could, when part of a sequence of errors or dependencies, ultimately have a profound impact. Taleb successfully summarizes the inherent human weaknesses associated with the process of identifying a discrete component of information and the dependence upon a human analyst who must assess the relevance of this component of information and determine that it is important enough to be entered into the environment for sharing. This process relies upon the same human frailty that presents itself in the Black Swan phenomenon, people are bad at assessing things objectively, partially because of memory, history, poor filtering, clustering, and a variety of other biases and limitations of imagination.

Consider the events surrounding 9/11, and the fact that no one at the airlines or at the FAA that day had ever dealt with multiple hijackings before, and were thus, not expecting them. Therefore, human frailty played a role in a delay in notification to other transatlantic flights concerning hijackings after the first report of possible problems. To quote *The 9/11 Commission*, “As news of the hijackings filtered through the FAA and the airlines, it does not seem to have occurred to their leadership that they needed to alert other aircraft in the air that they too might be at risk,” and when a United Airlines dispatcher finally took it upon himself to generate warning messages to United transatlantic flights, the

cockpit crew of United 93 did not believe the warning, with the pilot responding in puzzlement “Ed, confirm latest mssg plz-Jason.” (The 9/11 Commission Report: 2004, p. 11).

Frequent examples of similar kinds of situations demonstrate the point—people just are not good at recognizing or processing things they do not understand, whether these things are Black Swans or Black Swans without the Impact—still unusual and unexpected events that people probably are not going to be great at identifying as significant, or in the case of the ISE process, as important enough to warrant a SAR submission.

F. CHAPTER SUMMARY

The range of human frailty was described and specific cognitive challenges faced by intelligence analysts were outlined. The ISE was compared with the reference models identified earlier. It described a maturity model in which value and complexity of various systems can be measured, which shows that the ISE scores poorly in these measurements. The concept of Big Data, which involves the ability to leverage and process massive amounts of information to enhance business intelligence, was described as requiring three things: volume, velocity, and variety. The reference models all score better in these areas than the ISE, by having more information, more quickly, and from more sources. Specific weaknesses of the ISE are apparent in the areas of a lack of information and reliance on human analysts to determine the value of a potential indicator before it can be reported and made available for further analysis, which can best be summarized as limitations of human nature and failures of human imagination. These failures are embedded in the organizational processes that embody the errors, in this case, the ISE program itself. The ISE needs to reduce its reliance on human processes that artificially prevent complete information from being made available for assessment and sharing.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. SUMMARY

This thesis argues that the ISE cannot meet its objectives of removing barriers to information sharing among local, state and federal homeland security agencies and providing a platform from which to connect the dots, or to extract "previously unknown… information from data" (Taipale, 2003, p. 22).

1. Weaknesses

The ISE suffers from a lack of comprehensive information from which to develop situational awareness related to possible emerging conditions, which occurs because it relies on human gatekeepers that control information entry into the platform for analysis and because it lacks the advanced data analytics capabilities to assess the data to identify previously unknown indicators of potential pre-terrorist incident activity. When compared to other reference models, such as FinCEN, or when assessed from a Business Intelligence maturity perspective; or when examined within the framework of Big Data, the ISE fails to provide the Volume, Velocity, or Variety of information to allow for analytics to transform information into actionable output. The ISE as it now exists (with the limitation of human dependency that translates into a lack of complete information) will probably not achieve high performance in the areas described in Chapter IV (facilitating the initiation of terrorist investigations, identifying criminal terrorists, facilitating the arrest of terrorists, identifying terrorist cells, making connections across criminal terrorist organizations, identifying and thwarting terrorist plots, and so forth). In fact, the current platform is designed to fail due to limitations, which is primarily centered on human frailty. When the Business Intelligence maturity model is used to measure the ISE, it scores at the lowest levels of complexity and business value because it cannot support in-depth analysis due to a lack of volume, cannot tell what is happening now due to a lack

of velocity, and cannot predict what might happen in the future due to a lack of variety. ISE does a poor job even at this lowest-possible maturity level as suggested by the comparatively low percentage of SAR submissions referred for follow-up investigation when contrasted with FinCEN. This situation occurs because the environment has built-in limitations related to a lack of complete information, reliance on humans, which present weaknesses that limit their ability to evaluate information properly during the assessment phase, and a lack of analytical tools to make the information useful by identifying non-obvious relationships across and among data elements from various sources. When exploring effective models from non-traditional sectors, such as the military, other nations, and advanced data prediction implementations, the ISE exhibits stark differences, such as a lack of mandatory submission standards, a lack of integration of data sources, a lack of variety of sources, and a lack of advanced analytics capabilities. Almost by definition, the ISE will do a poor job of detecting emerging threats in areas inconceivable today, since the entire process is focused on SAR submissions that rise to the level of “suspicious” as determined by a series of human beings who must identify and document this suspicion based upon their imagination and ability to perform this function correctly.

