ORGANIZATIONAL CULTURE’S EFFECTS ON INFORMATION SHARING
WITHIN THE UNITED STATES INTELLIGENCE COMMUNITY

A Thesis
submitted to the Faculty of
The School of Continuing Studies
and of
The Graduate School of Arts and Sciences
in partial fulfillment of the requirements for the
degree of
Master of Arts in Liberal Studies

By

Alexander E. Montgomery, B.S.

Georgetown University
Washington, D.C.
March 20, 2012
ORGANIZATIONAL CULTURE’S EFFECTS ON INFORMATION SHARING
WITHIN THE UNITED STATES INTELLIGENCE COMMUNITY

Alexander E. Montgomery, B.S.

Mentor: Burton L. Gerber, B.A.

ABSTRACT

A major factor contributing to national security failures in the United States is the inability of the Intelligence Community to share information effectively. This failure is rooted within the organizational culture of the Intelligence Community. The U.S. government has failed to adequately identify, conceptually understand, and address culture as an impediment toward information sharing, particularly before September 11, 2011. This thesis examines the concept of organizational culture and its effect on information-sharing efforts. The author contends that the unique culture of agencies within the Intelligence Community is necessary to their mission success, but it may also inhibit the effective exchange of information. Using Edgar Schein’s theory and model of organizational culture, this thesis analyzes the culture of the Office of the Director of National Intelligence and the Federal Bureau of Investigation, with an eye toward how those cultures affect information sharing. The Office of the Director of National Intelligence is tasked with the mission of promoting information sharing across the Intelligence Community; however, its inability to conceptually grasp and apply key principles of organizational culture to its policies and initiatives has hindered the community’s ability to adhere to its guidance. The Federal Bureau of Investigation
struggles to move from a law enforcement culture to an intelligence-driven culture in support of those law enforcement efforts. Through understanding and applying the principles of organizational culture, the Intelligence Community will have the opportunity to improve its information-sharing environment.
PREFACE

In the course of this research, I interviewed three members of the Intelligence Community who had direct knowledge of the issues at hand. All interviews were confidential; the names of interviewees were withheld by mutual agreement.

I would like to express my sincere appreciation for the guidance of my mentoring professor, Burton L. Gerber, and for the patience and encouragement of my family and friends. Their support made this work possible.
FIGURES

Figure 1. Three levels of culture ................................................................. 48
Figure 2. ODNI 2008 Information Sharing Strategy .......................... 54
Figure 3. Primary and secondary culture-embedding mechanisms in the form of artifacts ................................................................. 88
CHAPTER 1

INTRODUCTION

In order for the Intelligence Community to execute its mission of protecting national security interests, the timely, accurate, and relevant sharing of information must occur. Within the Intelligence Community, information sharing can be defined as the exchange of intelligence (and related data) among individuals or organizations. How information sharing occurs and the ways it can be improved has been a significant issue that the Intelligence Community has worked diligently to address in recent years. Many potential causes have been identified for the inability of the Intelligence Community to share information effectively, such as, but not limited to, technology, data interoperability, policy, standards, leadership, and a unified architecture. What the Intelligence Community has failed to examine and conceptually understand to a detailed extent, however, is the effect that organizational culture has within its information-sharing environment.

The organizational culture of the Intelligence Community allows its agencies to achieve their specific missions, but by the same token often hampers those agencies’ ability to share information effectively with one another, thus affecting overall mission achievement. Edgar Schein, Massachusetts Institute of Technology professor and subject-matter expert on organizational culture and behavior theory, defines organizational culture as the shared attitudes, beliefs, and psychology developed by an organization’s members to adapt and thrive (Schein 2010, 18). As members develop
those traits necessary to adapt and survive within their respective organizations, the
shared coping mechanisms become engrained within the culture of the organization
and are passed on to new members as the appropriate way to perceive, think, and feel
in relation to their environment and challenges.

Organizational culture is a collective and learned pattern of behaviors passed
along by its membership. The Intelligence Community is a coalition of seventeen
federal agencies, each with incredibly diverse and complex memberships and
relationships. Therefore, it is important to examine the effect organizational culture
poses on the Intelligence Community membership’s ability to share information. The
National Commission on Terrorist Attacks upon the United States, commonly known
as the 9/11 Commission, cited the failure to share information effectively as a key
factor that might have prevented the attacks on the World Trade Center, the Pentagon,
and United Flight 93.

The 9/11 Commission official report detailing the causes of the attacks has
since inspired a myriad of policies, directives, and executive orders all geared toward
improving information sharing. These initiatives are well intended and designed to
promote national security interests. However, through the analysis of such policy
reform and initiatives it will become evident that the U.S. government has inadequately
identified organizational culture as a cause for ineffective information sharing. The
organizational culture of the Intelligence Community may impede the effective sharing
of information often necessary to prevent security failings.
Using Schein’s theory of organizational culture as a lens, this thesis will examine the extent to which organizational culture has impeded information sharing within the Intelligence Community. Such impediments will be examined further with analysis focused on the individual cultures of the Office of the Director of National Intelligence (ODNI) and the Federal Bureau of Investigation (FBI).
CHAPTER 2
THE INTELLIGENCE COMMUNITY:
LEARNING TO SHARE

The Intelligence Community embodies multiple agencies and organizations tasked to collect and analyze intelligence for the purpose of promoting national security and informing key government leaders and decision-makers. The mission of protecting national security often requires a necessary level of secrecy by the Intelligence Community, while simultaneously ensuring information is shared and readily available. In this paradigm, performing specific job functions, such as intelligence analysis, while attempting to preserve secrecy is often difficult to reconcile.

The 9/11 Commission extensively reviewed such challenges, among many others. The commission was established to determine the security failures that had occurred resulting in the September 11, 2001, tragedies. The commission’s investigation revealed that information had not been shared in a timely and appropriate manner among agencies within the Intelligence Community; had such information been shared, the 9/11 attacks may have been prevented. The organizational culture of the Intelligence Community took the route of preserving secrecy, as opposed to sharing information. This thesis will examine the information-sharing challenges surrounding 9/11, as well as the potential effect of organizational culture on those efforts.

The agencies and organizations responsible for the oversight and action of U.S. intelligence initiatives are diverse and evolving. The Office of the Director of National
Intelligence (ODNI) heads the Intelligence Community, which comprises a large number of agencies, and a myriad of organizations whose missions, scopes, and reach are specialized to meet specific functions. There are 1,271 government organizations and 1,931 private companies in 10,000 U.S. locations that support the Intelligence Community (Priest and Arkin 2010, para. 4).

The 9/11 Commission’s 2004 investigation determined that a failure to share information was a major cause of the September 11, 2001, terrorist attacks. In its findings, the commission states that several challenges existed within the Intelligence Community preceding the attacks, which included a limited capacity to share information both internally and externally, limited intelligence-collection capabilities, limited strategic analysis, poor training, perceived legal barriers to the sharing of information, and inadequate resources (9/11 Commission 2004c, under “Problems with the Intelligence Community”). The Government Accountability Office (GAO) backed the commission’s findings in its “Reorganization, Transformation, and Information Sharing” report, which states the need for transformation within the entire Intelligence Community, moving from a need-to-know to a need-to-share environment (Walker 2004b, para. 1).

The Intelligence Community has undertaken significant efforts to improve its information-sharing efforts as a result of the investigations post-9/11. However, with increased efforts to improve information sharing there also exist potential security concerns. To illustrate one specific example, the Department of Defense (DoD) Netcentric Warfare Strategy (Holmes 2012, under “Why Should I Care?”) was created
in the aftermath of 9/11 as one initiative to improve information sharing. The strategy is essentially a database that provides for the alignment of military intelligence, using multimedia data management to move information seamlessly among strategists. Controversy immediately ensued, as the Pentagon asserted that the database was nonproprietary and should be shared with the entire Intelligence Community, not just the DoD. The Pentagon called for the relinquishing of rights from any one agency; thus, the underlying tone was that an obligation, perhaps even moral, existed to share these data openly with all members of the Intelligence Community (Holmes 2012, under “Why Should I Care?”).

There is legitimate need for concern, however, particularly in the aftermath of WikiLeaks, which released a wealth of secret and transmitted government documents, including the “collateral murder” video (WikiLeaks 2010) and State Department cables allegedly leaked by U.S. Army private Bradley Manning, a 23-year-old intelligence analyst, who asks:

If you had free reign over classified networks … and you saw incredible things, awful things … things that belonged in the public domain, and not on some server stored in a dark room in Washington DC … what would you do? … I want people to see the truth … because without information, you cannot make informed decisions as a public [boldface in original]. (Bradley Manning Support Network n.d., para. 1–2)

The ongoing battle between providing information to all while maintaining the appropriate level of secrecy is illustrated by the case of Manning, who allegedly abused the access to information he was provided. The excerpt stresses the issue facing the Intelligence Community in that the greater the flow of information among mission
partners, the greater is the risk for security breaches. However, an argument could be made that increasing information-sharing efforts that allow people like Manning wide, unprohibited access to classified intelligence is only one piece of the overall problem.

The separate issue that may be raised is that people like Manning were allowed to become a part of the Intelligence Community to begin with, and that a failure exists within the community’s indoctrination process of new intelligence professionals. For a person to become a member of the Intelligence Community and be granted a security clearance, he or she must pass a background investigation, which involves screening that person’s history, including drug use, and a criminal history check. Psychological tests to screen for overall mental health are also administered.

Although Manning will eventually stand trial, it could very well be deemed that the point of failure was the Intelligence Community’s inability to conduct a rigorous background investigation or execute counterintelligence/security measures in a timely and appropriate fashion, which would have caught Manning long before he allegedly released secret information to the public. At this point, the cause for the inability to prevent the Manning security failure is still speculation and under investigation, but it raises interesting questions concerning promoting an Intelligence Community culture of “need to share” versus a “need to know.”

When summarizing the Intelligence Community’s challenges to information sharing, it is also necessary to cite the issues in collaboration between the FBI and the Central Intelligence Agency (CIA) with respect to the 9/11 security failings. The CIA was aware of the presence of two 9/11 terrorists in the United States before the attacks;
however, the FBI had not been informed, and the August 23, 2001, all-points bulletin came too late for the FBI to track them down.

The CIA/FBI information-sharing breakdown leading up to 9/11 is a brief summary of what occurred. The point is necessary to make up front in the problem summary, however, because it addresses an issue larger than just the CIA and FBI. The issue is that unlike the aforementioned example concerning the DoD’s best efforts to share information, which backfired, serious communication breakdowns existed between the FBI and CIA leading up to 9/11. There are examples that illustrate security failings associated with both the sharing of information and the lack of sharing of information. It would appear that the country is in a “no win” situation, because security risks are associated with each scenario. It is the intent of this thesis to shed light on how organizational culture affects such information-sharing challenges.

The complex relationships within the Intelligence Community are often as confusing as the abundance of information-sharing initiatives and policies that seek to promote the effectiveness of the information-sharing environment. The ability to distinguish and decipher who shares information with whom is often challenging, as in many cases information-sharing efforts are redundant, overlap, or are seemingly disconnected.

In an effort to clear any potential confusion given the wealth of policy documentation resulting from the 9/11 attacks, it is only necessary to summarize the key information-sharing initiatives and policies that have driven information-sharing efforts post-9/11 and the extent to which organizational culture was (or was not)
identified as affecting the information-sharing environment. Further analysis within this thesis will seek to explore how organizational culture affects agencies within the Intelligence Community by exploring the specific culture of the ODNI and FBI.
Information-sharing challenges date back as early as the 1970s within the FBI. In 1995, the information-sharing challenges that the FBI faced became more apparent. Before the 9/11 attacks, the 9/11 Commission investigation found formal information-sharing initiatives commenced in July 1995 under the direction of then-Attorney General Janet Reno, who moved to link Justice Department prosecutors and the FBI; these procedures required the FBI to share intelligence with prosecutors within a highly regulated process.

The commission found that the procedures were “immediately misunderstood and misapplied,” ultimately resulting in what is commonly referred to as “the wall,” meaning that even greater barriers were erected under this policy (9/11 Commission 2004b, 79). The commission concluded that the divide was due to the Department of Justice (DOJ) Office of Intelligence Policy and Review’s unauthorized assumption of the role of sole gatekeeper for passing data to the Criminal Division. With the DOJ threatening to wield its powers, the information flow stagnated.

Additionally, the commission addressed the limited application of the 1995 procedures, which spoke only to sharing between the FBI and prosecutors, entirely overlooking two critical types of agent positions: intelligence analysis and criminal investigations. Misinterpretation of the Foreign Intelligence Surveillance Act (FISA)
(Library of Congress 2003, 4) and misuse of authority further confused the information-sharing environment between the roles of analysis and investigations within the FBI.

FISA prescribes guidance for the surveillance and collection of foreign intelligence information by foreign powers and agents of foreign powers, which may include U.S. citizens. “FBI Deputy Director Bryant reinforced the Office’s caution by informing agents that too much information could be a career stopper. Agents in the field began to believe—incorrectly—that no FISA information could be shared with agents working on criminal investigations” (9/11 Commission 2004b, 79).

Additionally, before 9/11, the FBI operated under an “origin of office” system as a means of avoiding duplication and conflicts throughout the ranks. The 9/11 Commission says that this segregation provided no incentive to receive assistance from other field offices, which lacked authority in the investigation as well as recognition for their achievements.

Decades of change in regulations and activity resulted in the 1998 FBI designation of terrorism as a top priority. Deputy Director Bryant said, “Cultural change had to occur within the FBI.” The plan mandated:

1. Stronger intelligence collection efforts;
2. A nationwide, automated system to facilitate the collection, storage, analysis, and dissemination of data;
3. A professional intelligence cadre of experienced and trained analysts.

(9/11 Commission 2004b, 76)
The plan failed. The commission asserts that the success of this strategy would have championed a new era of systematically addressing terrorism by taking a holistic approach to identification and response. The stated reasons for this failure include an inability to restructure human capital and misallocation of funding to reflect this reprioritization.

Overall, mismanagement is the root of this breakdown. Organizational leaders lacked the experience and insight to effect cultural change. Instead, the problem was compounded. The commission identifies the following inefficiencies in Bryant’s plan: (1) failure to comprehend the role and significance of analysis in counteracting terrorism; (2) lack of an effective intelligence collection effort; (3) nonexistent source validation schemes; (4) misuse of funds; and (5) woefully inadequate information systems (9/11 Commission 2004d, para. 40). Even the FBI could not access or decipher its information base, let alone participate in relevant data transmission and knowledge management.

The 9/11 Commission reports that three separate reviews conducted in 1999, 2000, and 2001 independently confirmed that information sharing was nearly nonexistent and routinely ignored. Furthermore, perception continued to cripple collaboration, as both prosecutors and agents cited legal limitations barring sharing grand jury information. The FBI, maintaining its interpretation despite policy allowances, applied this silencing to the mass of information discovered during the investigation.
Executive orders compounded the issue by discouraging the “co-mingling of domestic information with foreign intelligence,” while the National Security Agency (NSA) began blocking criminal investigator and prosecutor access to Osama bin Laden reports (9/11 Commission 2004b, 80). Even in the deliberate attempt to open the pipelines of information flow, the agencies and actors resisted these objectives, overtly and subtly, intentionally and unintentionally stunting mutual advantage.

The Federal Aviation Administration

The 9/11 Commission reports that the Federal Aviation Administration (FAA) was caught in a conflict of what it perceived to be contradictory goals, given the breadth of its mission. The FAA’s responsibility for the conflicting goals of industry safety while enforcing security regulation muddied the vision of the administration. Using historical precedence, the FAA placed sabotage as a greater threat than hijacking and similarly ranked explosives as a greater concern than firearms; the possibility of suicide hijackings failed to hit the radar.

Historically, the FAA rarely had to address domestic hijacking security threats or potential scenarios. The majority of the FAA threats came from potential sabotage to aircraft, such as the intentional tampering of wires aboard Boeing planes in 2001 (Isidore 2012). The FAA security plan took a layered approach to systematic defense under the assumption that failure at one layer would not destabilize the entire systems of continued checks and balances. “But each layer relevant to the hijackings—intelligence, passenger prescreening, checkpoint screening, and onboard security—was
seriously flawed,” as evidenced by the fact that none of the hijackers was stopped in any of the three airports or the four aircraft boarded (9/11 Commission 2004b, 83).

FAA policy relied on external intelligence to assist in specific and general threat identification. The 40-member FAA intelligence unit received data from other national security agencies, chiefly the FBI and the CIA. However, of the large volume of information disseminated, only a small fraction pertained to terrorist activity within the United States. For example, the FBI’s 1998 report on terrorist flight training or the 2001 FBI’s Phoenix Field Office electronic communication warning of radical Middle Easterners’ attendance of flight training were not delivered to the FAA (9/11 Commission 2004b, 272).

The commission also stated that the FAA intelligence unit responsible for analyzing and processing intelligence reports received from external agencies did not receive the appropriate attention from superiors within the administration. It was concluded that FAA leaders did not take an active role in daily intelligence review, and what intelligence they did review had been provided at only a high level for time efficiency, as opposed to in-depth investigation.

Nowhere within the 9/11 Commission report did the subject of culture arise in connection with the FAA’s intelligence units’ relationship with the administration’s superiors with respect to the review of intelligence reports. From an organizational or cultural perspective, questions should have been raised about the attitudes, belief systems, and standard operating procedures already in place that drove a mindset that
superiors did not need to be given detailed intelligence information, because they were too busy.

The next security layer, passenger screening, consisted of a twelve-name “no-fly” list of terrorists known to pose a direct threat to civil aviation, despite government watch lists containing thousands of known and suspected terrorists. According to the 9/11 report, the FBI and the CIA were ordered to author lists for screening purposes. However, four years after the creation of TIPOFF, a database detailing approximately 60,000 names of potential no-fly suspects, the longtime FAA chief reported no knowledge of its existence. Those FAA employees aware of the resource were denied access, given the supposed difficulty of navigating the system.

The second FAA prescreening component, known as the Computer Assisted Passenger Prescreening System (CAPPS), used algorithms to identify passengers whose risk level might have exceeded minimal risk. However, the 9/11 Commission found that these measures were weak in that CAPPS only monitored passengers who checked baggage. The commission detailed a number of infrastructure, training, and policy facts that destabilized the FAA’s already poor performance and engagement, but failed to mention culture as a potential cause for FAA security failings.