The ISE does not deliver the volume, velocity, or variety of information required to exploit Big Data to find meaningful, actionable intelligence within the data, which is to separate the “wheat from the chaff” and improve the system’s fidelity, or the signal-to-noise ratio of actionable intelligence to information (Lowenthal, 2009, p. 72). Thus, the ISE cannot meet its design objectives because it lacks information, relies on humans at too many stages of the information fusion process, and does not leverage advanced information processing necessary to transform the data into actionable intelligence, which leads to an inquiry on how the ISE platform can be refined to overcome the aforementioned limitations and to understand better and make transparent the influence of human bias on the various phases of the system.

2. Potential for Improvement

Such modifications could take several courses. The precursor to FinCEN evolved over time from detecting financial crimes to include the role of detection of terrorist financing. The Bank Secrecy Act of 1970 established the first reporting requirements for certain financial transactions, and over subsequent decades, additional requirements were added and information-sharing capabilities were enhanced (History of Anti-Money Laundering Laws, n.d.). The ISE itself was born from a catastrophic event, the terrorist attacks on September 11, 2001, just as the PND was developed as a result of a catastrophic crime. Will it take another catastrophic act to demonstrate that the ISE cannot perform as designed in its current implementation, and thus force a reactive adaptation after the loss of lives? Will it be necessary to wait four decades before it is realized that changes need to be made?

An example of one path these enhancements can take is already in progress in the Department of Homeland Security's efforts to perform analytics on social media by looking for certain key words and phrases that might be indicators of potential pre-terrorist activities. The DHS National Operations Center (NOC) is authorized to analyze open source information from sources, such as Twitter, Facebook, and blogs to assist in forming a common operating picture and assessing situational awareness, in most cases without collecting personally identifiable information but rather to identify emerging activities with a potential nexus to terrorism (Written Testimony, 2012, p. 5). Ironically, this effort allows more information from the open source social media space to be available for real-time assessment than sources created or maintained by the organs of local, state, and federal law enforcement agencies. The characteristics of this assessment platform, including the measures of volume, velocity, and variety, would likely achieve a higher score and maturity level than the ISE itself.

3. Bottom-Up Approach

The DHS open source social media analytics activities are an example of a top-down national approach; developed, implemented, and managed by a federal agency in Washington. Another path might follow a process that better respects U.S. core constitutional values and engenders public support, by starting from a local or state decentralized bottom-up approach rather than a federal top-down method. Using a fusion center model, state or regional data-sharing efforts could be developed that would integrate many of the characteristics of an effective information-sharing platform. These regional databases could then be linked, with each forming a node on a national, interoperable information exchange platform that is managed by state and local entities and respects values of state and local communities, while realizing the objectives of accessibility to other partners. This process could occur in partnership with privacy advocates, such as the American Civil Liberties Union, which would then have a stake in helping to develop guidelines for privacy controls that still ensure effective outcomes for keeping local communities safe. Involving local law enforcement agencies as core contributors to the process will help guarantee that tests of criminal predicate are met in accordance with existing laws and constitutional values, and will also recognize some of the founding principles upon which this nation was built that traces its history back to the American revolution itself: that government and policing should occur at the local level, not at the level of the "King," where it was very far away. In other words, policing should not occur at the level of the "king-father" but rather at the "local level… in the town… perhaps the colony" (Dubber, 2005, p. 83). This local approach might allow the dual requirements of respect for privacy and comprehensive access to information to be met. In addition, a distributed architecture with local control allows "privacy protection by diversifying control" (Taipale, 2003, p. 42). Rather than the "king" ensuring privacy, the people are ensuring it through their local government agencies.

A regional or local “system of systems” is proposed, in which fusion centers are responsible for the management of databases at the local agency level that form a comprehensive, multi-mode platform for “persistent surveillance” using both human analysts and automated analytics processes, and in which information with a connection to crime that needs to be pushed up to the national ISE, is vetted and pushed once identified. Two forms of the ISE would exist, regional and national, or in other words, a Multi-ISE. Transparency is a critical part of gaining public trust for this process to work. The FinCEN annual report is filled with performance metrics on the number and type of submission to the environment. The ISE annual report is filled with one qualitative survey on levels of participation at various agencies. Public trust will be gained by sharing whatever performance metrics and characteristics can be disclosed without compromising system security.