The Intelligence Community

The 1947 National Security Act established the position of Director of Central Intelligence (DCI); this position was separate from other primary and secondary policy programs, including the departments of Defense, State, and Justice. At the time of the
9/11 attacks, the DCI was the head of the entire U.S. Intelligence Community and thus the disseminator of information to the panoply of federal agencies. According to the 9/11 Commission, the CIA was “the sole element of the Intelligence Community” through which data are collected, analyzed, and shared (9/11 Commission 2004b, 86).

The CIA is independent, operating under the president’s direction, including clandestine and covert operations. According to the 9/11 Commission, the DCI’s power was legally limited despite setting agendas and coordinating budgets. The commission found that the DCI’s authority was often misperceived and, in reality, had more do with the personal relationship the director had with the president.

Nearly 80 percent of U.S. Intelligence Community spending is consolidated in the Department of Defense (DoD); this grouping includes the NSA, responsible for intercepting and analyzing foreign communications, codes, and data (9/11 Commission 2004b, 103). “An almost obsessive protection of sources and methods by the NSA, and its focus on foreign intelligence, and its avoidance of anything domestic, would … be important elements in the story of 9/11” (9/11 Commission 2004b, 88).

The commission cites other principal divisions operating within DoD, including all military branches supporting intelligence efforts within the community. The expanse of the intelligence agencies, departments, and branches reveals the interrelated complexity in attempting to understand who should be sharing information with whom. The policies and procedures in place, which were expected to unite the Intelligence Community in its information-sharing efforts, were evidently not strong enough.
The commission’s intricately detailed evaluation of the historical sources of leadership, policy, purpose, and, in some cases, culture logically traces the forces battling one another by demonstrating examples chronologically whereby organizations tended toward compartmentalizing information. For this analysis, there is no need to prove what has already been investigated so deeply; instead, this brief sketch of the commission’s findings bolsters the relevance of information sharing to national security.
CHAPTER 4
SUMMARIZING THE COMMISSION’S STANCE

In view of the 9/11 Commission’s findings, it is my opinion that U.S. intelligence agencies had access to an enormous body of intelligence, including databases that could be integrated to improve analysis and correlation. However, the processing system was cumbersome in some cases, requiring intuition and approval to access data.

The compartmentalization of information is a repeated theme throughout the story leading up to the 9/11 tragedies. The 9/11 Commission concluded that the several agencies within the Intelligence Community often perceived greater benefit and less risk in closely holding information, rather than sharing it. This may plausibly be seen as a primitive mentality, considering the almost overwhelming policies and directives ordering members of the Intelligence Community to share information, and yet information challenges still exist.

Adherence to contemporary methods of information sharing demands cultures that are able to embrace these changes in policies and procedures. To expect the Intelligence Community to share without a fundamental understanding of the organizational culture that drives the attitudes and psychology of individuals not to share to begin with is a mistake. With each agency operating under different directives and security structures, information-sharing capacity is unduly complicated and risky. Additionally, each organization is rooted in incentive structures that deter data sharing.
The system of rewards and punishments predetermines information-sharing products. The 9/11 Commission concluded that upholding a “culture of information protection” rather than a “culture of integration” poses a critical risk to the future safety, security, and responsiveness of the nation (9/11 Commission 2004b, 417). The commission offers the following recommendations to help remedy this vulnerability:

1. *Connect incentives for sharing with formal information procedures to better balance security and data exchange.*

   Intelligence should be set to national quality standards; thus, collected information can then be articulated in reports that are then nationally transferred, regardless of data discovery origin. Understandably, data must be made “sharable” without compromising sources or security; the aim is to minimize extraneous details while maintaining the meaningfulness at a level for maximized distribution. The 9/11 Commission states the need for improved network security and creating a paper trail on all networks that people in the Intelligence Community access. The 9/11 Commission suggests a horizontal sharing of information in a decentralized network model creating shared database access with secrets protected by the design of the network.

2. *Using the “trusted information network” model, the President should lead the intelligence institutions into the information revolution.*

   From the commission’s perspective, national security requires national cooperation and collaboration. This type of cultural shift is a tremendous leap from the historical modus operandi. The existent technology must be integrated and employed. Policy and law are the backbone of this proposed achievement. Strong presidential
leadership and leadership of the Intelligence Community and its agencies must reflect clear communication and guide the acquisition, access, sharing, and use of the vast databases and storage locations. Unleashing the power of data exchange requires practical policy guidelines and constraints to pipeline information effectively and appropriately.

3. Employ a joint-action, joint-intelligence approach.

Though each agency player is distinct in its skill set and focus, the team has one shared goal: winning. This metaphor is applicable to national security; coordination is vital. The commission recognizes through the information-sharing challenges of 9/11 that one agency may have the identity of a suspected terrorist in a report, while another agency may have information regarding the travel patterns of that same terrorist. Management necessitates a comprehensive understanding of organizational needs, talents, and capacities. With this awareness, a manager can strategically deploy intelligence data, actors, agencies, and action while monitoring performance and progress for quick resolution.

The commission’s conceptualization of joint action moves beyond mere coordination, suggesting more intimate tactics to solution strategies. The unified effort ideology is based on the rationale of the advantages of joint planning, shared purpose through leadership, and efficient use of expertise. The commission pairs “joint intelligence” and “joint action,” stating, “A ‘smart’ government would integrate all sources of information to see the enemy as a whole. Integrated all-source analysis
should also inform and shape strategies to collect more intelligence” (9/11 Commission 2004b, 401).

**The GAO in 2004**

The GAO, following the 9/11 Commission report release, addressed the following two issues by commission request: “the lack of effective information sharing and analysis and the need for executive branch reorganization in response to the 9/11 Commission recommendations” (Walker 2004a, 2). GAO Comptroller General David Walker testified that the major transformational challenges facing the Intelligence Community are of the same thread as those facing the government at large, signaling the complexity of reorganizing government, given the severity of both risk and opportunity. Walker illustrates the threat advisory alert system as an effort toward improved and immediate analysis through simplified expression (i.e., alert). Walker also reiterates the commission’s stance on needing to move from the traditional intelligence “need-to-know” presumption with that of a “need to share.”

**Analysis: The Grown-Up Government**

The 9/11 report directly and repeatedly identifies the problem of culture at a superficial level. The commission reports that the Intelligence Community faces information-sharing challenges that were derailed through law, policy, leadership, and infrastructure—all of which influence organizational culture. The government is correct in the sense that these factors do influence culture. Also important are the
attitudes, perceptions, beliefs, and psychology behind the people who are responsible for implementing these changes.

The government has taken a stance that if technology fails, for example, it is necessary to build better technical standards to ensure interoperability among databases, thus improving information sharing. This is a good solution; however, what is the country doing to ensure that the people who use these systems do so appropriately, and to what extent will they feel encouraged to share the information that is available to them?

With factors such as risk versus reward, potential consequences for leaking information, and conflicting policies and guidance, it becomes a challenge for a person using the system to know what to do. Additionally, fear of change—and, therefore, subsequent resistance—marks the discourse. Those reared with the myths of secret handshakes, invitation-only meetings, and other clandestine engagements are skeptical of streamlined technologies, where data can be traced, infiltrated, and compromised.

This skepticism is somewhat rational, because it raises the question of how to protect sources and methods. Understandably, this fear, which dates back to the Cold War era of intelligence forays, is rooted in some level of common sense, especially considering the sophistication of criminality that often transcends the sharpest network security. Undoubtedly, there is a large degree of risk involved in electronic communication, as humans are susceptible to either being victims of security leaks or causing them. However, the point remains that agencies are digitized on the individual level; thus, information is still susceptible to intrusion. These organizations have the
opportunity and responsibility to take a holistic approach to national safety and security. The 9/11 Commission reveals that law, policy, infrastructure, and objectives alone cannot actualize the potential energy behind its research and recommendations.
CHAPTER 5

THE AFCEA REPORT: THE NEED TO SHARE

In 2007, six years following the 9/11 attacks and three years after the 9/11 Commission’s findings, the International Committee of the Armed Forces Communications and Electronics Association (AFCEA) released a white paper entitled, The Need to Share: The U.S. Intelligence Community and Law Enforcement. AFCEA is a nonprofit trade association and lobbying group that the government contracted following 9/11 to document its findings of information-sharing challenges potentially still pervading the Intelligence Community.

The AFCEA report stated that the continued struggles of the Intelligence Community to adapt to redefining its priorities and practices remained an issue. AFCEA reiterated the 9/11 Commission’s findings, underlining the prior division between domestic and international focus, as well as prosecution within the limitations of the Fourth Amendment, which protects U.S. citizens from unreasonable searches and seizures. AFCEA stated that government’s desire to conduct surveillance on its citizens in the interests of national security was further complicated by Americans’ Fourth Amendment rights.

AFCEA’s findings delineated the necessity for information sharing. AFCEA cites three primary legislative actions passed under the consensus for integration: (1) the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) of 2001, (2) the Homeland
Security Act of 2002, and (3) the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). According to AFCEA, these laws were instrumental in removing legal and perceptual barriers to information sharing through mandated change in the handling of both domestic and international threats.

In reference to the historical dilemma of information sharing within the Intelligence Community, AFCEA highlights varying interpretations of legal allowances as the main cause, making a rather benign critique of the community’s resistance to share information due to multidimensional motivators and influences. The AFCEA report stated that imposed legal and governing barriers were “excessively stringent” in both bureaucratic and cultural contexts (AFCEA 2007, 4). However, AFCEA posits that, despite attempts to broaden cooperation, the lack of impetus for change stagnated efforts in a greater acceptance of and comfort in the status quo. Implications had failed to affect policy as many continued to view engagement between intelligence and law enforcement agencies as inappropriate and disadvantageous to civil liberties protections. The challenge that presents itself is how to strike the appropriate balance between allowing law enforcement to do its job, while simultaneously protecting the civil liberties of the public.

Congressional action under IRTPA included the creation of the Information Sharing Environment (ISE), which provided the necessary infrastructure, policies, processes, standards, and directives to facilitate information sharing. Additionally, the ISE program manager position was established to measure progress, track outcomes, and ensure interoperability compliance. AFCEA enumerated other agency bodies and
oversight committees created under the various legislation in the hopes of promoting information sharing; however, many of those efforts failed or were stifled. The committee determined that “understanding the cultural differences between the intelligence and law enforcement community is key to understanding the lack of progress” (AFCEA 2007, 5).

From this perspective, AFCEA concluded that law enforcement’s approach works backward, using evidence to build a case in a crime that has already been committed in alignment with a prescribed legal scheme based on admissibility and chain of custody, working within distinct parameters, wherein failure to comply could jeopardize an entire case. Secrecy is a powerful tool in navigating this terrain, as prematurely released data endanger prosecutorial advantage. In other words, sharing information on a particular case could compromise the entire investigation. The following were AFCEA’s recommendations for improvement:

1. Communicate and reinforce the need for sharing;
2. Earn public trust;
3. Manage risk;
4. Create, clear, understandable, consistent guidelines;
5. Eliminate the construct of “data ownership”;
6. Use technology in a meaningful way;
7. Emphasize training;
8. Share good ideas and lessons learned.

(AFCEA 2007, 9)
Analysis of AFCEA’s Findings and Recommendations

AFCEA concluded that cultural resistance had sidelined communication efforts, despite the overwhelming evidence in favor of collaboration. Furthermore, AFCEA reported that many current rules, guidelines, and policies are unclear, inconsistent, and complicated, stating that this created unnecessary confusion, and that humans tend to “give up if the rules are too hard to follow” (AFCEA 2007, 9). Additionally, if the Intelligence Community cannot effectively navigate policy and information technology databases, then national security would continue to be faced with potential security failings. The committee argued that effective information sharing required a broadening of inclusivity and relevancy, understanding that the best advocates may not be the obvious candidates and that there is a need to seek out information meaning regardless of source classification. AFCEA concluded:

Although Congress has removed many of the existing barriers to cooperation, and limited examples of progress exist, implementation is lagging. The key to change is strong leadership in both the law enforcement and Intelligence Community’s [sic]. Leaders must understand and nurture cultural change that emphasizes a responsibility for providing information—not just for sharing it. They must also communicate to their subordinates a willingness to accept risk in sharing data and must deemphasize data ownership. These steps, along with clear guidelines, inter-community training, the exchange of lessons learned, and the effective use of technology, can open doors of cooperation that have been closed for too long. (AFCEA 2007, 11)

Similar to the recommendations found by the 9/11 Commission, AFCEA recommended changes in leadership; policy; procedures for transfer and storage of data; training; and better overall coordination among mission partners. Although at this point an in-depth analysis of Schein has not been conducted, it is important to note that
AFCEA’s recommendations contain a misunderstanding of the term *culture*. AFCEA conveniently uses culture as an umbrella term encompassing the majority of changes required to promote overall information sharing between law enforcement and the Intelligence Community.

AFCEA recommends changes in Intelligence Community agency leadership, stating that “leaders must understand and nurture cultural change that emphasizes a responsibility for providing information—not just for sharing it. They must also communicate to their subordinates a willingness to accept risk in sharing data and must deemphasize data ownership” (AFCEA 2007, 11). AFCEA’s flaw is not in its ability to identify culture as a cause for ineffective information sharing, but rather a misunderstanding of what organizational culture is.

As is the case with the 9/11 Commission findings, there is a failure to address the elements of organizational culture, such as attitudes, beliefs, and values that would propel the changes the Intelligence Community would like to see embraced. Using Schein’s model of organizational culture in the following sections, this thesis will shed light upon what is culture and how the U.S. government failed to conceptually understand and apply its principles toward effective information sharing within the Intelligence Community.

**The Schein Model: Culture’s Basic Building Blocks**

Edgar H. Schein is a former Massachusetts Institute of Technology Sloan School of Management, Stanford, and Harvard University professor, who received his
PhD in social psychology. Schein is an organizational development pioneer, and the first edition of his 1985 book, *Organizational Culture and Leadership*, was the first major commentary on the topic of organizational culture.

In the book’s fourth edition, Schein categorizes organizational culture as a microculture woven into the fabric of macroculture, including national, ethnic, and religious groupings of global importance (Schein 2010, 2). Schein describes how globalization and technological advancement have altered previous scholarly understandings of culture, given the increase in external influences and infiltrations. Schein states that these immense changes involve more partnerships among multiple macrocultures and can leave organizations vulnerable to increased scrutiny.

Increased technological complexity and global networking offer opportunities and threats in regard to enhancing organizational development. Schein emphasizes the subconscious realm where culture operates, taking from perspectives in fields such as anthropology, neurology, and psychology to enlighten this interrelation and forge avenues through which organizations can deliberately shape culture to drive desired performance outcomes and corporate citizenry.

It is important to note that Schein’s model primarily uses corporate culture to illustrate the concepts of organizational culture and leadership. For example, Schein uses the concept of the corporate citizen, which denotes the dynamic of an individual who is both an employee of an organization and who has also embraced the corporate culture of that organization; however, Schein’s model is very general to all groups.
Schein’s model of organizational culture has been designed so that even though he primarily refers to corporate culture, the model can be still be applied to any organization, even the Intelligence Community. Organizational culture, like that of more traditional concepts of culture, is an indoctrination process as new members are taught, much like children, how to perceive, think, and feel in relation to their external environment. The external environment determines the individual internal experience, which then translates into outward actions, ideas, and behaviors.

There are many ways to be indoctrinated into the Intelligence Community. A person may be indoctrinated into any one of the Intelligence Community’s seventeen agencies and, depending upon which one, receive varying training techniques, standards, and rules to abide by, or different styles of leadership, to name a few examples. All of these factors affect a person’s perceptions, attitudes, and beliefs concerning how to perform his or her specific job function—more specifically, with respect to this thesis, how to share information.

When examining the Intelligence Community as a whole, and noting that each of the seventeen agencies has its own individual culture that drive and influence behavior, it is difficult to imagine how they all ultimately work together to achieve mission success. The reality is that the Intelligence Community does share information in its own complex, sometimes confusing and sometimes haphazard way, to promote national security objectives. The dilemma, of course, is how information sharing can be improved and the extent to which organizational culture has and continues to affect the sharing of information. The specific factors that affect organizational culture,
according to Schein, will be discussed in further detail and will become more apparent as specific analysis is conducted on the individual cultures of the ODNI and FBI in further sections.

From a leadership perspective and citing Schein, William B. Locander, author and founding director of the Davis Center for Business Leadership, says, “The only thing of real importance that leaders do is creating and managing culture” (Locander 2005, 52). Admittedly, Locander may be making a strong generalization concerning the type and amount of responsibilities delegated to leaders; nonetheless, the quote emphasizes the importance of leaders in managing culture. Interestingly enough, Locander does not state that leaders manage people, but rather manage culture.

Corporate citizens share a set of basic assumptions that they believe secure their standing or reputation with respect to others in their environment. Thus, culture can be created, manipulated, managed, and developed to pass on to new generations joining the Intelligence Community. Leaders must compete with an abundance of messages—both internal and external—that may impair their overall objectives in culture creation.

The leaders of today’s intelligence agencies often face messages and guidance from external agencies or even Congress that can potentially conflict with their internal practices and procedures. It is up to leaders to make sense of these conflicts and then translate the appropriate information down their chains of command to the members of their organizations. Without strong coherent leadership, the members of organizations
will inevitably be as confused as their leaders concerning with whom to share information, for example.

Major Virginia Egli, a U.S. Army intelligence officer, studied the culture of leadership and its effects on information sharing within the Intelligence Community. In Egli’s scholarly research, she suggests that leadership is the key to making the leap from a “need to know” to a “need to share” organization, as “culture is connected directly to leadership” (Egli 2011, 4). The leader is the primary instrument of cultural communication and enforcement, but, as Schein argues, once the cementing of culture occurs, the leader then has to reexamine existing values and how such values will be harmonized with the new direction passed down.

From an organizational cultural perspective, there are difficulties in that those introduced to the new corporate environment are previously programmed with a lifetime of experience, teachings, and beliefs. Rewiring behavior and response can be problematic, especially if the culture is not effectively managed and developed. Leadership is thus the bridge between effective orientation and culture maintenance; however, according to Schein, once culture is established, it then determines the leadership style and criteria for powering the people. Therefore, the leader’s position and perspective are different when attempting to change culture, as opposed to creating it.