4. Privacy Issues

In an outstanding article entitled “Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data,” K. A. Taipale provides a discussion of data privacy issues and suggests that technology itself can include safeguards to protect individual privacy rights through the use of “selective revelation” that can apply technology controls to shield the exposure of a person’s individual identity while alerting to potentially relevant suspicious activity through data analysis, and thereby, allow due process considerations to be followed before specific identity is revealed (Taipale, 2003, p. 66). Consistent with Taipale’s suggestion, this thesis argues that the system itself can include privacy protections while still meeting the objectives of identifying potential pre-terrorist incident indicators across various databases.

In *Terror and Consent*, Bobbitt describes an approach that is exactly opposed to the state and local-centric method proposed in this thesis, an effort to develop an information assessment platform with similar goals to the ISE that resulted in the resignation of the project’s director, Admiral John Poindexter. The

project, known as Total Information Awareness, was a series of research initiatives to define hypothetical profiles consistent with imagined terrorist attack scenarios, and then canvassing huge quantities of data to detect terrorist preparation efforts in pursuit of the implementation of the imagined scenarios. Even though various controls were established, such as the requirement that detailed access to personal identifier information would have required approval from an outside authority, Congress "killed the project completely" after "inept public relations," including the use of a "pseudo-Masonic all-seeing eye… blaz[ing] forth from the pyramid depicted on the Great Seal of the United States" (Bobbitt, 2008, p. 338). This project is a lesson on exactly what not to do to engender public support, a system directed by an Admiral at the Pentagon using a symbol that conjured images of mind control and suggesting that the military could see everything from its Masonic eye.

Although not a perfect approach from a technical perspective since some level of human review is still needed to approve data for sharing from the regional ISE to the national ISE, it removes the key barrier to efficacy in the current ISE, manual human approval for entry into any sharing environment. While not a Panopticon, the Multi-ISE will see more than it sees today.

B. RECOMMENDATIONS

The following recommendations are discussed.

1. Minimize human dependency and expand volume, velocity and variety
2. Add analytics capabilities
3. Make reporting requirement mandatory

1. Minimize Human Dependency and Add Volume, Variety, Velocity

Complete information must be made available at the regional level, without relying upon humans to review and decide whether or not such information can be shared. To realize the inclusion of unfiltered information from

a wide variety of sources that would be accessible across jurisdictional lines, various rules need to be followed. 28 CFR (Code of Federal Regulations) Part 23 establishes standards that determine when information on subjects can be placed into multi-jurisdictional databases, and stipulates that "…the officer submitting the [individual, organization, group or business], must have enough information" to believe that the entity is involved in criminal activity, and such information cannot be part of an extra-jurisdictional database "automatically" unless such specific criminal belief can be articulated, and information on source reliability and validity be tracked for each subject entry (28 CFR Part 23: A Guideline). The regional or local approach would allow information to be stored in local agency databases that would then become nodes to a larger assessment platform; filters would not be necessary at this level, which would remove at least one barrier from the information entry gateway. Automated analytics could then assess this information at the local agency level and identify those elements that might allow an analyst to articulate a specific criminal belief, and thus, share this information across jurisdictional lines. An argument can also be made that in the case of some critical information sources, such as criminal incident reports, arrest warrants, arrest reports, and reasonable suspicion stops, a reasonable suspicion that a crime will occur or has occurred is intrinsic to the data, and thus, the specific criminal belief test would successfully be met, and thereby allow these elements to be shared with the national ISE. Volume would be increased as the human gatekeeper would no longer limit potentially critical data from reaching the environment. Velocity would be improved as the human delay point would be eliminated, and direct integration with allowable data sources would improve timeliness. Variety would be expanded based on additional access to direct data sources.

2. Add Analytics Capabilities

To reach the highest state of Business Intelligence, advanced data analytics capabilities would need to be added to the platform by utilizing

predictive and “Big Data” capabilities. Big Data refers to massive sets of information that exceed traditional approaches to collection, storage, and analysis and that demand new methods to leverage (Franks, 2012, p. 4). Working groups, including participants from the commercial, academic, military, health care, and criminal justice spaces, would need to participate in an effort similar in complexity and probably cost to the most complex technical efforts undertaken by human kind. Volume, velocity, and variety must be present: enough information, without delay, and of adequate breadth and scope to allow Business Intelligence activities to occur that will allow the data to be useful. Analytics need to occur at the regional and national levels. Thus, machines are assessing vast quantities of information, conditions outside the baseline of expected activity, and performing the functions they are good at, but the human analyst is still performing critical functions assisted by new analytics tools and informed by more data from more sources.