This point is integral to understanding the trials facing the Intelligence Community as leaders are trying to change a culture that has historically resisted information sharing, given the need for secrecy, depending on the situation and
context. Instead of having the luxury of inventing new culture when entering an organization, leaders are caught in the need of enacting cultural change in an environment that does not always necessarily want to be changed. Leaders must comprehend the supremacy of culture, if they seek to authentically lead the corporate citizenry; paramount to this understanding is recognizing that existing culture, as it gains momentum over time, may be the primary source of resistance to change (Schein 2010, 305).

This can be problematic to leaders within the Intelligence Community who are replacing former leaders and, as such, essentially inheriting this cultural momentum. Schein guides the often difficult to conceptually grasp terrain of what is organizational culture, using characteristics and observable elements of culture to keep things simple. Throughout this discourse, Schein’s model and characteristics and elements of culture will be referred to and expounded upon in direct application to the Intelligence Community.
CHAPTER 6
ORGANIZATIONAL CULTURE AND
INFORMATION SHARING

In its simplest definition, culture is the framework through which people view
the world around them. Organizational culture seeks to explain how human beings
interact with one another and new situations or information within a community and
the context of what they already know. Shining light on culture will aid in
comprehending the underlying reasons for resistance to information sharing.
Organizational culture is the field of organizational studies and management, which
includes attitudes, psychology, beliefs, experiences, and values of a given organization.
Schein defines organizational culture as follows:

… [a] pattern of shared basic assumptions learned by a group as it solves its
problems of external adaptation and internal integration, which has worked well
enough to be considered valid and, therefore, to be taught to new members as
the correct way to perceive, think, and feel in relation to those problems.
(Schein 2010, 18)

First, culture emerges in relationship to a group. Traditionally, to have a group
to begin with, elements of inclusion and exclusion exist. Does one want to fit in or
should one be different and risk being outcast? The element of risk versus reward
comes into play, as the individual is forced to harmonize the perceived risks of sharing
information with the perceived consequences of not sharing information.
Hypothetically speaking, what is an FBI intelligence analyst supposed to do, if the
overarching policies of the ODNI state that he or she must share information, yet the
FBI’s policy is not to disseminate intelligence outside the bureau? Whose guidance does the analyst follow, and what are the repercussions for either choice?

Ultimately, there are members who belong and others who do not, perhaps based on the aforementioned hypothetical scenario. Those who belong follow direct and indirect cultural guidelines as part of their membership acceptance. Those who do not comply are considered outsiders, not privy to the insider information, rituals, events, and cohesion that act to define the group. After all, what if the FBI intelligence analyst chose to follow ODNI guidance instead of FBI guidance? What message would he or she be sending to his or her organization about where his or her loyalties lie?

It is worthwhile to draw a parallel between the Intelligence Community and the private sector, in terms of the effects of efficiency in changing organizational culture. Globalization has transformed the business sector’s understanding of group dynamics. Cooperation and integration have proven to be financially profitable. For example, multinational corporations now use technology to power cost-cutting solutions. This integration and information sharing is grounded in applying contemporary business theories of supply chain management, just-in-time delivery, and other collaborative synergies that streamline production through networking.

Of course, to accomplish this, companies such as the big-box retail giant Wal-Mart have had to embrace transparency, defined as complete, accurate, and timely disclosure of information. Intellectual property and trade secret protection are often concerns, but business practice has evolved beyond fortiessing, instead forfeiting privacy for higher profit generation. The Intelligence Community microculture often
rejects this approach, because certain agencies feel the need to safeguard intelligence, rather than share it, and understandably so—it is the job of agencies within the Intelligence Community to protect sensitive information. The worry, as previously stated in this thesis, is that an increase in information exposure correlates to an increase in information leak risk.

Schein contends that the four characteristics of organizational culture are stability, depth, breadth, and patterning and that group identity strengthens an organization’s stability, meaning that its membership is firmly established (Schein 2010, 16). Cultural change is thus an active attempt to redefine group identity; this ignites the organism’s fear of death, as the whole and the individual participants are thrust into survival mode, regardless of the cited benefits of change. Preserving the status quo becomes the interest of most group members. Often this struggle plays out both on the subconscious and conscious level; the group rationalizes how and why the comforts of safety are preferable to the advantages of change. The individual serves as an example of how these fears are perpetuated as well as how reactions can be predicted. The status quo—often no matter how uncomfortable, dangerous, or disadvantageous—is clung to, because the organism at least knows what to expect in this environment.

In weighing outcomes, it is difficult to switch to a mentality that willingly embraces the unknown. People often resist change until the scales are tipped so far that taking the risk is perceived as better than the status quo, or the repercussions of not taking the risk are so undesirable that there is seemingly no alternative. For the
Intelligence Community, 9/11 highlighted issues affecting organizational effectiveness. In remedying this information-sharing conundrum, culture can both be the answer and the problem. Additionally, “the depth of an organizational culture is the level at which members of the organization intrinsically know how to behave within their culture” (Egli 2011, 4). The Intelligence Community is deeply entrenched in its identification with the group. Drawing parallels to private industry, for example, police officers tend to be lifelong members of this special society, even long after they have retired their badges. For law enforcement and military alike, membership is an identity, not an occupation. In the Marine Corps, the “Once a Marine, Always a Marine” slogan epitomizes such a cultural dedication.

*Breadth* is an important characteristic in analyzing organizational culture and is defined as the means through which culture permeates and influences organizational performance and function. Breadth is perhaps the most critical point in understanding the various cultural roadblocks erected within the Intelligence Community. The Information Sharing Environment (ISE), previously defined in this thesis, is an example of how unimpeded information sharing is substantially detoured by the breadth of the organizations’ culture, as outdated processes, policies, attitudes, and behaviors convolute information-sharing guidance. In reaching its mission, the Intelligence Community often is married to secrecy, as abundantly described throughout this thesis. Source and data confidentiality is believed to be vital to personnel and national security.
The Navy Sea, Air, and Land (SEAL) Team 6 al-Qaida compound invasion in 2011 that led to the death of global terrorist leader Osama bin Laden was a combined strategic effort of highly covert training, preparation, and expertise. The two Blackhawk helicopter, 25-person operation involved high levels of security. A senior White House administration official in an interview with CNN stated, “We shared our intelligence on this bin Laden compound with no other country, including Pakistan. That was for one reason and one reason alone: We believed it was essential to the security of the operation and our personnel. In fact, only a very small group of people inside our own government knew of this operation in advance” (Walsh 2011, para. 15).

President Obama and his national security team watched the mission in real time as the operation was carried out. After bin Laden was killed, a Navy SEAL uploaded a photo from a pocket camera and, using face recognition technology, positively identified their target as eliminated. According to then-CIA Director Leon E. Panetta (2011), CIA analysts worked intimately with National Security Agency eavesdroppers and the U.S. Geospatial Intelligence Agency in identifying the compound target as bin Laden’s hideout. This example expertly illustrates the importance of confidentiality and collaboration. A breach in secrecy could have easily thwarted the entire operation; any leak of information might have compromised the target and the personnel involved in the operation. However, failure to team with internal and external resources would diminish the integrity of the data, thereby introducing a similar threat.
In this scenario, balance was achieved; thus, analysts can study the planning, communications, leadership, and involvement that facilitated this specific effort. Furthermore, these agencies can evaluate this success from the perspective of culture, enumerating the context that fostered effective information sharing. However, some argue too much information was released concerning the bin Laden operation, particularly following its completion. Mark Bigham, vice president of business development for Raytheon Intelligence & Information Systems and a former U.S. Air Force all-source operations intelligence officer, stated: “There was too much information shared about the Osama bin Laden take-down” (Murray 2012, 7).

Bigham, in an article published by the Geospatial Intelligence Forum, suggests that wide publicity about the methods used to take down bin Laden could make it more difficult to use the same methods in the future (Murray 2012, 7). Bigham raises an important point concerning the amount of information that should be shared with the general public, not just the Intelligence Community. Releasing information concerning U.S. military special operations tactics to the public may render those same procedures less effective in the future. Proposed solutions to optimally reconcile secrecy and information-sharing efforts such as counterintelligence, network security, and background investigations will be discussed within further sections of this thesis.

The final characteristic of organizational culture that Schein describes is patterning; he defines this characteristic as the means through which humans make sense of their environment. “Culture implies that ritual, climates, values, and behaviors tie together into a coherent whole, and this pattern or integration is the essence of
A significant point Schein presented is that messages must be consistent both in their tone and purpose. This concept ties back to the importance of leadership through setting an example.

If leaders hesitate to share information and adopt integration, it is likely that members of their organization will follow their example. Such an assertion is understandable, given that the leadership position symbolizes power, authority, and prestige; to some extent, the leader’s actions resonate more loudly than the policies and regulations in place. If a CIA director advocates information sharing but does not share information him/herself, it is likely members of his/her organization will not share information either by sheer example. Actions speak louder than words. Culture springs at a level much deeper than the language, more complex than law. It is vital that the leaders of the Intelligence Community understand the complexity and sensitivity of organizational culture, particularly when the objective is to change behavior.

**Schein-ing the Light on Culture**

Schein stipulates that studying the *what* and *how* members are taught empowers individuals to understand culture. This is a crucial point in relation to the Intelligence Community, as the tendency toward secrecy has been identified and verified as problematic. Yet organizational integration efforts at times remain stalled, despite the efforts of community leaders. On the surface, this disconnect is elusive, as many of the policies, structure, and technologies have long been systematically crafted since the
9/11 Commission findings to support information sharing, and still the issue of how to better integrate the Intelligence Community continues.

The Intelligence Community has had a decade since 9/11 to actualize this cultural change; still, information sharing and integration challenges continue to plague the community. The Intelligence Community is a paradox at times, because while there are instances of agencies sharing information appropriately and effectively, many do not. The attempt to unify the community under the one-leader heading is a top-down approach that does not recognize the underlying problem of subcultures. Further sections of this thesis will discuss this issue when examining the role of the ODNI.

The lack of clarity and consistency is challenging for these divergent groups to translate; instead, unit leaders focus on their specific interests and motivators, using analytic methods and routine practices that bolster their job performance. Each subculture acts as a distinct unit, and the ISE approach is striving to unite the groups through shared purpose; however, this tactic is inherently flawed, as sovereignty and separation leash progress. Instead, the aim is better suited to seek synthesis throughout the entirety of the Intelligence Community. At this level, each team becomes a spoke in the wheel. This dynamic restructures the entire Intelligence Community from a bottoms-up approach that begins with the subcultures, such as the ODNI and FBI, instead of from their leadership. As Schein states, the culture is profoundly ingrained on practical and psychological levels. Therefore, it is important to understand the elements of organizational culture that are observable.
Artifacts

In Schein’s model, artifacts are considered observable and are defined as the first, surface level of organizational culture. Artifacts are not easily defined in scope, because they include sensory aspects operating within the culture, such as what can be seen, heard, and felt. Schein points to the physical environment as well as habits, language, technology, norms, attire, manners, emotions, mission statement, myths, rituals, ceremonies, and legends as key observable artifacts (Schein 2010, 23). This level acts structurally and functionally as well. Routine behaviors are also considered artifacts. The multitude of artifacts is unimportant; instead, the focus is better served when examining how these items create meaning.

Interpreting the meaning and depth of artifacts is a difficult task. These symbols become increasingly permeated with greater effect the longer the member is a part of the group. Egli uses the uniform as an example. Outwardly, a uniform offers immediate definition of group membership and function, as well as pointing to hierarchal standing within the group, depending upon the use of the uniform as an indicator of rank or role (Egli 2011, 12). Internally, the uniform’s value is an amalgamation of philosophies, legends, and expectations; this convergence represents the organization’s past, present, and future identities and stability.

Understanding artifacts can be incredibly important to understanding information sharing. Within the Intelligence Community, much of the intelligence that is produced contains both origination and dissemination markings, which denote what
agency has produced the product and the agencies with which that product can be shared. In some cases, agencies have the opportunity to collaborate with each other on particular intelligence products and often decline to do so to give their agency “full credit” for a particular product.

An interview that I conducted on February 14, 2012, with a Defense Intelligence Agency (DIA) employee, who wished to remain anonymous, sheds light on a potential theory for not collaborating on intelligence products. The DIA employee stated that by not collaborating on a particular product with other agencies, one is then not obligated to give other agencies “credit” for their input (DIA interview, 2012). Granted, one runs the risk of not producing a better, well-rounded product, because one has limited the number of people who can provide analytical insight. However, the trade-off is that by not giving other agencies recognition for their efforts, the agency that one represents takes full recognition in the eyes of the Intelligence Community.

When Congress allocates funding for the Department of Defense annually, the amount of quality work, security threats detected, and other recognition factors play into the decision of the dollar amount each agency receives. Agencies that do good work and prevent security failings get more money—the rationale is not complicated. The DIA employee speculated that it was his impression that funding plays a significant role in the decision of whether to share information—furthermore that leaders of agencies recognize this and, in turn, have subtly impressed a nonsharing culture at times. Although no DIA documentation exists that states that information is not shared due to budgetary concerns, the motivation not to share in order to receive
“credit” remains an example of a potential sensory aspect (i.e., artifact) that can be felt throughout the DIA.

Artifacts offer cultural clues; however, they do not stand alone in defining the culture. Artifacts are puzzle pieces that assist the observer in directing attention to certain aspects of inquiry. Artifacts require context. One puzzle piece may picture water and fish; if the observer jumps to the conclusion that the entire puzzle is of the ocean, he or she may completely miss the reality that the puzzle piece was a fishbowl kept in a corner. Therefore, Schein uses espoused beliefs and values to describe his theoretical model and bring shape to the total puzzle picture.

Espoused Values and Beliefs

Schein is stringent in pointing out that “all group learning ultimately reflects someone’s original beliefs and values, their sense of what ought to be, as distinct from what is” (Schein 2010, 25). This is a powerful statement, as it reveals the hidden intent of learning as a means of shaping individual perception and behavior. Reality and experience are truncated by the organizational mantra of ideal action. As such, leadership creates a story or myth, casting the group in specific roles and detailing the plot lines. The script is written, and the learning process is a continual rehearsal of that predetermined storyline.

Training programs and indoctrination procedures within the Intelligence Community’s agencies then carry forward the script and pass down to their membership the behavior and perceptions of that agency. The advocating of specific
values and beliefs manipulates the citizens to align with the organizational heartbeat, even to the sacrifice of personal preferences or inclinations. There are clear means of achieving status and acceptance within the group; to be successful in the group, members rely on instinct and training to ascertain these cultural instructions.

Organizational culture establishes the boundaries, often using overt and subtle forms of punishment and reward to reinforce these perimeters. After enough conditioning, these values and beliefs are internalized, and the citizens no longer need leadership oversight, training, and reminding. Instead, these members reflect the lessons as if they are from their own belief system. Such conditioning is important to the success of an organization and its ability to achieve its mission. However, understanding the espoused beliefs and values that drive organizational change also empowers leaders to make changes for improvement in the information-sharing enterprise.

The 9/11 Commission and the GAO report articulate the need for linking performance expectations and rewards with information sharing. In other words, the people within the Intelligence Community who share information should be rewarded. This approach is an attempt to rewrite the organizational values and beliefs of those people at the personal level of reinforced learning. The ultimate goal of which is to change the mentality of Intelligence Community members from a “need to know” to a “need to share” mindset. Members are told the performance review process will reward their behavior if information sharing occurs. The 9/11 Commission and GAO reports deserve credit for recognizing this key aspect of organizational culture in influencing
behavior. The issue remains, however, that the proponent for enforcing the system of rewards, namely, the ODNI, has done a poor job of doing so. In further sections, this thesis will address specifically why this is the case.

Egli offers the concept of tactics, techniques, and procedures (TTPs) to illustrate the embodiment of espoused values in organizational development. According to Egli, a TTP is a detailed, standard course of action for a specific task. “A TTP is developed through group learning in response to a known and adaptive adversary” (Egli 2011, 8). The doctrine is the filter through which group members interpret their environments and interactions with the adversary. The adversary is integral to the game; without an enemy in the “us versus them” match, there is no winner. The leader thus integrates policy, intelligence, and procedures to outsmart the adversary. If the leader’s solution is validated through outcome, the TTP transfers to doctrine, becoming a pillar in the organization’s conscious of best practices and lived experience.

Again, as Schein cautions, espoused beliefs and values are merely parts of the puzzle. In giving the puzzle shape, there is still ample room for the observer to misinterpret the group message (Schein 2010, 141). In this realm of culture creation, communication is vital. To effectively communicate and manage the culture of the community, leaders must realize that the message will be internalized by the recipients. This may seem like a fairly simple point, but recalling once again the reference to Locander, leaders manage culture, and communication is a form of managing the culture. Mistakes in messages that Intelligence Community leaders articulate to their
agencies can, if not caught and corrected in a timely fashion, become conditioned within their agency and become part of their belief system. The larger the audience to whom the message is conveyed, the greater the effect on culture.

“If the beliefs and values that provide meaning and comfort to the group are not congruent with the beliefs and values that correlate with effective performance, we will observe in many organizations espoused values that reflect desired behavior but are not reflected in observed behavior” (Schein 2010, 27). This point deserves deeper investigation. Clearly, the Intelligence Community is loudly proclaiming the importance of information sharing, as evidenced by the research, the policies, the analytics, and its restructuring; however, the truth remains that information sharing is often hindered. The final and deepest level of culture, according to Schein, is the basic assumptions foundation.

**Basic Assumptions**

Basic underlying assumptions are the most embedded and unconscious level of culture. Figure 1 depicts the three levels of culture, with basic assumptions lying at the deepest level.

The repeated testing of a hypothesis leads to a theory; theories are then used scientifically to explain what is observable as fact. An apple falls (fact); it is due to gravity (theory). In culture, similar ideologies develop, creating the perceived natural environment in which the culture exists. After time, organizational solutions are taken for granted, instituting the premise of group behavior (Schein 2010, 28). In the
Intelligence Community, as with many other organizations and groups, just because something has been done the same way forever doesn’t necessarily make it the right way. Such a conclusion is evidenced by the 9/11 Commission’s findings on information-sharing challenges previously discussed in this thesis.

On the other hand, many groups and organizations conduct operations the same way consistently with excellent results, proving that taking organizational solutions for granted is not always a bad thing. The U.S. military requires all of its members, regardless of branch, to qualify in at least one type of firearm during basic training. Firearms proficiency has historically been proven to be a useful skill, and it is a part of the military training regimen that will likely not go away anytime soon. Basic assumptions guide the group in directing attention, emotional reaction, interpretation, and normative responses to various situations (Egli 2011, 4). These rules define dichotomies: good and bad, acceptable and unacceptable, desirable and undesirable.
Egli’s example of the evolution of TTPs to doctrines demonstrates the strengthening of these shared ideas to the point where they naturally become part of the culture. The word *indoctrination* is paramount in grasping the intensity and depth of this entrenchment. Through repetition and reinforcement, the members are indoctrinated as these underlying principles and philosophies are permanently impressed upon their psyches.

According to Egli’s analysis, the Army’s doctrines were tested in the Global War on Terror, as these traditional methods of maneuvering were challenged in this new landscape of unknown enemy combatants and often unanticipated warfare tactics. Schein states that the human psyche’s need for stability is shaken when basic assumptions are challenged; thus, the group may cling to ineffective methods when under severe environmental pressures to maintain this pseudosafety, even to the potential detriment of the organization as a whole. Despite the enormous cost to American psyche and sense of safety suffered in the 9/11 attacks, culture seems to prevail stronger than any policy or directive attempting to enforce information sharing. Transitioning from a “need to know” to a “need to share” culture, however, attacks the core assumptions that have guided these separated agencies since their inception. Even when national security is in question, group survival tends to dominate as the subcultures are predominantly interested in protecting their identity and sense of belonging.
CHAPTER 7
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE: PRESENT-DAY CONTEXT

The director of national intelligence (DNI) position was established when President George W. Bush signed IRTPA on December 17, 2004, in which the DNI’s authorities are outlined. The DNI heads the Intelligence Community and ended the 57-year reign of the DCI as the nation’s chief intelligence officer (CIO). The DNI heads the Office of the Director of National Intelligence (ODNI). The combined mission of the DNI and the ODNI is to oversee and direct the implementation of the National Intelligence Program and act as the principal adviser to the president, the National Security Council, and the Homeland Security Council for intelligence matters related to national security. Additionally, the DNI’s goal is to effectively integrate foreign, military, and domestic intelligence in defense of the homeland and of U.S. interests abroad.

It is of particular importance to address the ODNI’s mission in this thesis, because of the influence the DNI position has on the information-sharing environment and the organizational culture of the Intelligence Community as a whole. The establishment of the DNI’s position has been controversial. Fred Kaplan, author and senior Schwartz fellow at the New America Foundation, argues that the DNI’s powers and effect are limited due to legislative drafting compromises. According to Kaplan’s analysis, IRTPA includes a key passage asserting that the DNI cannot “abrogate the statutory responsibilities” of DoD. As indicated by Title 10 of the U.S. Code (Chapter
21) and in DoD Directive 5100.20, these protected “responsibilities” include the personnel, operations, and budgets of the Defense Intelligence Agency (and military subbranches), the National Reconnaissance Office, the National Imagery and Mapping Agency, and the National Security Agency (NSA) (Kaplan 2004, 5–6). These agencies comprise approximately 80 percent of the Intelligence Community’s budget. Therefore, Kaplan says, “this ‘reform’ bill places about 80% of the entity that’s supposedly being reformed outside the direct control of the official—the new national intelligence director—who is supposedly the reform’s centerpiece” (Kaplan 2004, 7).

It is reasonable to suggest that the DNI’s role is challenging, given the mixed signals in terms of power that the position holds. The DNI’s mission is to integrate the Intelligence Community’s capabilities, and yet his or her authority to do so has been limited to various restrictions in power outlined within IRTPA. Admiral Dennis Blair, former DNI, resigned from office, stating that “institutional and technological barriers remain that prevent seamless sharing of information,” suggesting that despite the ODNI’s mission to solve such challenges, he didn’t have the “authority” to do so.

Former Representative Peter Hoekstra, once the top Republican on the House Permanent Select Committee on Intelligence, states that “the Office of the Director of National Intelligence clearly is not working the way the 9/11 Commission or Congress intended. We obviously need a DNI to force our 16 intelligence agencies to share information and cooperate with each other on time sensitive national security threats” (Hoekstra 2010, para. 6). Hoekstra implies that the DNI’s position is essentially set up for failure. Opponents of Hoekstra’s opinion would argue that former DNI Blair should
have taken more initiative and pushed Congress to grant him greater authority for the responsibilities he was delegated. In either case, it is important to note the controversy and challenges associated with the DNI position when analyzing the information-sharing initiatives the ODNI executes.

The ODNI identifies culture in addressing mission effectiveness and information protection. The ODNI states that “a new culture of collaboration and risk management will require that people and organizations understand and trust how their partners manage risk,” calling for a “uniform trust model across the Intelligence Community” (ODNI 2008a, 8). The ODNI mentions the necessity to establish a “need to provide” culture in its 2008 Information Sharing Strategy (replacing the outdated 2007 version), offering that creating this environment demands the following:

1. Consistent certification and accreditation practice;
2. Tying performance rewards to information sharing;
3. Repair fragmentation;
4. Generate collaboration opportunities;
5. Cross-level communication;
6. Determine strategy and decision processes.

(ODNI 2008, 11)

The 2008 Information Sharing Strategy asserts the need to address culture, in addition to what the ODNI refers to as the “building blocks” of information sharing, which include governance, policy, technology, and economics (ODNI 2008a, 17). This misunderstanding of the importance of culture as the bedrock of all organizational
performance overvalues infrastructure and process (which, granted, are important and necessary), but fails to grasp the core of the information-sharing problem. The ODNI does well to recognize the need to incentivize individuals in order to promote information sharing, but with respect to Schein’s model, it is only one aspect of shaping overall organizational culture. The issue is that the ODNI differentiates culture as a separate problem that requires fixing and as a parallel piece alongside the desire to change policy, technology, and other factors that promote information sharing. The problem ODNI should address is how culture affects those aforementioned factors, as opposed to distinguishing culture as a separate effort in need of resolution. This fundamental misunderstanding of how culture affects human behavior is presented in figure 2.

The diagram clearly illustrates the ODNI’s misperception of how organizational culture affects the factors of governance, policy, technology, and economics. A more appropriate diagram would have illustrated culture as the centerpiece, with all other blocks branching outward from its core. The ODNI takes the position that each building block should be tackled separately, as if they are isolated issues, ignoring the fact that culture is embedded and driving each block. To be more specific and as stated previously in this thesis, the 9/11 Commission found that a lack of understanding and training in how systems (i.e., technology) operated was one determining factor in leading to the 9/11 attacks. Technology is listed in ODNI’s diagram as a building block in need of addressing. The FAA took responsibility in
<table>
<thead>
<tr>
<th>Governance</th>
<th>Description</th>
<th>Key Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The “environment” influencing sharing</td>
<td>Oversight and leadership that help govern information sharing. How managers drive initiatives within organization and across agencies. Standards and guidelines to ensure a consistent approach.</td>
<td>- Is there a clear value proposition for sharing among partners, i.e., quid pro quo or negotiated trade-offs? Are MOUs or service-level agreements required? &lt;br&gt; - Do people understand how to abide by the law and policies? &lt;br&gt; - How are information sharing disputes resolved? &lt;br&gt; - Who are the key stakeholders?</td>
</tr>
<tr>
<td>Policy</td>
<td>National policies, internal policies, rules of engagement, standards, and role of players internal and external to the organization.</td>
<td>- Are laws, regulations, policies, and procedures in place that authorize, mandate and/or enable the organization to share? Is the organization complying with these mandates? &lt;br&gt; - Do laws/regulations/policies/procedures impede or constrain the organization/people from sharing? &lt;br&gt; - Are privacy and civil liberties sufficiently protected?</td>
</tr>
<tr>
<td>Technology</td>
<td>The technology, systems, and protocols that provide the platform for enabling the sharing of information and that address security and privacy issues.</td>
<td>- Are there common data standards and systems for organizing, identifying, and searching? &lt;br&gt; - Can participants push and pull data across networks? &lt;br&gt; - How is information protected; is the system auditable? &lt;br&gt; - Are tools/mechanisms available to manage identities; authorize, authenticate, and audit users; and ensure confidentiality?</td>
</tr>
<tr>
<td>Culture</td>
<td>The organizational approach and philosophy around sharing information and its ability to realign and adapt as circumstances change.</td>
<td>- How do we motivate people and create incentives to collaborate and share information across organizations? &lt;br&gt; - Does the organization communicate across all levels? &lt;br&gt; - How does the organization adapt to change, and how responsive is it to stresses and opportunities? &lt;br&gt; - How are decisions and conclusions reached?</td>
</tr>
<tr>
<td>Economics</td>
<td>Ability to obtain and provide resources for information sharing initiatives, and external pressures (e.g., budget) that influence how resources are allocated and managed.</td>
<td>- Has sufficient funding been appropriated to support the initiative? &lt;br&gt; - Have incentive structures been developed? &lt;br&gt; - Is the funding reaching the appropriate level within the enterprise to fully implement the sharing program? &lt;br&gt; - How do we measure performance?</td>
</tr>
</tbody>
</table>

Figure 2. ODNI 2008 Information Sharing Strategy. Source: Office of the Director of National Intelligence 2008, 15.
admitting that its employees were not adequately trained on the TIPOFF system, which was one influencing factor leading to the 9/11 attacks.

The ODNI has addressed technology in its Information Sharing Strategy, but it has not tied technology to culture by asking, “What would motivate individuals to use this technology to begin with?” Similarly, the ODNI has drawn a differentiation between governance and culture illustrated in this diagram, asserting that leaders must drive the initiatives that promote information sharing—when, in reality, culture and leadership are connected. The federal government has long had the backing of policies and capacities, as well as the insight of data exchange potential, and has often failed at information-sharing efforts. Even as progress has certainly been made under the ODNI’s objectives, challenges still exist. The nature of the ODNI’s problem is not in its ability to recognize culture as a cause for ineffective information sharing, but rather a misconception of its principles and application.

In an effort to execute the ODNI’s Information Sharing Strategy, the *United States Intelligence Community 500 Day Plan: Integration and Collaboration* (ODNI 2007b) was created. In principle, the plan outlines at a tactical level the steps that would be required to implement the ODNI’s Information Sharing Strategy. To create a culture of collaboration, the ODNI 500 Day Plan states that the Intelligence Community must:

1. Formalize the National Intelligence University;
2. Improve Recruiting, Hiring and Retention of Heritage Americans (1st and 2nd Generation Americans);
3. Develop an Intelligence Enterprise Exercise Program;
4. Improve Foreign Language Capability;
5. Strengthen Recruiting Relationships with Colleges and Universities;
6. Complete Design, Begin Deployment of an IC Performance-Based Pay System;
7. Catalog and Connect IC Human Resource Capabilities.

(ODNI 2007b, 3)

The 500 Day Plan is weak in its efforts to identify ways to promote information sharing through shaping organizational culture. The objectives listed in the plan speak more to the end result of what the ODNI hopes to achieve, rather than addressing culture directly. For example, objective 6 states, “Complete Design, Begin Deployment of an IC Performance-Based Pay System.” Objective 6 should state, “Incentivize individuals to remain and perform better within the Intelligence Community.” By rearticulating the goal to the latter method, it addresses the behavioral aspect of what incentivizes individuals. In the case of the 500 Day Plan, the ODNI has identified pay as a motivating factor. The ODNI would benefit from restructuring its list of objectives to address human behavior first, then as secondary objectives list the actual steps it would require to change the overall culture.

Objectives 2 and 5 speak to the need to improve recruiting. Rather than having these objectives listed separately, the 500 Day Plan could state, “Create interest and a desire to become a member of the Intelligence Community.” Objectives 2 and 5 could then be listed as subactions required to directly target and pique human curiosity,
which may lead to a career in the Intelligence Community. There are also other subactions the ODNI could take to arouse people’s interest, which may include marketing efforts, for example; marketing could then be added as a subaction.

Although these efforts are well intended, the ODNI is misdirected in its attempts to truly affect organizational culture. As Schein attests, leadership is the key to organizational culture, as a leader affects the development of shared basic assumptions of a community through external adaptation and the internal integration of problem solving (Schein 2010, 220). There is no mention within the ODNI’s 500 Day Plan of how leadership is expected to execute the initiatives that promote a culture of information sharing. The expectation seems to be that once the 500 Day Plan is released, leaders within the Intelligence Community will simply execute the plan without hesitation.

The ODNI’s fundamental mistake is the assumption that through its powers of authority, which, to reiterate, have been limited, the ODNI alone will be able to demand that agencies within the Intelligence Community follow its prescribed guidance. Creating an approach that articulates how the ODNI will empower the leaders of organizations to then empower their middle management to then empower their staff-level employees is never addressed. The false presumption is that leaders of organizations will read the ODNI’s guidance and simply execute the plan. There exists no incentive to follow the ODNI’s guidance, because no incentive exists within the 500 Day Plan to reward agencies for sharing information. The impression is then given to agencies within the Intelligence Community that self-promotion of their individual
missions will be more rewarding than promoting overall information-sharing objectives.

Finally, operations such as intelligence and collection are the Intelligence Community’s daily business processes and thus the heart of the behavior that affects culture, not policy and guidance. If the ODNI continues to talk about changing culture by simply articulating goals in a strategic plan and expecting people to listen, then there will be no action taken toward a demonstrable change in analytic tradecraft, for example—one of the actual daily business processes of the Intelligence Community. As Schein states, the daily process must “work well enough to be considered valid” before cultural change can be achieved (Schein 2010, 18). There is no follow-up action within the 500 Day Plan that speaks to monitoring the Intelligence Community’s progress in these information-sharing initiatives to the point where such progress can be considered “valid” and, hence, a positive cultural change.

In addition to the Information Sharing Strategy and 500 Day Plan, the ODNI has created several initiatives that it believes will improve the Intelligence Community’s information-sharing enterprise. This collection of ODNI initiatives falls under an umbrella term that the ODNI refers to as Analytic Transformation: Unleashing the Potential of a Community of Analysts (ODNI 2008b, 2). One specific initiative that the ODNI oversees is a program called “A-Space.” A-Space, also known as “Analyst Space,” is a social collaboration tool built on commercial software that was put into production within the Intelligence Community on September 22, 2008. The A-Space program currently has more than 22,000 users accessing it from across all
agencies in the Intelligence Community. The primary purpose of A-Space is to serve as a centralized platform for members of the entire Intelligence Community to virtually gather within a single environment in order to collaborate on intelligence-related products and ideas.

The premise behind A-Space is to allow analysts representing multiple agencies to collaborate on mission topics their respective agencies feel are important, thus promoting the overall information-sharing environment. “After logging in, analysts have access to shared and personal workspaces, wikis, blogs, widgets, RSS feeds and other tools. To log in, analysts will need to prove their identity using public key infrastructure, and their agencies must list them in the governmentwide intelligence analyst directory” (Bain 2008, para. 6). A-Space is essentially the Intelligence Community’s version of Facebook, but at a highly classified level. For users to gain access to A-Space, they must possess a minimum of a Top Secret (TS) Sensitive Compartmented Intelligence (SCI) clearance. This is undoubtedly the ODNI’s best effort to get at the heart of what is the Intelligence Community’s primary tradecraft—intelligence analysis. Analysts often may be unaware that there are other people working in other agencies on the same topics they are. By connecting analysts through a common environment, the rationale is that this will result in redundancy of work and improve the quality of a shared product.

A-Space is not designed for managers or supervisors, and, in fact, they are not even allowed access to the program. The ODNI’s fear in allowing managers access to A-Space is that they will attempt to take ownership of products and ideas and impede
analysts from doing what they do best, which is uninhibited analysis. Furthermore, there is a fear within the ODNI that managers, who are often more senior by virtue of their position, are more engrained in the culture of not sharing, given the Intelligence Community’s history of sharing challenges, particularly before 9/11. The ODNI view is that if managers were to access A-Space, a potential risk is that they may actually hurt information-sharing initiatives, not help them.

Theoretically, the ODNI’s A-Space program appears to be very sound. The ODNI has attempted to break down the cultural stovepipes that impair information sharing by providing a common platform for analysts to collaborate within. The ODNI has also targeted one of the Intelligence Community’s main business practices, which is intelligence analysis. Rather than attempting to take a top-down approach in which policy and infrastructure drive information-sharing efforts, the ODNI has taken a bottom-up approach in which analysts and other intelligence professionals drive information-sharing efforts, forcing the rest of the community to pay attention. By showing off national security success stories arrived at by analysts through A-Space, the ODNI hopes to tear down the remaining walls of cultural barriers erected over decades of nonsharing conditioning.

In principle, an analyst from the FBI and one from the DIA, for example, should each be able to access the A-Space program and share information without fear of management interfering and also with the understanding that whomever they are collaborating with has a “need to know” based on the security enclave of the system. It must be noted that the ODNI’s initiative is very bold, as it opens the door to a wide
range of security threats. If the Intelligence Community hires another Bradley Manning who then gains access to A-Space, the reality is that the individual will not only have access to classified material, but also access to 22,000 users’ worth of material, representing every agency in the Intelligence Community. If such material were leaked, the results could be a grave security failing.

The problem with the ODNI’s A-Space initiative is that it underestimates the culture of agencies that are consumed with security concerns and source protection. One very obvious concern is the aforementioned fact that one person with access to A-Space suddenly holds the keys to the kingdom. That person can view and potentially abuse a significant amount of information, all through accessing just one program. Dr. Mike Wertheimer, former ODNI assistant deputy director, has openly admitted that A-Space is a “counterintelligence nightmare” (Sevastopulo 2007, para. 9). The fact remains that there are still agencies within the Intelligence Community that simply have to keep information so proprietary that it cannot be shared even with the rest of the community, regardless of clearance level and whether the ODNI states they must do so.

An interview that I conducted with an ODNI employee who wished to remain anonymous and directly supported the A-Space program revealed several interesting cultural barriers preventing the system from achieving its originally intended purpose. The ODNI employee stated that it had been brought to his attention over a period of time that the FBI was gaining access to the A-Space program, but not using the system to collaborate with other analysts from across the community. FBI employees were
accessing A-Space to view other analysts’ work and to use the program’s built-in search engine, among other tools and capabilities, but were refusing to collaborate with other analysts or share any FBI-originating intelligence. In other words, the FBI was more than happy to access A-Space to view and extract other analysts’ work, but would not post or share information with other analysts from other agencies.