3. Make Reporting Requirement Mandatory

Perhaps most importantly, SAR submission to the regional ISE, along with approval for sharing critical information with the national ISE, must become mandatory. The reference models discussed in this thesis, including FinCEN, the PND, and the military’s use of persistent surveillance, do not allow discretion to play a role in event submission, this occurs either automatically (in the case of direct access to source data from the various INTs, for example; or on a mandatory basis when certain criteria are met (in the case of FinCEN), which effectively removes at least one potential point of failure, an analyst lacking imagination to recognize the potential value of a component of information and failing to submit it. The ISE needs both, real-time access to automated information sources along with mandatory SAR submissions when analysts become aware of suspicious activity that might have a nexus to terrorism. Reporting should not be optional.

Privacy proponents will overwhelmingly oppose these recommendations. Utilizing the bottom-up approach will enable this strategy to be implemented with the support of the public and with the involvement of privacy advocates, who will prefer this method to the top-down federal approach. Individual states will be free to establish criteria for SAR submissions and automated data transfers based upon community standards and the capabilities of the agencies that comprise the local jurisdictions. Some states, due to levels of technology advancement, may be required to adopt a manual process for some information entry. The key to this approach is the decentralized, local control that will allow for greater potential for public acceptance. Since data is collected at the local level primarily for local use, the processes and procedures for collection, verification, and updating such information are also local, as are rules that might vary from jurisdiction to jurisdiction (Taipele, 2003, p. 42), which is both the position of this thesis and of Taipele.

Figure 4 depicts this Multi-ISE scenario, in which no human barrier exists to information entry to the regional ISE; in addition, a human vetting process occurs before information may be pushed to the national ISE (with some exceptions, if allowable, for those data sources that represent criminal activity, such as arrest reports, criminal incident reports, and reasonable suspicion stops).

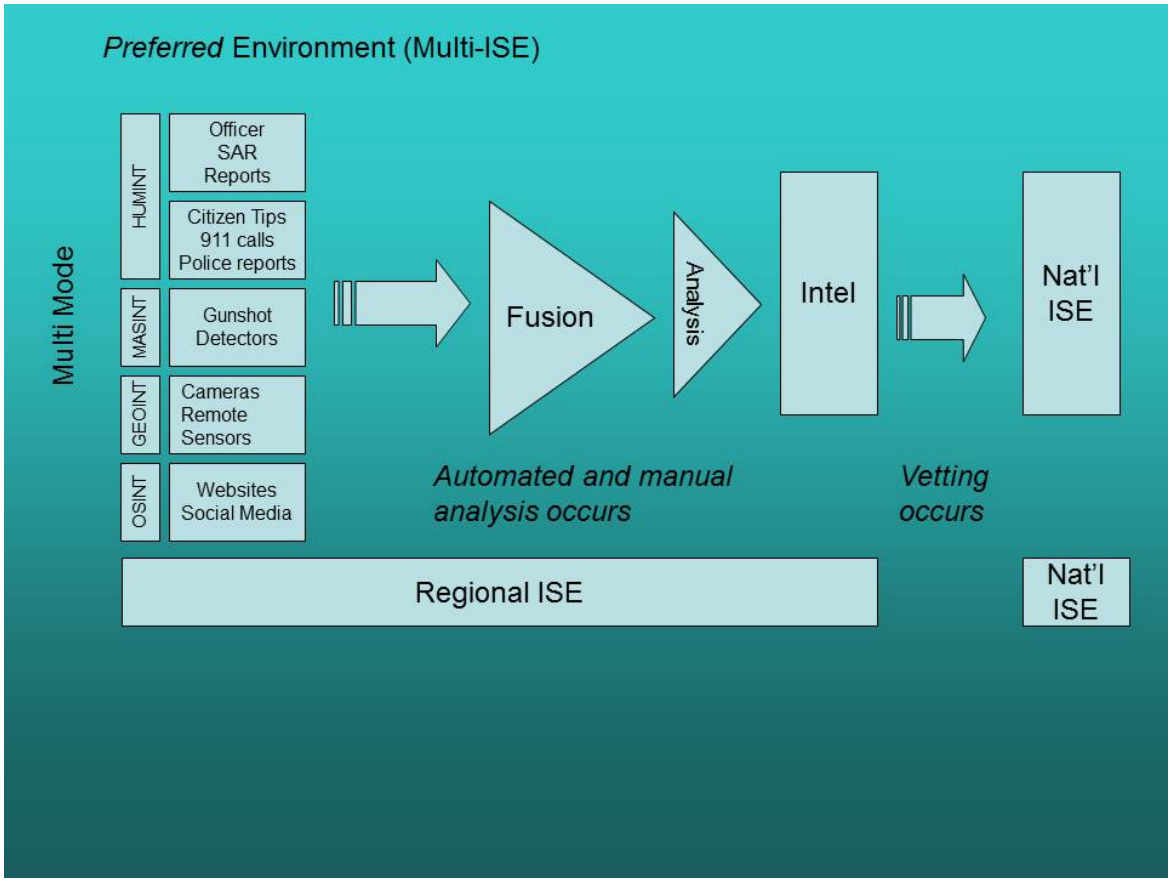

Figure 4. Preferred ISE/SAR Environment

Systems and processes need to be designed to compensate for human frailty whenever possible, to the extent practical, given that humans, of course, design the systems and processes themselves. A system can be designed so that as many points of human decision making as possible are removed, and remaining human decision points can be spread across a group of people, and ideally, in different locations to remove the danger of cross contamination to help ensure that the dependency is not limited to a single point of failure. Humans will always be involved in various stages of the intelligence analysis process, but removing barriers to information availability will at least allow for the concept of "multiple advocacy," which ensures that multiple analysts with varying viewpoints have access to complete data from which to perform analysis activities, and thereby, reduce the negative potential impact of human bias (Butterfield, Jr.,

1993, p. 55). The challenge is to remove barriers while protecting the rights of the public. In *Terror and Consent*, Bobbitt suggests that, “Most of the rules that have hamstrung U.S. agencies in the wars against global terrorism are not constitutional in nature,” but rather arose from the 1970s and the “ugly” practices by some federal agencies disclosed after Watergate (Bobbitt, 2008, p. 318). As Bobbitt suggests, “some increases in the power of the State may increase, or at the least do not diminish, the liberties of the People” (Bobbitt, 2008, p. 314). An opportunity thus arises to begin trusting the government with additional power to ensure that liberties remain intact.

C. THE PATH FORWARD

The ISE was established to address key intelligence failures that occurred prior to 9/11. In its current state, it cannot meet its design objectives because it is hampered by a lack of data necessary to form a complete operating picture and lacks analytical tools to identify emerging conditions, patterns, and trends across data elements. This lack of information is due to an overreliance on the human decision-making process, which creates an unnecessary barrier to information entry. When compared to reference models, such as FinCEN and the PND, and private sector best practices, the ISE performs poorly in key measurement areas, such as volume, velocity, and variety of information necessary to provide an effective assessment platform. It is impossible to assess its performance completely, due to limited and largely qualitative, anecdotal reporting metrics when compared to more mature platforms, such as FinCEN. In its current manifestation, the very lack of human imagination that is at the root of most historical intelligence failures (including 9/11) is not only present but amplified in the ISE, which thereby ensures that this same lack of imagination will limit the performance of this platform.

To address these shortcomings, the successful national fusion center model, in which regional centers engage in the intelligence process at a decentralized level, should be strengthened and should allow appropriate

information to be aggregated up to a centralized assessment framework. In this way, process rules can be established and enforced at the regional level, under local and state control, with a more comprehensive level of data available for assessment from all potential sources (including such areas as open source social media and police databases, in addition to suspicious activity reports completed by human analysts). Concepts of Big Data, such as information volume, velocity, and variety, can be integrated into these regional centers, which can develop analytics tools for assessment and identification of patterns and trends at the regional level. The national ISE can access appropriate, allowable information from these regional centers, with privacy controls built in to the systems themselves. For example, personal identifier information can be stripped from the data shared to the national platform, which would still allow analytics to occur but with references to contact local authorities to learn specific personal identities. The DHS, which takes a leadership role in the fusion center process, needs to become a champion for developing these improvements and an improvement plan to facilitate desired outcomes.

LIST OF REFERENCES

The 9/11 commission report: Final report of the national commission on terrorist attacks upon the United States. (2004). New York: Norton.

Aftergood, S. (2009, June 2). *National Crime Information Center (NCIC)*. Federal Bureau of Investigation. Retrieved from American Federation of Scientists website: http://www.fas.org/irp/agency/doj/fbi/is/ncic.htm

Ang, G., & Luikart, K. (2003). Transforming homeland security: Intelligence indications and warning. *Air & Space Power Journal*, *17*(2), 69.