Because the interviewee was assigned to the ODNI’s Analytic and Transformation Directorate and directly supported the A-Space program, he felt obliged to investigate the issue. The interviewee was able to meet with an FBI intelligence analyst under the partially false premise that the meeting was intended to solicit general feedback regarding ways to improve the A-Space program’s tools and features. The questions became more in-depth, and what was discovered is that the FBI intelligence analyst had been directed by his supervisor not to share information with others analysts within A-Space. The supervisor explained that there was no official policy or directive that he could point to stating that the FBI could not share information via A-Space, but that to protect their sources, the risk of sharing information could not be assumed (ODNI interview, 2012).

Perhaps the most surprising revelation was not that an FBI policy could not be produced stating a restriction in information sharing, but that the supervisor himself did not even agree with the guidance he was providing his analysts. Further discussions revealed that the FBI supervisor had received the orders not to share information on A-Space from his supervisor. This highly indicates the depth of the cultural problems affecting agencies. Again, there is a correlation between the seniority of agency leaders
and their unwillingness to share information, because the ancient culture of nonsharing tends to be more deeply engrained in older, pre-9/11 generations. This historical belief is then passed down from generation to generation, regardless of ODNI initiatives and Intelligence Community policies directing agencies to do otherwise.

This was the ODNI’s initial fear and the main reason why managers are not allowed to access A-Space. And yet, it appears as if the culture of nonsharing runs deeper than access controls the ODNI has put into place. To complicate matters further, the interviewee speculated there was a connection between the FBI’s perceived paranoia regarding sharing information and the ODNI’s mission. The interviewee theorized that the FBI was well aware of the controversy and pressure surrounding the ODNI’s mission to better integrate the Intelligence Community. The ODNI is under a tremendous burden to promote information sharing, and continued funding by Congress to the organization is dependent upon the success of its initiatives. It is possible that the FBI recognized this burden and perceives that the ODNI, in an effort to promote the information-sharing enterprise through A-Space, had not fully considered the security concerns associated with it. In an effort to ensure maximum security of its information, the FBI most likely made the decision that sharing intelligence via A-Space was not worth the risk.

It appears as if the ODNI’s initiative to push information-sharing efforts on the Intelligence Community through a single piece of technology may have underestimated the depth and power of cultural barriers still prevalent in the FBI. Another issue with the A-Space initiative is that it does not allow for the presence or
input of leadership into the program. Schein states that leadership is the main proponent and architect of transforming culture (Schein 2010, 297). Therefore, if a particular agency within the Intelligence Community has 8,000 of its members using A-Space daily, and leadership is not permitted to be involved with its members through this platform, then how is leadership expected ever to change its agency’s culture?

Furthermore, the ODNI contradicts itself by stating the need for leadership in its Information Sharing Strategy for transforming culture. The building block of “governance” is listed as a necessity in promoting information sharing. It makes little sense that the ODNI would articulate the need for leadership to effect change, then create a major initiative to promote information sharing that reflects a complete absence of leadership.

Another major issue with the A-Space program is that it is only designed for analysts to use. Intelligence analysis is only one of the ODNI’s main business practices. Other practices include but are not limited to collections and targeting. If both collectors and targeteers are not permitted to access A-Space, the ODNI has eliminated the presence of significant tradecrafts of the Intelligence Community within the program. Critical intelligence that collectors may have access to, for example, cannot be shared with analysts in A-Space to provide an improved, well-rounded picture of a potential threat.

It is apparent that agencies such as the FBI are wary of the security risks associated with programs that promote information sharing, such as A-Space. This is understandable given past security incidents such as WikiLeaks, which have
undoubtedly contributed to a culture of nonsharing. The issue of how best to harmonize the dissemination of information while maintaining security interests is ongoing. The analysis of the ODNI’s initiatives to transform the Intelligence Community has touched upon FBI challenges associated with information sharing, which will be discussed in further sections. The A-Space discussion is an excellent segue into the security challenges associated with sharing versus nonsharing.
CHAPTER 8
SECURITY: SHARING VERSUS NONSHARING

The 9/11 Commission deemed that information sharing must occur to prevent future security failings. Ironically, however, it was the sharing of information that led to past security failings such as in the case of Bradley Manning, previously described in this thesis. The question remains as how to strike an appropriate balance between promoting the exchange of information while taking robust security measures into consideration to protect that information. The GAO conducted an audit on homeland security in 2003, which described the steps required to improve security while permitting the exchange of information to flow freely and widely.

The GAO addressed these steps in congressional testimony titled *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues* (Dacey 2003). The GAO report states up front the two main security threats facing information sharing. The first threat is internal, which are the employees of the Intelligence Community. The second is external, which are the threats from foreign countries and other adversaries. Both threats are formidable, as proven through historical security failings. The GAO report states that there is undoubtedly greater security risk commensurate with the increased sharing of information. In other words, the more parties, agencies, and systems in which information is shared with or through, the greater the risk of security failures.
The Manning case certainly showcases the danger in sharing information widely within the Intelligence Community. While enlisted in the U.S. Army and stationed in Iraq as an intelligence analyst, Manning had access to highly classified information residing on the Joint Worldwide Intelligence Communications System (JWICS). JWICS is a system of interconnected computer networks primarily used by the departments of Defense, State, Homeland Security, and Justice. By having access to the JWICS system, one inherently has access to classified information shared by multiple agencies in the Intelligence Community within a single network. The benefit of the system is that through a single access point and without having to use multiple login credentials, one may automatically view classified information from multiple agencies.

Manning was given access to the JWICS system throughout the course of his career. Manning allegedly used the JWICS system to download classified material to his personal laptop, which he then allegedly uploaded to WikiLeaks. Although JWICS is an outstanding solution to improving information sharing given its wide user and agency base, the security risks are potentially severe as in this case. On the other hand, 9/11 highlighted the dangers of not sharing information, so the Intelligence Community has found itself in a precarious situation.

However, is the issue really about sharing information widely, or is the real issue that the Intelligence Community allowed an individual like Manning to receive a security clearance? When Manning was receiving his intelligence training and undergoing the investigation that granted him a security clearance, it was discovered
that he was uploading videos to YouTube that discussed details and locations of classified facilities. Manning “was three months into his 16 weeks of training as an intelligence analyst when about 25 of his fellow students got together to report him for the videos in July 2008” (Poulsen and Zetter 2010, para. 2). Therefore, the question must be raised as to why Manning’s interim clearance was not terminated when these security incidents were brought to light?

It was discovered that the U.S. Army had taken a traditional approach to disciplining Manning. The specific type of punishment that Manning received was never disclosed, but he was ordered to remove the videos, which is technically a form of damage control, not a punishment. Although it is speculation, the type of punishment that Manning most likely received, based on traditional military disciplinary procedures, would have involved some type of rigorous physical exercise, a loss of base privileges, a demotion, and perhaps paperwork to sign admitting his faults, which would remain part of his permanent military record.

More likely than not, the specific punishment Manning received will be discussed during his trial, which is still pending. What is clear in the meantime, however, is that the type of punishment Manning did receive did not ultimately result in the loss of his interim clearance. Manning did not lose his then-provisional Top Secret security clearance and graduated from intelligence training in August 2008 (Poulsen and Zetter 2010, para. 8). In response to why Manning was not immediately stripped of his interim clearance at the first sign of trouble, U.S. Army spokeswoman Tanja Linton stated, “In a training environment, where we’re dealing with young
people who aren’t used to the Army, we deal with a wide variety of folks doing inappropriate things. They have issues, and it’s dealt with, and they go on to do great things for the Army and the country” (Poulsen and Zetter 2010, para. 7).

The U.S. Army’s attitude appears to be very accustomed to dealing with these types of incidents and that in most cases it’s just a matter of “boys will be boys.” Unfortunately, this type of passive aggressive attitude fails to truly appreciate the understanding that possessing a Top Secret clearance is a privilege, not a right. Had Manning been caught drinking and driving, getting into altercations with other soldiers, or any other number of fairly common acts of breaking the rules, a traditional approach to discipline would have been understandable. However, the military cannot take a traditional approach to discipline in matters affecting national security. Manning should have been stripped of his clearance when he committed his first deliberate security violation, and in retrospect it is very difficult to argue otherwise. Background investigations for people applying for clearances or holding interim clearances must be more thorough, and stricter consequences for security violations must be enforced. This is my first recommendation to the Intelligence Community for improving the security of the information-sharing environment.

Because Manning’s YouTube activities failed to cost him his clearance, the next best case scenario would have been that network security measures would have detected his suspicious activities before he had the opportunity to leak classified information. The Federal Information Security Management Act of 2002 (FISMA), requires federal agencies to “provide information security protections commensurate
with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of ... information collected or maintained by or on behalf of an agency” (FISMA 2002, § 3543(a)(2)). In other words, the network security procedures in place within an agency must be robust enough to the point where they are able to meet or exceed the perceived threat to the network.

This was not the case with Manning, who from October 2009 through May 2010 allegedly leaked classified information and was never detected by network security. During this time, Manning confessed that he had leaked classified information to a number of different sources, one of which was Julian Assange, founder of WikiLeaks. Over a period of eight months, Manning allegedly uploaded more than 250,000 State Department message traffic cables and numerous classified videos, including the infamous “collateral murder” video (WikiLeaks 2010), to his personal computer and eventually to the public. Manning’s downfall came when he spoke via live chat to former computer hacker Adrian Lamo and confessed the plethora of information he had released to WikiLeaks. Lamo turned the chat log files in to the FBI, and Manning was soon after arrested by military police. Ultimately, it was a public informant who caught Manning, not network security.

Network security is designed to prevent and monitor the unauthorized access, abuse, modification, or denial of computers and network-accessible resources. FISMA reinforces the need for stringent network security within agencies. Not only would network security have had the ability to monitor Manning’s chat log files, but it would
have had the technical expertise to realize that information was being transmitted and removed from classified devices.

My second recommendation to the Intelligence Community is an improvement in network security measures. Counterintelligence measures are often designed to complement network security or act autonomously in efforts to detect threats. Counterintelligence refers to efforts made by intelligence organizations to prevent potential threats from successfully gathering and collecting intelligence against them. The scope of intelligence efforts has increased over the years with the advent of new emerging threats. Counterintelligence efforts can be very complex and involve everything from using undercover employees to monitoring potential threats to using high-technology surveillance techniques. The 2007 ODNI National Counterintelligence Strategy of the United States of America “elaborates the fundamental responsibility for U.S. intelligence to warn of and help prevent terrorist attacks against the homeland, engage other asymmetric threats, and provide reliable intelligence on traditional and enduring strategic issues” (ODNI 2007a, iii).

The 2009 version of the National Counterintelligence Strategy was updated to include language that calls for stricter counterintelligence measures against insider threats. “Insiders have caused grave, long-term damage to national security. History has demonstrated the intent of foreign intelligence services and entities to penetrate the Intelligence Community and extract information through the use of a trusted insider—recruiter or volunteer” (Office of the National Counterintelligence Executive 2009, 5). Manning would qualify as an “insider threat” and “volunteer.” The Manning case has
revealed very little about what, if any, counterintelligence measures were taken to prevent the security failings.

It may very well be the case that revealing any counterintelligence efforts used to thwart Manning would undermine their effectiveness in the future, and therefore such efforts may remain classified. What can be deduced, however, is that if any counterintelligence measures were being conducted to target Manning, they ultimately did not work—unless, of course, Adrian Lamo was working for the Intelligence Community; nothing brought to public light suggests he did or does.

My third recommendation to the Intelligence Community is an improvement in counterintelligence measures. Perhaps one of the most overlooked threats to national security is the ethical implications of the Intelligence Community’s actions. Manning has made a moral case for the need to put information out in the open, staking the claim that the public has a right to know about potential crimes against humanity, among other crimes. WikiLeaks supports Bradley’s perspectives, stating: “Publishing improves transparency, and this transparency creates a better society for all people. Better scrutiny leads to reduced corruption and stronger democracies in all society’s institutions, including government, corporations and other organizations” (WikiLeaks 2012, sec. 1.3).

The “collateral murder” video (WikiLeaks 2010), which shows a U.S. military air strike on a van full of alleged Afghani citizens, raised scrutiny about whether innocent people were being killed. Manning made an ethical case that crimes against humanity should not exist on a classified server, but rather a public domain, so that
those responsible for crimes could be exposed and held accountable. If the damage report soon to be released by the Intelligence Community reveals that, in fact, none of the information Manning leaked actually endangered lives or harmed national security, then Manning has more ground to stake his ethical claim.

Ultimately Manning saw himself as a whistle-blower, not a traitor. Whether the Intelligence Community or the U.S. military committed any crimes remains a topic of debate. The point is, however, that the Intelligence Community needs to maintain its integrity and ethical values to reduce potential negative effects on its reputation. If information is developed that raises and implies unethical behavior, the Intelligence Community needs to deal with it appropriately. If not, eventually agencies within the Intelligence Community will become wary of the idea of exchanging information to a greater extent, if they believe that ethical procedures are not in place for the storage and transmission of that information. Systems must be “cleansed.”

Agencies within the Intelligence Community will become even more wary than they currently are of what they share and with whom to reduce the risk of their information being leaked. Furthermore, public scrutiny and the media are powerful. They have the ability to threaten the efficiency of the Intelligence Community’s information-sharing environment. The Intelligence Community must encourage a culture of sharing information in an ethical manner, while improving its clearance investigation procedures, network security, and counterintelligence measures.
The Bureau of Investigation was founded in 1908 and did not become known as the Federal Bureau of Investigation (FBI) until 1935. The FBI has always been and remains a law enforcement-centric organization. The culture of law enforcement that the bureau adopted has been engrained for nearly a century. This is a significant span of time for the culture to develop and permeate its fundamental values and practices, when considering the multiple decades of continued reinforcement and repetition.

Today the FBI is working toward becoming a more intelligence-driven and threat-focused national security and law enforcement organization. Although the FBI is leaning toward becoming more intelligence focused in support of its law enforcement mission than it has been historically, the bureau holds its position that it has conducted intelligence analysis in support of criminal investigations and domestic as well as international threats for decades.

The history of FBI intelligence began in 1917, when the bureau was authorized to detain enemy aliens during World War I. Since then, the FBI’s intelligence mission has evolved to adapt to changes in terrorist and criminal threats. One thing remains certain, however: the FBI has always maintained that the heart of its operations lies in its investigations and law enforcement, which serve, as the FBI mission states, “to protect and defend the United States against terrorist and foreign intelligence threats and to enforce the criminal laws of the United States” (FBI 2012d, para. 1).
intelligence-related functions that the FBI executes exist to underpin and serve all investigative programs.

A significant change in the FBI’s intelligence history occurred shortly after and mainly in response to 9/11, in which FBI Director Robert Mueller called for a reengineering of the bureau’s structure and operations. Specifically, Mueller wanted the FBI to focus on preventing terrorist attacks, countering foreign intelligence operations against the United States, and addressing cybercrime-based attacks and other high-technology crimes. This was a significant change for the bureau, as it involved initiatives to be more forward-leaning in its intelligence and criminal investigation responsibilities, rather than reactive and after-the-fact, as it had been historically.

In addition to the aforementioned initiatives, the FBI remains dedicated to protecting civil rights while combating public corruption, organized crime, white-collar crime, and major acts of violent crime. Many of the initiatives Mueller enacted were designed to address the information-sharing challenges the FBI experienced, as the 9/11 Commission had found. The FBI has come a long way in its evolution of intelligence efforts and initiatives to share information, both internally and with the Intelligence Community. Although the FBI is and most likely will always remain a law enforcement organization, it is working toward becoming more intelligence-focused to support its law enforcement mission. The issue, however, is that the FBI remains overwhelmingly law enforcement-centric to the point where this focus inhibits its ability to execute its intelligence-related responsibilities effectively.
The FBI continues to take a law enforcement approach when dealing with counterterrorism and homeland security issues. Internal and external challenges plague the relationship and exchange of information between agents focused on law enforcement and analysts focused on intelligence within the bureau, despite sharing the same high-level mission objective. It is important to examine the organizational cultural challenges that still prevail in the FBI’s information-sharing environment. Closely examining FBI law enforcement and intelligence relationships, history, and present-day context, using case studies to illustrate cultural shortcomings, will aid in this analysis.

The 9/11 Commission has produced a report titled *Law Enforcement, Counterterrorism, and Intelligence Collection in the United States Prior to 9/11: Staff Statement No. 9* (9/11 Commission 2004a). The report revealed findings regarding law enforcement and intelligence collection in the United States before the 9/11 attacks. The report’s findings will serve to guide a significant portion of this analysis, as the investigations conducted were thorough. It is important to note, however, that the report does not identify culture as a hindrance or solution for promoting cooperation and information-sharing efforts between law enforcement and intelligence within the FBI. This should serve as yet another significant piece of evidence toward the U.S. government’s inability to identify culture as affecting information-sharing efforts within the Intelligence Community.

The relationship and sharing of information between law enforcement and intelligence within the FBI is critical to its mission success. In principle, the
relationship should be symbiotic. It is equally as important for intelligence analysts to share information with agents as it is for agents to share information with analysts. Information is passed from analyst to agent, as agents use that information to build cases, make arrests, and conduct other law enforcement-based efforts. Without intelligence backing investigative efforts, agents may be missing the total information picture.

Similarly, intelligence analysts need agents to relay information to them to adjust their analysis accordingly. FBI agents may discover information in the field that they believe could improve the overall intelligence picture and should relay that information back to the analysts. Before 9/11 the FBI focused primarily on executing law enforcement responsibilities primarily after crimes had occurred. To be more forward leaning, the FBI must focus on intelligence capabilities such as collections and analysis, in order to better support its law enforcement mission.

Historically and “consistent with its traditional law enforcement approach, most of the FBI’s energy during this period was devoted to after-the-fact investigations of major terrorist attacks in order to develop criminal cases” (9/11 Commission 2004a, 1). The majority of FBI counterterrorism expeditions were focused on targeting insurgent operations outside the United States, primarily in Saudi Arabia, Somalia, and other areas where U.S interests were located in foreign territories. Today, particularly as a result of 9/11, the FBI’s counterterrorism efforts are becoming more focused on domestic threats. The FBI had been forced to expand its intelligence responsibilities as
a result of 9/11. Counterterrorism was considered a critical intelligence activity by the FBI needed to support law enforcement objectives.