Ariely, D. (2008, December). *Dan Ariely asks, are we in control of our own decisions?* Retrieved from Ted Talks website: http://www.ted.com/talks/dan_ariely_asks_are_we_in_control_of_our_own_decisions.html

Bamberger, K. A. (2010). Technologies of compliance: Risk and regulation in a digital age. *Texas Law Review 88*(4).

Berkowitz, B. (2008, Spring). The R & D future of intelligence; The U.S. intelligence community faces a changing landscape. Here is a blueprint for how it can best harness the potential of technology. One key: Foster risk-taking. *Issues in Science and Technology*.

Big Data. (n.d.). *What is big data?* Retrieved from SAS website: http://www.sas.com/big-data/

Bjelopera, J. P. (2010, June 10). *Terrorism information sharing and the nationwide suspicious activity report initiative: Background and issues for Congress* (Congressional Report No. R40901). Washington DC: Library of Congress Congressional Research Service.

Bobbitt, P. (2008). *Terror and consent: The wars for the twenty-first century*. New York: A. A. Knopf.

Brehm, R. P. (2012). *What CIOs and CTOs need to know about big data*. Eugene: University of Oregon.

Brinner, R. (2011). Suspicious activity reports: Shifting the analytical paradigm. In Richard Wright (Ed.), *Criminal Intelligence for the 21st Century*. (pp. 1–12). Richmond: LEIU & IALEIA.

Burke, P. A. (2009). *Collecting and connecting the dots leveraging technology to enhance the collection of information and the dissemination of intelligence* (master's thesis). Naval Postgraduate School, Monterey, CA.

Butterfield, Jr., A. P. (1993). *The accuracy of intelligence assessment: Bias, perception, and judgment in analysis and decision* (master's thesis). Naval War College.

Chambliss, S. (2005). We have not correctly framed the debate on intelligence reform. *Parameters 35*(1).

Colby, E. A. (2007). Making intelligence smart. *Policy Review* 144, 71.

Dahl, E. J. (2011). The plots that failed: Intelligence lessons learned from unsuccessful terrorist attacks against the United States. *Studies in Conflict & Terrorism 34*(8), 621–48.

Dewey, E. R., & Dakin, E. F. (1947). *Cycles: The science of prediction*. New York: H. Holt and Company.

DHS/DOJ fusion process technical assistance program and services activity overview. (2012). 26th ed. District of Columbia: DHS/DOJ.

Diaz, G. (2005). *Methodological approaches to the concept of intelligence failure*. UNISCI Discussion Papers.

Duarte, N. (2007). *Unleashing our untapped domestic collection is the key to prevention* (master's thesis). Naval Postgraduate School, Monterey, CA.

Dubber, M. D. (2005). *The police power: Patriarchy and the foundations of American government*. New York: Columbia University Press.

Dumbill, E. (2012). *Planning for big data*. Sebastopol: O'Reilly.

Eckerson, W. W. (2007). *Predictive analytics: Extending the value of your data warehousing investment*. Retrieved from Toolbox.com website: http://hosteddocs.ittoolbox.com/sas-predictive-analytics-062508.pdf

Edmondson, A. C. (1996). Learning from mistakes is easier said than done: Group and organizational influences on the detection and correction of human error. *The Journal of Applied Behavioral Science 32*(1), 5–28.

The Egmont Group of Financial Intelligence Units. (n.d.). Retrieved from http://www.egmontgroup.org/.

Executive Office of the President. Office of Science and Technology Policy. (2012, March 29). *Obama administration unveils big data initiative: Announces $200 million in new R&D investments*. Retrieved from the White House website: http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release_final_2.pdf

Federal Bureau of Investigation. (2008, September 19). *Connecting the dots with EGuardian*. Retrieved from http://www.fbi.gov/page2/sept08/eguardian_091908.html

Financial Crimes Enforcement Network. (n.d.). *History of anti-money laundering laws*. Retrieved from http://www.fincen.gov/news_room/aml_history.html

Financial Crimes Enforcement Network. (2011, December). *Financial crimes enforcement network annual report 2011*. Retrieved from http://www.fincen.gov/news_room/rp/files/annual_report_fy2011.pdf

Franks, B. (2012). Taming the big data tidal wave: Finding opportunities in huge data streams with advanced analytics. Hoboken, NJ: John Wiley & Sons.