The intelligence professionals whom the FBI employed before 9/11 focused primarily on analyzing ways to deter crime in support of law enforcement operations. The FBI generally confronted criminal activity only after a law was breached. “The FBI took a traditional law enforcement approach to counterterrorism. Its agents were trained to build cases. Its management was deliberately decentralized to empower the individual field offices and agents on the street” (9/11 Commission 2004a, 3). For a long time, the FBI continued to operate in a decentralized manner, where agents and intelligence analysts were often encouraged to work independently in separate locations, and a very low premium was placed on sharing information or solving problems collaboratively. Not until after 9/11 did the FBI began shifting its priorities to focus more on counterterrorism.

Issues with outdated technology within the FBI further complicated agent and analyst information-sharing efforts. “Given the poor state of the FBI’s information systems, field agents usually did not know what agents in their own office, let alone in other field offices, were working on. Nor did analysts have easy access to this information. As a result, it was almost impossible to develop an understanding of the threat from a particular international terrorist group” (9/11 Commission 2004a, 3). Technology specialists comprised a very small percentage of FBI staff, and the technology the organization used was often outdated. In some cases, the technology the FBI used was based on designs produced in the 1980s.
The FBI’s primary information management system, designed using 1980s technology was already obsolete when installed in 1995, limiting the Bureau’s ability to share its information internally and externally. The FBI did not have an effective system for storing, searching, or retrieving information of intelligence value contained in its investigative files. (9/11 Commission 2004a, 9)

The lack of adequate technology severely limited the FBI’s ability to make effective interventions when attempting to understand potential terrorist threats. This lack of cohesion and effective communication between agents and analysts as a result of technology barriers created an information disconnect. Ultimately, the disconnect led to situations where analysts were often unaware of what agents knew about any particular case. “Agents investigated their individual cases with the knowledge that any case information recorded on paper and stored in case files were potentially discoverable in court” (9/11 Commission 2004a, 3). This resulted in a disincentive to share information from agents to analysts in the fear of information leaking and compromising a case.

FBI agents had deep concerns regarding the possibility that the information they might choose to share could be exploited by defense attorneys, and that could negatively affect the professional standing of an agent within the bureau. To minimize the threat of undermining the strength of the FBI’s court cases against defendants, agents took all necessary precautions to refrain from sharing information that could undermine the agency’s ability to prosecute alleged criminals successfully. Successfully prosecuting alleged criminals had gained a higher priority than sharing intelligence that may have been critical to promoting national security.
“According to another external review of the FBI, by the year 2000 there were twice as many FBI employees devoted to drug enforcement matters than towards counterterrorism issues. On September 11, 2001, only about 1,300 agents, or six percent of the FBI’s total personnel, worked on counterterrorism” (9/11 Commission 2004a, 4). This shed light on how the FBI prioritized its tasks, and clearly counterterrorism was not regarded as one of the main priorities.

A report by the Justice Department inspector general in 2003 stated that before 9/11, “the Bureau devoted significantly more special agent resources to traditional law enforcement activities such as white collar crime, organized crime, drug, and violent crime investigations than to domestic and international terrorism issues” (9/11 Commission 2004, 4). Far more agents were assigned to duties regarding domestic law enforcement than terrorism, while analysts were too preoccupied with drug-related crimes to pay sufficient attention to terrorism.

The aforementioned actions and attitudes the FBI exhibited indicate that the bureau had underestimated the threat of terrorism on home soil. This was understandable in light of the fact that before 9/11, the U.S. had not suffered a terrorist attack that affected the psyche and sense of security among Americans so deeply. The attitudes that FBI agents commonly displayed before 9/11 with regard to combating terrorism were also understandable, in light of the fact that the FBI had traditionally been a domestic law enforcement agency, and the attention to counterterrorism had historically been only a supplemental undertaking.
Artifacts: Cultural Challenges in FBI Promotion and Hiring

FBI policy and institutional requirements, among other factors, play an important role in guiding the behavior of its members. FBI employee actions, however, are also guided by more subtle sociocultural forces that they are often unaware of. Schein’s model operates under three elements of culture previously described in this thesis: artifacts, espoused values, and basic underlying assumptions. These cultural elements are intertwined as they influence one another and contribute to the overall cultural worldview embraced by the FBI. To understand the nature of the FBI’s worldview and how this perspective affects the bureau’s information-sharing efforts, it is necessary to engage in an analysis that breaks down each cultural element.

The best cultural elements to use as a starting point are artifacts. According to Schein, artifacts are the easiest cultural elements to recognize, because they are often observable, unlike the more subtle elements of espoused values and basic underlying assumptions. The artifacts that will be examined within the FBI are its highly visible behaviors, which include its promotion system.

The FBI is working toward improving its law enforcement mission by supplementing it with a myriad of intelligence responsibilities and functions. This primarily included counterterrorism efforts, as previously described. This transition has led to the acquisition of new intelligence skill sets within the bureau, such as collections and analysis. The FBI has been forced to grow (and take initiative) to adapt to its new internal and external demands. Organizational culture’s two major functions
are external adaptation and internal integration (Schein 2010, 18). If an organization such as the FBI cannot adapt to changes in the internal and external environment, it runs the risk of becoming less effective. The FBI has been forced to grow due to its expanded intelligence mission, and its newly hired staff now includes, but is not limited to, intelligence analysts, collectors, cryptographic linguists, imagery analysts, signals analysts, and a myriad of technical experts.

With new employees come new challenges. The FBI has historically determined how well it believes it is performing to expectations by its capture and arrest record; however, adopting new intelligence professionals introduces new challenges in terms of how the FBI evaluates its performance and, as a result, its employee promotion system. It has always been very easy for the FBI to set the expectations for agent promotions, as the number of arrests or investigations successfully concluded are criteria that are easy to quantify and assess. Just like the police who need to issue a certain number of tickets per month to make their quota, FBI agents are promoted based on quantifiable criteria such as the number of arrests—the logic is very simple.

Intelligence analysis production and performance, on the other hand, can be very difficult to evaluate. The main reason why is that not all intelligence leads to a final end-product. In many cases, analysis is conducted simply because there is a perceived threat. That threat, however, may only contain a very small chance of occurring, which is completely normal in intelligence production; this, in turn, means that intelligence is unlikely shared from analyst to agent, as in the case of the FBI.
Therefore, the analyst may have very little to show for his or her efforts other than perhaps a report on a perceived threat that never occurred. This does not mean that the intelligence analyst has not done a good job; it just means that the analyst has a difficult time proving he/she has done a good job.

An interview I conducted on February 17, 2012, with an intelligence analyst from the National Counterterrorism Center (NCTC) provided insight into its promotion system. The NCTC mission is to lead the effort to combat terrorism both in the United States and overseas by analyzing potential threats and sharing that information with mission partners. The analyst claimed that a significant portion of the criteria for promotion of a government analyst within NCTC was based on the number and quality of intelligence products produced. The interviewee said that it did not matter whether the product did not result in preventing a national security disaster; it only mattered that the product was analytically sound and well received primarily by NCTC and secondly by the Intelligence Community (NCTC interview, 2012).

It appears that NCTC has discovered an effective method for evaluating performance in terms of intelligence products produced. The interview further revealed that in many cases, the nature of intelligence is based on situations or threats that may never occur, and by design such intelligence is not necessarily intended to prevent terrorists from entering the United States or to avert major security failures, for example. In many cases, intelligence analysts simply create products on historical findings, knowing that the vast majority of such products do little more than provide some helpful insight to other analysts or leaders.
The interviewee stated that the quality and amount of such research products are considered criteria for promotion, and, therefore, the opportunity to accept such a responsibility is usually embraced. This issue of intelligence analysts’ being able to prove worth is compounded in the FBI more so than any other agency in the Intelligence Community, mainly because of the FBI’s law enforcement-centric mission. The FBI would benefit from embracing an evaluation structure similar to that of the NCTC, which emphasizes the quality of an analyst’s product and not necessarily whether that product has led to an arrest or capture or prevented a national security failing.

Before 9/11, it was discovered that within the FBI the opportunity to embrace such tasks was rare. FBI personnel who had the professional responsibility to engage in intelligence efforts were rarely given sufficient incentive to perform to the best of their abilities. Intelligence analysts who specialized in counterterrorism were rarely treated with professional respect commensurate to their value to the organization, skills, and accomplishment. On many occasions, FBI intelligence analysts were required to perform menial tasks that were clearly not related to their professional responsibilities, such as data entry and answering telephone calls (9/11 Commission 2004a, 9).

There is a promotion culture and history engrained within the FBI to reward employees based on arrests, convictions, and successful investigations. “The Bureau rewarded agents based on statistics reflecting arrests, indictments, and prosecutions. As a result, fields such as counterterrorism and counterintelligence, where investigations
generally result in fewer prosecutions, are viewed as backwaters” (9/11 Commission 2004a, 3).

Expecting the FBI to change its culture of hiring and promotion overnight when it has existed for decades is a challenge. Additionally, why would an FBI intelligence analyst feel motivated to share information with an agent for which the analyst may ultimately receive no credit? This creates yet another information-sharing gap between analyst and agent. The FBI’s system of promotion is an element of culture as defined by artifacts. It is observable, and its implications are vast. If intelligence analysts are not given incentives to remain in the FBI, because they cannot advance, information-sharing efforts will inevitably worsen, and employee retention potentially will decline. Intelligence analysts’ ending their careers early because they cannot move up the chains of command means that expertise in various intelligence disciplines does not grow. It also means that over time there will be fewer intelligence leaders within the FBI who can grow and nurture the intelligence workforce.

According to the 9/11 Commission, there were some cases where promotions were issued to individuals solely on the basis of loyalty to the organization and a willingness to follow orders. The FBI implements the same system as the federal Office of Personnel Management for hiring and promotion. Therefore, background and experience should determine grade level. Recruitment bonuses are occasionally awarded for hard-to-fill critical skills positions, such as subject matter expertise and in-depth knowledge of specific cultures. Such bonuses are not guaranteed and, if awarded, are given one to three years into employee service in the organization.
According to the FBI’s Directorate for Intelligence (DI), promotions, rewards, and recognitions are based on demonstrated knowledge, skills, and abilities outlined in each grade level. The DI states that “the higher up on the promotion ladder, the more comprehensive and complex are the promotion criteria—with emphasis placed on technical skills and subject matter expertise” (FBI 2012a, under “Promotions, Rewards, and Recognition”). This would indicate that an FBI intelligence analyst must earn his or her promotion by displaying various skills and working hard.

In contrast, however, there is an automatic promotion structure built into the FBI special agent promotion system. FBI special agents are automatically promoted from GS-10 to GS-13 after five years of service, without any additional interview process (Egli 2011, 34). This appears to be somewhat unfair to the analyst when comparing the bureau’s two promotion systems. The FBI special agent system seems to emphasize the importance of loyalty to the organization, with less emphasis on background, experience, and skills.

As previously stated, FBI intelligence analysts are faced with a myriad of challenges, including a lack of incentive to share, difficulty in proving their worth, and outdated technology crucial to doing their job effectively. Remaining loyal to the organization becomes difficult for the analyst when considering the contrast in promotion systems. It is also important to note that the criteria for FBI analysts to advance in General Schedule (GS) status do not include consideration of how effectively the analysts share information or collaborate with others. Therefore, it can
be concluded that the criteria for promoting within the FBI lack sufficient incentive to encourage information sharing.

If the FBI truly wants to encourage information sharing, there must be an incentive to do so that is built into the bureau’s systems for promotion, reward, and recognition. Both the promotion and reward systems are considered observable artifacts within Schein’s model. “The most powerful mechanisms that founders, leaders, managers, and parents have available for communicating what they believe in or care about is what they systematically pay attention to,” both explicitly and implicitly (Schein 2010, 237). Therefore, FBI leaders have an obligation to show they care about the sharing of information consistently and through all channels available to them, including the bureau’s promotion system.

The artifacts that can be identified within the FBI that influence its culture are vast. Promotion procedures and hiring are just a few examples of observable elements. According to Schein’s model, there are primary and secondary culture-embedding mechanisms that further drive cultural development in organizations. In new developing cultures, the secondary articulation and reinforcement mechanisms act to support culture, not create it (Schein 2010, 250). Figure 3 illustrates the relationship between primary and secondary culture-embedding mechanisms.

It is important to remember that each observable element (i.e., artifact) ultimately contributes to the overall shaping of an organization’s culture. Taking one of the examples in figure 3 of an artifact titled “Observed criteria by which leaders allocate rewards and status,” one can see that it translates to “Stories, legends, myths
about people and events.” It is visually easier to comprehend through this figure how if rewards, incentives, and ultimately promotion are not addressed fairly across both the intelligence and investigation departments of the FBI, it will not be long before such incidents translate to rumors and stories concerning inequality.

The danger is that the stories affect people’s perceptions regarding the reputation and organizational culture of the FBI. Rumors concerning the agency’s business practices eventually leak outside into the Intelligence Community and alter people’s perceptions of the bureau. Ultimately, intelligence professionals will become deterred at the prospect of working for the FBI, which ultimately will affect the efficiency of its information-sharing environment, at a key point in history when the FBI is struggling to transition. Furthermore, these rumors, if frequent enough, can

<table>
<thead>
<tr>
<th>Primary Embedding Mechanisms</th>
<th>Secondary Articulation and Reinforcement Mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>What leaders pay attention to, measure, and control on a regular basis</td>
<td>Organization design and structure</td>
</tr>
<tr>
<td>How leaders react to critical incidents and organizational crises</td>
<td>Organizational systems and procedures</td>
</tr>
<tr>
<td>Observed criteria by which leaders allocate scarce resources</td>
<td>Organizational rites and resources</td>
</tr>
<tr>
<td>Deliberate role modeling, teaching, and coaching</td>
<td>Design of physical space, facades, and buildings</td>
</tr>
<tr>
<td>Observed criteria by which leaders allocate rewards and status</td>
<td>Stories, legends, myths about people and events</td>
</tr>
<tr>
<td>Observed criteria by which leaders recruit, select, promote, retire, and excommunicate organizational members</td>
<td>Formal statements of organizational philosophy, values, and creed</td>
</tr>
</tbody>
</table>

Figure 3. Primary and secondary culture-embedding mechanisms in the form of artifacts. Source: Schein 2010, 236.
become deeply entrenched in the cultures, becoming part of the organization’s espoused values or basic assumptions.

**Espoused Values: FBI Priorities and Core Values**

Espoused values primarily reflect group learning. In an organization such as the FBI, the group leader establishes values and goals for the organization (Egli 2011, 7). There is an expectation that is passed down from leaders to managers to staff members that the values should be adhered to. Espoused values may be communicated verbally or appear in the form of strategies, philosophies, or doctrines. The FBI maintains a list of its mission objectives in order of most important to least important, which are numbered and clearly listed on its official website. These are the FBI’s priorities:

1. Protect the United States from terrorist attack;
2. Protect the United States against foreign intelligence operations and espionage;
3. Protect the United States against cyber-based attacks and high-technology crimes;
4. Combat public corruption at all levels;
5. Protect civil rights;
6. Combat transnational/national criminal organizations and enterprises;
7. Combat major white-collar crime;
8. Combat significant violent crime;
9. Support federal, state, local and international partners;
10. Upgrade technology to successfully perform the FBI’s mission.

(FBI 2012c, under “Our Priorities”)

The 9/11 Commission determined that inadequate technology and lack of training were two significant causes for the attacks. In the case of the FBI, the commission’s investigations determined that its systems were severely outdated and in desperate need of upgrading. The risk of not improving the FBI’s systems could lead to future security failings such as terrorist attacks. Protecting the United States from terrorist attacks is listed as priority 1 on the FBI’s website. It would seem logical, however, that to prevent future attacks, the technology systems that have the ability to assist in identifying terrorists should probably reside at a higher priority, because one is affected by the other.

There also appears to be an error in logical sequencing even when examining priority 3 against priority 10. Priority 3 dictates the need to protect the United States from cyber-based crimes and high-technology attacks. Realistically, one needs technology to defend and fight adversary technology, so again the point is raised as to why upgrading the FBI’s systems remains its lowest priority. It also appears as if training on those technology systems is absent from the listed FBI priorities. As was the case with the FAA’s TIPOFF system, a lack of training on the program’s features may have contributed to the 9/11 attacks. Training on technology is absent from the FBI’s list of priorities, but, more importantly, there seems to be a failure to recognize how A affects B. In other words, the advancement of technology (priority 10) and the
training of technology (no priority listed) together effectively promote other objectives, such as priorities 1 and 3.

Furthermore, the sharing of information among mission partners is not listed as an FBI priority. It would be reasonable to conclude that given the 9/11 Commission’s findings, the FBI would have made information sharing one of its top priorities. The closest the FBI comes to addressing the potential for information sharing in its list is priority 9—support federal, state, local, and international partners. The term *support* is very general and may imply information-sharing efforts with mission partners, but why not state it explicitly? If the FBI intended to mean support to mission partners in the form of training, equipment, data exchange, or other means, then it would behoove the bureau to be explicit in order to avoid misinterpretation of its priorities.

The analysis of the FBI’s priorities would not be complete without identifying culture as missing from its list. Similar to the ODNI’s list of objectives outlined in its 500 Day Plan, every one of the FBI’s priorities would require a certain degree of cultural change to accomplish its goals, and yet culture is absent from its list. However, the goal is not necessarily to conduct an audit of the FBI’s priorities listing. Rather, it is to show how FBI leadership has set goals to which it expects its organization to adhere and how those goals ultimately translate to the espoused values of the bureau.

To drill down one cultural level further, it is necessary to examine the FBI’s core values. The FBI is guided by the motto, “Fidelity, Bravery, Integrity,” and these core values:
1. Rigorous obedience to the Constitution of the United States;

2. Respect for the dignity of all those we protect;

3. Compassion;

4. Fairness;

5. Uncompromising personal integrity and institutional integrity;

6. Accountability by accepting responsibility for our actions and decisions and the consequences of our actions and decisions; and

7. Leadership, both personal and professional.

(FBI 2012c, under “Our Core Values”)

Schein states that artifacts, espoused values, and basic assumptions are often connected and influence one another. For example, the core values or espoused values that an organization holds dear can ultimately influence its observable elements or artifacts. There is an intimate relationship between what an organization values and what those values ultimately translate to on the surface in order to be observed by its members.

First, the FBI’s list of core values is excellent, because, particularly in a law enforcement environment, the need to obey the Constitution, be fair, be compassionate, and maintain integrity are more crucial than in most other occupations. Police, for example, hold tremendous power that can easily be abused, and so they view the values of integrity and fairness as being extremely important (Department of Maryland State Police n.d., under “Our Values). By virtue of their position, law enforcement
professionals can become more susceptible to corruption or abusing their power, and, therefore, the values that guide them must be tailored accordingly.

Although the FBI’s listed core values are outstanding and, in fact, good personal values by which to live, not just professionally, the issue is that they are very law enforcement-centric. Mueller states on the official FBI website that its core values “need to be preserved and defended by the FBI in performing its statutory mission” (FBI 2012b, under “FBI Core Values”).

It could be perceived that the FBI is still very much engrained in the legalities and constitutional authorities of its mission. The FBI is still struggling to become less overwhelmingly law enforcement-focused to incorporate greater intelligence responsibilities within its framework. If the FBI truly wants to instill change at a deeper cultural level of its organization, it should consider tailoring its core values to ones that also speak to the importance of intelligence efforts.

When one combines the FBI’s list of priorities, which do not mention the need to share information, with its list of core values, which are heavily based on law enforcement, the result is a culture that will find it a struggle to change and adapt to counterterrorism and information-sharing efforts. Furthermore, there is a risk in confusing FBI agents and analysts, who by all accounts may be told either verbally or through policy to share information. But at the end of the day, the priorities and values that are embedded in the culture do not promote such an environment.

The FBI would benefit from revising its list of priorities and core values to include language that promotes its law enforcement mission, while also articulating the
importance of intelligence in support of that mission. If the FBI hopes to revise its list of priorities and core values, it may require leadership intervention. According to Schein, leadership acts as the main architect of creating culture (Schein 2010, 297). An individual such as Director Mueller could potentially tailor the values of the FBI to shape the culture in order for the bureau to be more focused on sharing and intelligence in support of its law enforcement mission.

The FBI desires to operate in a way reminiscent of a law enforcement agency, and understandably so. More than a century of law enforcement-centric culture is embedded within the FBI, and its adherence to that culture is apparent by its list of core values. The FBI is still in a transition phase, and the bureau does not deny this transition. The FBI’s official website has posted the following statement: “The FBI’s transformation to an intelligence-driven organization remains a work in progress” (FBI 2011, para. 3).

**Basic Underlying Assumptions: FBI Hiring and Training**

Basic assumptions are the deepest level of culture and provide an organization’s members a set of rules to guide their behavior. The rules are not necessarily literal, but provide members the guidance to feel, interpret, and pay attention to certain things. “When a solution to a problem works repeatedly, it comes to be taken for granted” (Schein 2010, 27). Members may not even realize that alternative solutions exist when preexisting solutions have worked well for an extended period of time. Because so much of what guides members of organizations to feel in relation to
their environment is based on conditioning, the analysis of the FBI’s basic assumptions will focus on the hiring and training of its employees.

Schein asserts the vital importance of employee selection in affecting culture (Schein 2010, 249). Leaders tend to replicate the current workforce in their hiring. Those perceived to be the best and brightest are those who resemble current top performers and culture adapters “in style, assumptions, values, and beliefs” (Schein 2010, 249). Before 9/11, the FBI displayed considerable resistance to accepting qualified intelligence analysts from external sources, even analysts from other intelligence agencies. Instead, the FBI preferred to promote employees from within the bureau.

The desire and practice to promote internally is understandable, as employees want to see their fellow coworkers and themselves move up the chains of command. Such a practice improves employee morale and workforce retention, which is deeply important to the culture of an organization. This proved to be highly problematic for the FBI, however, as the bureau sold itself short in its potential to hire qualified and experienced intelligence professionals externally. There was an “FBI tradition of hiring analysts from within the agency rather than recruiting individuals with the relevant educational background and expertise. In our field visits, we encountered several situations in which poorly qualified administrative personnel were promoted to analyst positions, in part as a reward for good performance in other positions” (9/11 Commission 2004a, 9).
Intelligence analyst candidates submit online applications through the FBI’s self-service system. The most qualified applicants are selected for interviews and additional testing. The results of this phase then determine whether the FBI makes a conditional job offer, which is contingent upon a background check, budget allotment, and the bureau’s critical skills needs. The background check is extensive, including credit and criminal checks, interviews with associates, reference checks, educational verification, and a polygraph. The hurdles are rigorous; this is considered essential to maintaining a professional and valuable workforce.

Given the rigorous nature of the hiring process, it is more vital than ever for the FBI to ensure that once intelligence analysts are brought onboard they are retained. Prospective FBI intelligence analyst candidates may become deterred by both an exhaustive hiring process and the lack of potential to advance their careers. Such a situation could lead to the FBI’s having to compromise on the rigorous nature of its hiring process to attract more candidates, which may result in security compromises due to the quality of candidates, or to the bureau’s being forced to change its promotion system. I favor the latter. If the FBI can improve its promotion system for intelligence analysts, then it can market this system to prospective candidates. Such an effort would be significant, as the FBI would have the opportunity to instill a culture of “need to share” at the earliest possible stages of employees’ careers.

Before 9/11 the FBI had very limited training in intelligence, given its focus on law enforcement, and it often struggled to find opportunities to gain a deeper understanding of intelligence techniques needed to combat terrorism effectively. The
problem of insufficient manpower devoted to issues of defense from foreign aggressors was compounded by administrative dilemmas. “Specifically, they believed that neither Congress nor the Office of Management and Budget fully understood the FBI’s counterterrorism resource needs. Nor did the FBI receive all it requested from the Department of Justice, under Attorney General Janet Reno” (9/11 Commission 2004a, 4).

Only a very small portion of the budget was dedicated to the FBI’s counterterrorism resources, and the government officials who were charged with the responsibility of providing intelligence analysts with resources, such as training, were altogether unaware of what was required to establish and operate an efficient department of counterterrorism. “FBI agents received very little formalized training in the counterterrorism discipline. Only three days of the 16-week new agents course were devoted to national security matters, including counterterrorism and counterintelligence, and most subsequent counterterrorism training was received on an ad hoc basis or ‘on the job’” (9/11 Commission 2004a, 8).

If the FBI were to create certifications in intelligence analysis, this would show employees that the bureau is taking its move toward an intelligence-focused agency seriously. The FBI should also encourage agents to receive this certification and perhaps even make it mandatory that they become familiar with certain intelligence analysis functions and technology systems. Not only would this improve the agents’ expertise on various intelligence disciplines, but it also would nurture a culture of
information sharing. Agents who are now familiar with their analyst counterparts’ job could learn the true value of intelligence analysis and collaborate more effectively.

**Case Study: The Fort Hood Shooting and the FBI**

The highly publicized Fort Hood shooting occurred on November 5, 2009, at a heavily populated military base in Killeen, Texas. A gunman killed thirteen soldiers and significantly injured twenty-nine others. The alleged culprit was Major Nidal Hasan, a military doctor stationed at Fort Hood. The attacker was shot and wounded, then arrested by military police. Hasan is facing thirteen counts of premeditated murder and thirty-two counts of attempted premeditated murder (Fox News Radio, 2011, under “#Twoppics – Military/Security”). Hasan’s trial is scheduled for June 2012, and if convicted, he faces the possibility of capital punishment.

The Fort Hood shooting revealed that several potential intelligence failures occurred that could have been prevented. In a 2010 annual report to Congress, the Program Manager for the Information Sharing Environment (ISE), Kshemendra Paul, stated that “the Fort Hood Shootings highlight challenges, successes, and gaps in our ability to effectively share and access information” (ISE 2010, 7). Furthermore, the Senate Homeland Security Committee stated in an official report that the FBI and DoD had sufficient information before the attacks that could have prevented the tragedies altogether (U.S. Congress 2011, 7–8). The Fort Hood shooting clearly shows that the Intelligence Community still faces information-sharing challenges nearly a decade after 9/11. The FBI was a key player in the investigations resulting from the Fort Hood
tragedies. Exploring the FBI’s role in the Fort Hood shooting will help reveal cultural factors still affecting its information-sharing efforts today.

The Fort Hood attack showed Hasan was psychologically disturbed, displayed antagonism toward “American imperialism,” and displayed sympathetic sentiments for jihadists and radical Islamists. Hasan was not only an ideological sympathizer with militant Islam, but he also maintained a personal relationship with a known member of al-Qaida, Anwar al-Awlaki. Hasan and al-Awlaki maintained an extensive e-mail correspondence, where the latter encouraged the former to take militant action against Americans and praised Hasan for his willingness to protect the religion of Islam (Baugmartner 2012, 32).

When Hasan was investigated after the shooting, his e-mail correspondence with al-Awlaki was discovered (Baumgartner 2012, 54). Al-Awlaki was known to be a member of al-Qaida and an online activist who openly promoted an attitude of hostility toward the United States (Shawcross 2012, 17). Al-Awlaki was an engineer and a professional educator who received a master’s degree from the University of San Diego and was working on a PhD at George Washington University (Shawcross 2012, 19). As an eloquent, educated, gifted orator who was fluent in English, al-Awlaki assiduously aspired to influence the non-Arabic Islamic communities in an effort to ignite revolutionary ambitions within potential sympathizers of jihadism and embolden sympathetic audiences to fight American imperialism by all means necessary (Shawcross 2012, 18).
Al-Awlaki routinely posted videos of his sermons denouncing the United States and promoting terrorism (Shawcross 2012, 22). The Yemeni preacher was not only a gifted orator who was commended by his audience for forcefulness and eloquence of his sermons, but he also displayed remarkable psychological insight when selecting the targets of his indoctrination. Because al-Awlaki was educated in the United States and lacked the rigorous training in Islamic literature that many of his colleagues who were educated in the Arab world had, he struggled to gain a sizeable following within the Arab world; therefore, he faced the challenge of reaching out to a distinctly English-speaking audience.

Al-Awlaki’s messages were carefully designed to appeal to people who were solitary, alienated, and potentially sympathetic to radical Islamism. Many of the followers whom he attracted were impressionable young men who were easily influenced not only by his oratorical talents, but also by his ability to use social media websites effectively. Although Hasan was not as impressionable as many of al-Awlaki’s other acolytes, he was socially alienated and displayed sympathetic traits toward Islamic extremism, making him an excellent target. Al-Awlaki’s relationship and influence ultimately drove Hasan allegedly to commit the shootings at Fort Hood.

In February 2011, U.S. Senator Joseph I. Lieberman, chairman of the Committee on Homeland Security and Governmental Affairs, released a special report titled *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government’s Failure to Prevent the Fort Hood Attack* (U.S. Congress 2011). The report investigates what information the U.S. government had before the attacks, the actions it took or
failed to take to prevent the attacks, and future recommendations for improvement in preventing future attacks.

The overall conclusion that the Senate committee reached was this: “Although neither DoD nor the FBI had specific information concerning the time, place, or nature of the attack, they collectively had sufficient information to have detected Hasan’s radicalization to violent Islamist extremism but failed both to understand and to act on it” (U.S. Congress 2011, 7). The report goes on to state that “the FBI and DoD together failed to recognize and to link the information that they possessed about Hasan” (U.S. Congress 2011, 8). This information-sharing failure between the FBI and DoD is of the most concern to this case study.

The Senate committee report cited DoD for failing to respond to Hasan’s outward displays of radicalism from 2003 through 2009. “Hasan’s public displays of radicalization toward violent extremism during his medical residency and post-residency fellowship were clear and led two officers to describe him as a ‘ticking time bomb’” (U.S. Congress 2011, 27).

During Hasan’s medical residency at Walter Reed Army Medical Center in Washington, D.C., fellow classmates reported that he conducted open class presentations that showed support for principles of violent Islamist extremism. One of Hasan’s presentations included a statement that spoke to the possibility of fratricidal murder of fellow service members, and he spoke against Muslim Americans in the military being put in combat situations against other Muslims. Despite the fact that
 Hasan’s behavior disturbed his instructors and classmates, no action was taken against him.

The Senate committee report states that service members with religious preferences do not pose a risk, but if those views are based on radical ideology that is a corruption of religion, it can be detrimental to military operations. A person who “embraces violent Islamist extremist ideology clearly is unfit to serve in the U.S. military” (U.S. Congress 2011, 27). Hasan’s history of making Islamist extremist beliefs as public statements continued throughout his residency and career, even articulating at one point his support of suicide bombings and that his religion took precedence over his belief in the U.S. Constitution. In spite of Hasan’s extreme views and overt public comments, his superiors failed to discipline him, refer him to counterintelligence authorities, or seek to discharge him from the military. The Senate committee report concluded that DoD had full knowledge of Hasan’s extreme views and problematic behavior, yet took no action against it (U.S. Congress 2011, 8).

The FBI knew that Hasan was a radical extremist before the Fort Hood shooting occurred. In fact, the FBI had already flagged Hasan as a result of intelligence reports received that cited his radical views and questioned his loyalty to the United States. The FBI had created a Joint Terrorism Task Force (JTTF) in San Diego, which was composed of people representing several agencies within DoD, as well as state and local governments. The purpose of a JTTF is to act as a counterterrorism fusion center, pulling in expertise and resources from across the community to provide a well-rounded picture of perceived threats.
Through intelligence reports received, the San Diego JTTF learned that Hasan was communicating with al-Awlaki. Incidentally, al-Awlaki was the subject of a separate counterterrorism investigation already underway within the San Diego JTTF. The initial report that detailed Hasan’s interaction with al-Awlaki raised concern and was flagged for further inquiry. In due diligence, DoD representatives at the San Diego JTTF checked a military personnel database, but mistakenly concluded that Hasan was a military communications officer, not a military commissioned officer, by misreading “comm. officer” in his military file (U.S. Congress 2011, 35).

A person supporting a “communications” role in the military could very well be a counterintelligence officer or someone doing communications work as part of his or her job duties. The San Diego JTTF made the decision not to disseminate Hasan’s report via operational intelligence channels, but rather to keep the reporting solely within the JTTF structure. “In lieu of sending a normal intelligence communication, the FBI agent at the San Diego JTTF sent a detailed memorandum to the Washington, DC, JTTF on January 7, 2009” (U.S. Congress 2011, 36).

Ultimately, this would prove to be a critical mistake, because had the San Diego JTTF sent the report through normal intelligence channels, the odds of DoD counterterrorism officials linking the report to Hasan’s outward displays of radicalism by DoD counterterrorism would have increased dramatically. The memorandum requested that the Washington, D.C., JTTF investigate Hasan, because he fell within the Washington JTTF’s jurisdiction, given his assignment at Walter Reed.
The San Diego JTTF also cautioned the Washington JTTF to approach the matter with sensitivity, given the potential for Hasan to be involved in a “communications” role, which may have explained why he was in contact with al-Awlaki. Shortly after the San Diego JTTF forwarded the memorandum, it received an additional intelligence report detailing further communications between Hasan and al-Awlaki. This second report was more troubling, as it described Hasan’s asking al-Awlaki for recommendations on specific violent actions one should hypothetically take against the U.S. military. This second report was never linked to the first report, and the San Diego JTTF never sent it to the Washington JTTF.

Six weeks later, on February 25, 2009, FBI leadership in the Washington JTTF asked the Defense Criminal Investigative Service (DCIS) to take the lead on an investigation into Hasan. DCIS is not a counterintelligence or counterterrorism agency, but rather a part of the DoD Office of the Inspector General, which primarily investigates fraud, waste, and abuse. The DCIS agent’s FBI supervisor in the Washington JTTF did not provide specific guidance on what action to take in the investigation. After ninety days, the DCIS agent finally conducted an investigation into Hasan that lasted approximately four hours and was completed on May 27, 2009 (U.S. Congress 2011, 36).

The DCIS agent’s investigation did not focus on whether Hasan was in the process of radicalizing to violent Islamic extremism, but rather whether Hasan was engaged in terroristic activities. The DCIS agent’s investigation included a query into the DoD personnel database that confirmed that Hasan was a military commissioned
officer and physician, not a communications officer. Additionally, the DCIS agent queried FBI databases that would have revealed whether Hasan was the subject of any prior investigations and found nothing.

Last, the DCIS agent obtained files from a DoD manpower center, which included Hasan’s military officer evaluation reports from 2004 to 2008 (U.S. Congress 2011, 37). The reports stated that Hasan had been promoted to the rank of major recently. Furthermore, the reports revealed that Hasan’s public displays and knowledge of radicalization toward violent extremism were interpreted to be an asset by his commanding officers, who believed such skills were valuable in analyzing terrorist threats. Additionally, the DCIS agent noticed that Hasan had made no attempt to conceal his identity while communicating with al-Awlaki, which the agent believed implied that the communications were legitimate research efforts.

The DCIS agent decided not to interview Hasan or his supervisors for two reasons. First, he believed that “Hasan’s communications were an outgrowth of the San Diego JTTF’s investigation of” al-Awlaki and that the Washington JTTF needed to tread carefully to avoid disrupting that investigation. … The DCIS agent was concerned that interviews of Hasan’s superiors and colleagues would cause that investigation to be revealed given that the DCIS agent believed that such officers would brief their superiors about the interviews. Second, the DCIS agent felt that interviews might jeopardize Hasan’s career and thus potentially violate the requirement that FBI investigations use the “least intrusive means” possible. (U.S. Congress 2011, 37)

The DCIS agent summarized his recommendations in a report that his FBI supervisor approved. Neither the DCIS agent nor the FBI supervisor took any further
action to disseminate their findings other than to provide the San Diego JTTF with a memorandum stating their conclusions. The San Diego JTTF received the memorandum and was shocked at the brevity of the DCIS agent’s reporting. The San Diego JTTF drew the conclusion that Hasan might have been “a confidential human source” of the Washington JTTF, given how superficial the Washington JTTF’s investigation seemed to be (U.S. Congress 2011, 37).

The San Diego JTTF contacted the Washington JTTF to register its concerns. The Washington JTTF stood by its conclusions, stating that the investigation had been conducted thoroughly. The San Diego JTTF did not press the matter further and did not make a formal request that the Washington JTTF “conduct a more thorough investigation of Hasan including interviews of his superiors and colleagues that would not require an explicit description of the FBI’s investigation into Al-Awlaki” (U.S. Congress 2011, 41).