Forsman, S. (1997). *OLAP council white paper*. Retrieved from OLAP Council website: http://www.olapcouncil.org/research/whtpaply.htm

Fusion center guidelines. (2005, July). Retrieved from Federation of American Scientists website: http://www.fas.org/irp/agency/ise/guidelines.pdf

Government Technology. (2010, August 9). *Chicago using predictive analytics to fight crime*. Retrieved from http://www.govtech.com/public-safety/Chicago-Using-Predictive-Analytics-to-Fight.html

Grabowski, M., & Roberts, K. H. (1996). IEEE systems, man, and cybernetics society. *IEEE Transactions on Systems, Man, and Cybernetics 26*(1), 2–16.

Graves, P. (2011). Need it now! Banks are getting serious about business intelligence. they have to, in order to cope with market and regulatory demands. *ABA Banking Journal 103*(6).

Greenwood, C. (2011, June 17). *One in four Britons put on new police database*. Retrieved from Mail Online website: http://www.dailymail.co.uk/news/article-2004528/One-Britons-new-police-database.html

Harris, B. (2008, April 20). *Chicago fusion center gives police new criminal investigation tools*. Retrieved from Digital Communities website: http://www.digitalcommunities.com/articles/Chicago-Fusion-Center-Gives-Police-New.html

Hoffman, R. R. (2007). *Expertise out of context: Proceedings of the sixth international conference on naturalistic decision making*. New York: Lawrence Erlbaum Associates.

Hollywood, J., & Pope, M. (2009). *Building on clues: Methods to help state and local law enforcement detect and characterize terrorist activity*. Research Triangle Park: Institute for Homeland Security Solutions.

Hutchins, S. G., Pirollo, P. L., & Card, S. K. Card. (2007). *What makes intelligence analysis difficult?: A cognitive task analysis. Expertise out of context*. Robert Hoffman (Ed.). New York: Taylor & Francis.

IMPACT Programme: *Police national database—Privacy impact assessment report* (2009). London: National Policing Improvement Agency.

Information Sharing Environment. (2011, June 30). *ISE annual report to the Congress*. Retrieved from http://ise.gov/sites/default/files/ISE_Annual_Report_to_Congress_2011.pdf

Intelligence Reform and Terrorist Prevention Act of 2004 (2004).

Jonas, J., & Harper, J. (2006). Effective counterterrorism and the limited role of predictive data mining. *Policy Analysis 584*.

Jones, C. (2007). Intelligence Reform: The Logic of Information Sharing. *Intelligence & National Security 22*(3), 384–401.

Kimmons, J. F. (2008, October). Accelerating Army intelligence transformation. *Army*.

Kobielus, J. (2010, February 4). *The forrester wave: Predictive analytics and data mining solutions*. Retrieved from Oracle website: http://www.oracle.com/ocom/groups/public/@ocom/documents/webcontent/050922.pdf

Lapide, L. (2004). Sales and operations planning part Ii: Enabling technology. *The Journal of Business Forecasting Methods & Systems 23*(4).

Lowenthal, M. M. (2008). Towards a reasonable standard for analysis: How right, how often, on which issues? *Intelligence and National Security 23*(3), 303–15.

Lowenthal, M. M. (2009). *Intelligence from secrets to policy*. Washington, DC: CQ-Press.

Malphrus, S. (2009). Perspectives on retail payments fraud. *Economic Perspectives 33*(1).

McNeill, J. B. (2010). Keeping the homeland free, safe, and prosperous. *America at Risk, 10*(4), 1.

Moghaddam, F. M. (2011). *Multiculturalism and intergroup relations: Psychological implications for democracy in global context*. Washington, DC: American Psychological Association.

Nationwide SAR Initiative. (n.d.a). *A call to action: A unified message regarding the need to support suspicious activity reporting and training*. Retrieved from http://nsi.ncirc.gov/documents/A_Call_to_Action.pdf

Nationwide SAR Initiative. (n.d.b). *Nationwide SAR initiative 2011 annual report*. Retrieved from http://nsi.ncirc.gov/documents/NSI_Annual_Report_2011.pdf

Nationwide SAR Initiative. (2008, December). *Nationwide suspicious activity reporting initiative concept of operations.* Retrieved from http://nsi.ncirc.gov/documents/NSI_CONOPS_Version_1_FINAL_2008-12-11_r4.pdf

Nationwide SAR Initiative. (2010, January). *Final report: Information sharing environment suspicious activity reporting evaluation environment*. Retrieved from http://nsi.ncirc.gov/documents/NSI_EE.pdf

Office of the Director of National Intelligence. (n.d.). *Library of national intelligence.* Retrieved from http://www.dni.gov/content/AT/LNI.pdf

Paul, K. N. (2010). *Information Sharing Environment Annual Report to Congress*.

Pearsall, B. (2010). Predictive policing: The future of law enforcement? *NIJ Journal 266.*

Pendall, D. W. (2005). Persistent surveillance and its implications for the common operating picture. *Military Review 85*(6).

Pfeifer, J. W. (2007). Understanding how organizational bias influenced first responders at the world trade center. In B. Michael (Ed.), *Psychology of terrorism*. (207–15). Bongar. Oxford: Oxford UP.

The Police National Computer (PNC). *The PNC or police national computer*. (n.d.). Retrieved from InBrief website: http://www.inbrief.co.uk/police/police-national-computer.htm

The PND: Making a difference (Rep.). (2010). London: National Policing Improvement Agency.

Reuter, P., & Truman, E. M. (2004). *Chasing dirty money: The fight against money laundering*. Washington, DC: Institute for International Economics.

Rich, T. F. (1996, July). *The Chicago Police department's information collection for automated mapping (ICAM) program*. Retrieved from Abt Associates website: http://www.abtassociates.com/reports/icamprog.pdf

Rovner, J., & Long, A. (2005). The perils of shallow theory: Intelligence reform and the 9/11 commission. *International Journal of Intelligence and CounterIntelligence 18*(4), 609–37.

Seifert, J. W. (2007, January 18). *Data mining and homeland security: An overview*. (Congressional Report No. RL31798). Washington DC: Library of Congress Congressional Research Service.

Serious Organised Crime Agency. (n.d.). *The impact of SARs in reducing crime.* Retrieved from https://www.ukciu.gov.uk/(rkzecdfuf2ybj455i0hcu120)/Information/Info.aspx

Starr, B. (1998). Data mining is vital to intelligence-gathering. *Jane's Defence Weekly 029*(003).

Steiner, J. E. (2010, September 3). *More is better: The analytic case for a robust suspicious activity reports program*. Retrieved from Homeland Security Affairs Journal website: http://www.hsaj.org/?fullarticle=6.3.5.

Straw, J. (2010, March 24). *Terror threat tracking system shares thousands of tips from locals, FBI says*. Retrieved from Security Management website: http://www.securitymanagement.com/print/6888

Strom, K., Hollywood, J., Pope, M., Weintraub, G., Daye, C., & Gemeinhardt, D. (2010). *Building on clues: Examining successes and failures in detecting U.S. terrorist plots, 1999–2009*. Research Triangle Park: Institute for Homeland Security Solutions.

Taipale, K. A. (2003). Data mining and domestic security: Connecting the dots to make sense of data. *Columbia Science and Technology Law Review 5*(2).

Taleb, N. (2007). *The black swan: The impact of the highly improbable*. New York: Random House.

Technology update. (2007, Summer). Retrieved from Chicago Police Department website: https://portal.chicagopolice.org/portal/page/portal/ClearPath/News/Department%20Publications/TechUpdate07.pdf

Terrorist screening center. (n.d.). Retrieved from Federal Bureau of Investigation website: http://www.fbi.gov/about-us/nsb/tsc

Vision 2015: A globally networked and integrated intelligence enterprise. (2008). District of Columbia: United States Office of the Director of National Intelligence.

Weigle, B. D. (2007, March 30). *Prediction markets: Another tool in the intelligence kitbag*. Retrieved from The Homeland Security Digital Library website: https://www.hsdl.org/?view&did=8661

Werner, R. W. (2006, October 9). *Prepared remarks of Robert W. Werner, director financial crimes enforcement network before the American bankers association/American bar association money laundering enforcement conference.* Retrieved from Financial Crimes Enforcement Network website: http://www.fincen.gov/news_room/speech/pdf/20061009.pdf

Wernick, M., & Yang, Y., Brankov, J., Yourganov, G., & Strother, S. (2010). Machine learning in medical imaging. *IEEE Signal Processing Magazine 27*(4), 25–38.

The White House. (n.d.). *NSIS—Introduction and overview.* Retrieved from http://georgewbush-whitehouse.archives.gov/nsc/infosharing/sectionI.html

Widder, A., Ammon, R. V., Schaeffer, P., & Wolff, C. (2007). *Identification of suspicious, unknown event patterns in an event cloud. Proc. of 2007 inaugural international conference on distributed event-based systems, Toronto, CA*. New York: ACM.

Written testimony, 112th Cong., 5 (2012) (testimony of Mary Ellen Callahan and Richard Chávez).

Zikopoulos, P. (2012). *Understanding big data: Analytics for enterprise class hadoop and streaming data*. New York: McGraw-Hill.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California