Neither the San Diego nor Washington JTTFs linked the first report to the second report, which was more troubling regarding counterterrorism. The JTTF’s database was designed so that it did not allow for linking reports. The only way that reports in the database could be linked was by user memory. Analysts within the San Diego JTTF who received the second report on Hasan failed to link it to the first report, and, therefore, the Washington JTTF never learned of Hasan’s additional communications with al-Awlaki, which were of a greater counterterrorism concern.

To complicate matters further, only select people were allowed to access the database used to retrieve the reports. Access to the database was only granted to
specific agents and analysts, whom the FBI deemed as having a “need to know” (U.S. Congress 2011, 38). Therefore, the San Diego JTTF falsely assumed that the Washington JTTF had access to the database and would have known of any subsequent communications between Hasan and al-Awlaki. It was later revealed that not only did the DCIS agent not have access to the JTTF database, but he also did not even know that it existed. Furthermore, the DCIS agent assumed that the San Diego JTTF would automatically have sent him any additional communications that were pertinent to Hasan, as was the case with the first report.

Hasan’s final communication with al-Awlaki occurred in the summer of 2009. At no time were any of the reports that the San Diego JTTF received linked to one another. On November 5, 2009, the attack at Fort Hood occurred, and Hasan was arrested at the scene (U.S. Congress 2011, 41). Shortly after the media began reporting on Hasan’s attack at Fort Hood, the FBI agent told his DCIS colleague in San Diego, “You know who that is? That’s our boy!” (U.S. Congress 2011, 41).

The Senate committee reached several conclusions about how and why the FBI and DoD had failed to act effectively on intelligence received, which may have led to Hasan’s arrest. One conclusion was that “the FBI’s inquiry into Hasan failed to utilize intelligence analysts fully, in order to drive the purpose of the investigation and assess Hasan’s communications” (U.S. Congress 2011, 61).

Intelligence analysts were underused in assessing the threat that Hasan posed, and DoD information-sharing channels were considered an inappropriate route to disseminate the initial report on Hasan. Once intelligence analysts at the San Diego
JTTF had flagged the initial report on Hasan, they were never further consulted for analysis or insight. At the very least, an intelligence analyst could have assisted in interpreting whether Hasan was communicating with al-Awlaki for research or whether it was because Hasan was radicalizing toward violent Islamist extremism.

Furthermore, an analyst may have noted more traditional counterintelligence concerns and recommended further collaboration with DoD. The Senate committee concluded that “the lack of a role for intelligence analysts in the JTTF’s inquiry into Hasan raises alarm that the FBI’s effort to strengthen its intelligence analytic corps and to integrate it into the FBI’s investigative functions is incomplete” (U.S. Congress 2011, 63).

As previously stated in this thesis, the FBI’s attempts to improve intelligence before 9/11 were often met with cultural resistance, with analysts often performing secretarial or menial functions. This cultural divide between agents and analysts appears still to be prevalent, as the Fort Hood case study shows. A 2010 report by the FBI Intelligence Analysts Association stated that a “clear hierarchy exists in which agents occupy the ranks of senior executives, and analysts are still relegated to a category called ‘Support Employees’” (U.S. Congress 2011, 63). If the FBI wants to improve its intelligence functions to support its investigative operations, then it is critical that it ensures analysts have their rightful place within the bureau’s organizational culture. For agent-analysts relationships and information sharing to improve, analysts must be perceived as equals within the bureau. As previously stated
in this thesis, this can be achieved by improving the agency’s promotion and hiring systems.

Outdated or inefficient technology appears to be another recurring theme affecting information-sharing efforts within the FBI. The databases used by the JTTFs did not have the ability to link reports, which would have provided a greater overall picture of the perceived threat by Hasan. The 9/11 Commission cited the issue of outdated FBI technology as a major area of concern (9/11 Commission 2004a, 3). The issue appears to still be prevalent. Furthermore, there was the issue of access control to the JTTF database, which was only extended to select agents and analysts within the JTTF structure.

The DCIS agent in Washington not only did not have access to the database, but he also had no idea it even existed. Had the DCIS agent been able to access the JTTF database, he would have been able to view all communication reports pertaining to Hasan, providing a full picture of the perceived threat. The FBI relied on the DCIS agent to conduct a thorough investigation and yet did not provide him access to the database. The DCIS agent was, therefore, put in a position where he was relied upon heavily, but was not provided all the necessary tools to accomplish his objectives. Although the DCIS falls under the DoD’s command structure, the DCIS agent was assigned to the Washington JTTF and had an FBI supervisor. Once again, the FBI only granted database access to people who were deemed “need to know,” and therefore it appears as though there is a prevalent information-sharing challenge between the FBI and DoD.
The Senate committee concluded that “the inquiry into Hasan focused on the narrow question of whether he was engaged in terrorist activities, and not whether he was radicalizing to violent Islamist extremism and thus could become a threat” (U.S. Congress 2011, 66). Since the Washington JTTF had focused its brief investigation on whether Hasan was engaged in terrorist activities, it had failed to address whether Hasan could be in the process of radicalizing to violent extremism, which may have led to terrorist activity in the future. The Washington JTTF only focused on overt steps Hasan had taken and did not focus on the broader threat posed by a military officer communicating with a well-known terrorist (U.S. Congress 2011, 67).

Poor working relationships between agents and analysts at the San Diego JTTF compounded this problem. If agents had good working relationships with intelligence analysts within the San Diego JTTF, it is very difficult to comprehend why the misunderstanding of the term “comm. officer” could not have been investigated in a sensitive and secure manner. After all, DoD is part of the Intelligence Community, and DoD analysts working within JTTF could have reached out via classified channels to find the answers they were seeking regarding Hasan’s actual occupation.

Other key intelligence questions were never asked—questions such as what did the nature of Hasan’s communications with al-Awlaki teach about future modus operandi in the furtherance of terrorist objectives without actually breaking the law? It can be concluded that the FBI needs to work harder to ensure that its agents understand to a greater extent how intelligence affects investigative objectives. As iterated within this thesis, this may require an improved FBI intelligence training curriculum. An
improvement in the FBI’s training curriculum would foster greater collaboration between agents and analysts and provide the perception that intelligence and investigations are equally important to the bureau. In a response to the Senate committee’s report of the Fort Hood shooting on February 3, 2011, the FBI stated:

The FBI recognizes the value of congressional oversight and agrees with much in the report and many of its recommendations. During the internal FBI review undertaken immediately after the attack at Fort Hood, we identified several of the areas of concern outlined in the report, and, as noted in the report, have implemented changes to our systems and processes to address them. While concluding that the FBI’s transformation to an intelligence-driven organization remains a work in progress, the report recognizes the FBI’s substantial progress and many successes, led by Joint Terrorism Task Forces, in disrupting terrorist plots by homegrown extremists. (FBI 2011, para. 2)

It is evident that the FBI has made some progress in its effort to become less overwhelmingly law enforcement-focused, in order to better execute its intelligence responsibilities in support of its law enforcement mission. However, the FBI still struggles to complete this transition, and the Fort Hood shooting reveals cultural inhibitors still prevalent in the bureau since before 9/11. The FBI has publically agreed with the majority of the Senate committee’s identified gaps and recommendations for improvement. Looking to the future, the FBI will benefit greatly in examining the effect its organizational culture has on its information-sharing environment, particularly as evidenced by the Fort Hood security failings.
CHAPTER 10

CONCLUSIONS

The Intelligence Community’s progress since the 9/11 Commission’s investigations indicates that information-sharing efforts “seem to be improving and moving in a constructive direction” (Pellerin 2011, para. 8). The improvements are detailed in a progress report released by 9/11 Commission Chairman Thomas Kean and Vice Chairman Lee H. Hamilton, cochairs of the Bipartisan Policy Center’s National Security Preparedness Group (NSPG). Since 2001, the intelligence budget has increased to more than $80 billion. These funds have been used to establish or redesign 263 organizations, including 72 fusion centers and 105 joint terrorism task forces (Hamilton 2011, 3).

A significant portion of this budget has been geared toward resolving information-sharing challenges. Michael Vickers, undersecretary of defense for intelligence, stated that “the broader intelligence community has implemented significant reform, disrupting many plots and bringing to justice many terrorist operatives” (Hamilton 2011, 3). Vickers, who serves as the principal intelligence adviser to the secretary of defense, said that these accomplishments are in part highlighted by the Osama bin Laden operation, which “reflected the highest level of collaboration among IC agencies and the military” (NSPG 2011, 7). The NSPG reports that only nine of the forty-one 9/11 Commission recommendations are incomplete. The NSPG states that the FBI is still moving from being overwhelmingly law enforcement-
focused toward accepting a mission that places greater emphasis on the use of intelligence to achieve its objectives.

The NSPG calls for completion of the remaining nine recommendations and a vigilant, regular reassessment of priorities, expenditures, and vulnerabilities. The Intelligence Community has done well to address information-sharing challenges through a variety of solutions, correctly assuming that no single answer can fix the problem. Technology; policy; realignment and changes in priorities; and the creation of the ODNI are just a few examples of the positive steps enacted to address information-sharing gaps. During the past ten years, the Intelligence Community has attempted to enact change, but failed to identify all potential resisters to that change. Calls for changes in organizational culture are either absent from post-9/11 policies directing information sharing, or the concept of culture is misunderstood or misapplied within the context of those reports.

Although significant progress has been made in the information-sharing enterprise, the NSPG declares that there is still great room for improvement. “On the domestic side, however, there has been less unity of effort and much slower progress among multiple agencies that are either new or have new counterterrorism missions” (NSPG 2011, 11).

The FBI is one such agency still struggling with its newfound counterterrorism mission. The FBI has worked to modify the scope of its mission to encompass greater intelligence-related responsibilities and a more proactive counterterrorism approach. Although the FBI is still in transition, it has made some progress in its business process
by creating fusion centers to encourage in-person, multiagency, multimission collaboration. Additionally, the FBI has modified its list of top priorities to include counterterrorism and, in turn, revamped the language in its mission statements to support those priorities. The FBI still has work to do with improving its information-sharing efforts both internally and externally with mission partners, however, with such challenges being exemplified by the Fort Hood security failing.

A lack of cooperation between FBI and DoD officials, including a failure to take action on key intelligence, resulted in the tragedy that ensued on Fort Hood. That incident revealed the cultural issues still pervasive between agent and analyst relationships within the FBI. External FBI challenges still exist and were displayed through the lack of effective collaboration with DoD. The FBI’s potential success in achieving total information sharing will be heavily dependent upon its ability to address its organizational culture. The FBI must work toward promoting an environment that encourages the sharing of information through the changing of its employees’ attitudes, perceptions, and, ultimately, beliefs.

The recommendations outlined in this thesis include changes in FBI promotion, hiring, training, and core values. Specifically, the FBI must work toward improving these aforementioned systems to incentivize and encourage its intelligence and law enforcement workforce to share information. Schein states that learning and development cannot be understood without considering culture as the primary source of resistance (Schein 2010, 197). Intelligence analysts must feel the desire to retain employment, see the possibility of a future with the bureau through promotion, and be
provided with adequate training and technology to perform their jobs effectively. FBI analysts must feel they are equal to agents and possess the same potential to move up the chains of command. To accomplish this goal, the NSPG states that “a significant cultural change” must occur “which places the status of intelligence analysts on par with special agents, who have traditionally risen to management in the Bureau” (NSPG 2011, 7).

Furthermore, the FBI’s core values do not align with its new mission of becoming a more forward-leaning, intelligence-driven organization in support of its law enforcement mission. The FBI’s core values are heavily law enforcement-centric and do not speak to the transition that the bureau is attempting to enact. FBI employees are reminded of these core values each day they execute their mission, and these values ultimately influence information-sharing behaviors.

The Intelligence Community must work harder at shaping culture through its daily business processes and analytic tradecraft. Intelligence Community leaders must realize that although policy and directives assist in institutionalizing change, they are not singlehandedly the answers to transforming culture. Leaders must examine what the heart of their operations is—whether it is imagery, signals, collection, or analysis—and then modify the artifacts, values, and underlying assumptions to influence information-sharing objectives.

Shaping the organizational culture of the Intelligence Community will require a holistic and multifaceted approach that takes into consideration all the factors that drive information sharing. Ultimately, however, the most fundamental factor that must
be addressed is how to change the attitudes, perceptions, and beliefs of the Intelligence Community’s people.

Although efforts to encourage Intelligence Community members to change their behavior toward information sharing have been enacted, it is apparent that those members are still uncomfortable with the changes. All the individuals interviewed as part of this thesis have wished to remain anonymous. This is testament to the fact that members of the Intelligence Community still do not feel comfortable in their information-sharing roles and efforts. Many employees feel conflicted concerning when and how to share, as they receive mixed messages from the Intelligence Community’s leadership. This was apparent with the FBI interviewee who received guidance from ODNI leadership to share information via A-Space, but in contrast received guidance from the bureau’s leadership not to share information. It has been well recognized that each agency’s culture is unique, and, therefore, shaping the overall organizational culture of the Intelligence Community presents a great challenge.

Culture is the resistance to change as well as the solution, as Schein attests (Schein 2010, 350). Each agency maintains an identity to which many of its employees are personally and professionally attached. Many of the core values of organizations such as the FBI encourage a culture that extends beyond just the office and into their employees’ personal lives through such core values statements as “leadership, both professional and personal” (FBI 2012c, under “Our Core Values”). Thus, asking people to change their perceptions and attitudes toward intelligence, for example, can
be a sensitive matter, particularly among FBI agents who are engrained in a culture of law enforcement. Therefore, efforts to create intelligencewide initiatives such as the ODNI’s A-Space program must be handled with increased sensitivity concerning the existing cultural stovepipes these efforts are attempting to tear down.

The ODNI has impressed upon the community policies and directives demanding that employees share information, and the culture still has not had time to catch up. Former ODNI Assistant Deputy Director Wertheimer stated that “the goal is to empower a young new work force that will be leaders in five to 10 years and give them an environment in which they can excel and reach their potential” (AFCEA 2007, 2). It is to be hoped that Wertheimer is acknowledging that cultural change will not occur overnight and that a shift in people’s perceptions and attitudes will take time.

Changes in directives that stress that information sharing must occur immediately may need to reel back slightly or create a phased approach and allow (1) security and counterintelligence procedures to change and improve commensurate with advancements in technology, and (2) encourage culture and behavioral change commensurate with policy and directives. Ensuring that there is equal and parallel growth between these factors will reduce security failings and also ensure that the culture has had time to adapt to institutional information-sharing requirements.

If the ODNI hopes to achieve its continued goals of acting as the chief oversight and coordination authority for information-sharing initiatives, there must be a greater effort to reach out to the heart of analytic operations. Greater intelligencewide initiatives to share information should be introduced as close to the introduction of
employees’ careers as possible and further integrated into indoctrination and training procedures. Dr. Mark M. Lowenthal, president and chief executive officer of the Intelligence and Security Academy in Arlington, Virginia, states that “the community is good at intake training—getting a new hire grounded within each individual organization. However, individual agencies are not as good at training personnel in terms of the larger community” (AFCEA 2007, 2). The goal should be to promote a culture of Intelligence Communitywide sharing, as opposed to agency-specific. Moving forward, as agencies continue to share missions and values, the hope is that their cultures will align with the overall Intelligence Community information-sharing objectives. The artifacts, espoused values, and basic assumptions that drive cultural change will then be reflected in each agency.

The goal is not to exclude policy and directives among other initiatives, but rather to complement these important measures in order to provide a well-rounded approach to a common problem. However, “the formation of culture requires collective learning and repeated experiences of success or failure” (Schein 1995, 9). Therefore, once the foundation is laid through the heart of intelligence operations, then agency leaders can promote, reinforce, and condition the information-sharing culture more effectively.

Leaders must first conceptually understand what culture is (perhaps through a model such as Schein’s) and how it is embedded within their specific organization before they can change it. Such an effort will require leaders to understand their agency’s historical and existing culture in order to better understand the direction of
the future in which they want to take it. According to Schein, leaders in organizations must consider themselves “agents of change” and possess cultural expertise (Schein 1995, 6).

Because culture is socially constructed, each interaction reinforces, strengthens, or challenges the current organizational platform. Shifting the conversations can also change culture. Therefore, Intelligence Community leaders need to bridge the cultural transition, understanding how their own role-modeling, communications, and behavior influence other members in their organizations. Leadership is a social act, and this means that the Intelligence Community needs a strong executive culture that knows how to engage its members.

At this level, it is crucial for the Intelligence Community leaders to embrace a common culture of learning, information sharing, and continuous improvement in which they are socially involved with their people. Dysfunctional cultural elements cannot be immediately changed; however, they can evolve over time as these weaknesses diminish (Schein 1995, 7). When leaders see that cultural elements are changing in a desired direction, they must recognize and reward those behaviors. As a result, new standards of judgment and evaluation are needed, as is the case with the FBI’s much-to-be-improved systems of promotion and recognition.

Additionally, leaders must actively embody information-sharing values and act cooperatively. This includes ethical information-sharing practices while ensuring appropriate levels of security. Information needs to be both shared and protected. There are substantial security risks that need to be addressed as a priority to promote
overall national security. Restricting the flow of information is not always necessarily the answer, but rather controlling and monitoring access and usage is.

The larger the information-sharing pool, the greater the chance of a security failing. Responsible sharing of information can be achieved through (1) providing more robust counterintelligence efforts, (2) improving background investigations of people entering the Intelligence Community, and (3) improving network security to monitor potential internal and external threats.

Increased information sharing will also carry increased accountability for its associated risks, and, therefore, it is more important than ever for the Intelligence Community to ensure effective security procedures are in place. The Intelligence Community must create a culture of the highest expectations and standards to minimize security failings. By examining historical security failings like Manning as a learning opportunity, the Intelligence Community can improve the security of its information-sharing enterprise.

It is apparent by the failings of 9/11 and the initiatives since enacted that the Intelligence Community has made positive steps in the right direction to address improved information-sharing efforts. Although the Intelligence Community has made significant progress, there has been a failure to address organizational culture as significantly affecting these efforts. It is the hope that through this thesis the Intelligence Community will learn and understand the value of affecting agency culture and, as a result, continue to improve its information-sharing environment.
REFERENCES


National Commission on Terrorist Attacks upon the United States (9/11 Commission). 2004a. Law Enforcement, Counterterrorism, and Intelligence Collection in the


