COMBATING INSIDER THREATS: AN ANALYSIS OF CURRENT UNITED STATES INSIDER THREAT POLICIES AND NECESSARY IMPROVEMENTS

A Thesis

Presented to the

Faculty of the College of Graduate Studies at

Angelo State University

In Partial Fulfillment of the

Requirements for the Degree

MASTER OF SECURITY STUDIES

by

MICHAEL LAWRENCE PORTER, JR.

May 2014

Major: Intelligence, Security Studies, and Analysis

COMBATING INSIDER THREATS: AN ANALYSIS OF CURRENT UNITED STATES INSIDER THREAT POLICIES AND NECESSARY IMPROVEMENTS

by

MICHAEL LAWRENCE PORTER, JR.

APPROVED:

Robert S. Ehlers Jr., Ph.D.

Jeffrey D. Dailey, Ph.D.

James R. Phelps, Ph.D.

Manuel F. Zamora, Ph.D.

22 April 2014

APPROVED:

Dr. Susan E. Keith
Dean of the College of Graduate Studies

ACKNOWLEDGEMENTS

I would like to express the utmost gratitude to my advisor, Dr. Robert Ehlers. His dedication to teaching has helped me better understand the intelligence discipline and its relationship to national security policy, military strategy, and the domestic policy process. Without his guidance, mentorship, and expertise, this paper would not have been possible.

I would also like to thank the other members of my advisory committee, Dr. Jeff Dailey, Dr. James Phelps, and Dr. Manuel Zamora. Their comments and insights were invaluable to fully developing this topic and making my paper a success.

Special thanks to Mr. Gene Barlow, of the Office of the National Counterintelligence Executive, and representatives of the Federal Bureau of Investigation, for their assistance in understanding current Intelligence Community responses to Insider Threats. These insights provided me a better understanding of how policies are being incorporated in the real world and not just on paper.

I would also like to thank Dr. Chris Eddy, Dr. Steven Band, Chief Warrant Officer Jaime Turner, Mr. Craig Howe, and Mrs. Karen Amos for their support throughout the drafting of this thesis. Their guidance has helped me every step of the way and made me a better intelligence professional.

Most importantly, I would like to thank my wife Kelli and my daughters Kaylee and Mikalea. Without their steadfast love, encouragement, and commitment, I would not have been able to have finished this thesis.

ABSTRACT

In recent years, America has seen a rise in insider threat related incidents. Insider threats are individual with placement and access to critical infrastructures, military units, and the government and their supporting agencies who have turned against and targeted their parent organization aiding a foreign power or international terrorist organization. Understanding this, this paper analyzes how successful the United States Intelligence Community has been in responding to insider threats. For this thesis, literature will serve as a base for establishing doctrinal knowledge, with interviews, with current members of the IC working on insider threat issues, supplementing knowledge gaps about real world application. This paper has found that US policies in the past five years have made great advances in addressing insider threats problems, but there is room for improvement. These improvements will be difficult to adopt because of the impediments to reform, but are necessary to adequately counter insider threats.

TABLE OF CONTENTS

Page

List of Acronyms

CERT—Computer Emergency Response Team
CI—Counterintelligence
CIA—Central Intelligence Agency
DIA—Defense Intelligence Agency
DNI—Director of National Intelligence
EAP—Employee Assistance Programs
EO—Executive Order
FBI—Federal Bureau of Investigation
FISS—Foreign Intelligence Security Service
IC—Intelligence Community
ITAG—Insider Threat Advisory Group
ITO—International Terrorist Organization
LE—Law Enforcement
NCIC—National Counterintelligence Center
NCIS—Naval Criminal Investigative Service
NCIX—National Counterintelligence Executive
NIPF—National Intelligence Priorities Framework
NIS—National Intelligence Strategy
NTIPA—National Threat Identification and Prioritization Assessment
NITTF—National Insider Threat Task Force
ODNI—Officer of the Director of National Intelligence
OSI—Office of Special Investigations (Air Force)
PERSEREC—Defense Personnel and Security Research Center
SSCI—Senate Select Committee on Intelligence
USC—United States Code

Preface

When a portion of the population, no matter how incredibly small and seemingly insignificant, turns against its own, whether it be through violent acts or espionage, a largely invisible but very dangerous threat is present. The people who commit these crimes of betrayal are no different than the average person. They go to school, work, eat, and live in the same places their fellow citizens do, but their true loyalty is not to America, it is to the foreign powers that control them. This threat, which exists from within our own ranks, can kill indiscriminately and damage American national security severely and in various ways. However, it can be prevented, and there are ways to mitigate and prevent the threats posed by "insiders."

The United States has done a good job of adapting in recent years to the increase of these "insider threat" activities. However, the efforts to date are not enough, and the large importance stressed by the President shows the threat is not diminishing. We must make further improvements, including the fundamental ways in which we perceive, identify, and counter insider threats. This thesis will seek to answer one main question: How successful has the United States Intelligence Community (IC) been in responding to the increase of insider threats?

In order to answer this overarching question, we must first answer five sub-questions.

1. What is an insider threat?
2. Where do insider threats come from?

3. How have these threats impacted the Intelligence Community?
4. How will the different Insider Threat Groups increase the IC's ability to target insider threats?
5. What changes are still needed to best defend the United States?

Answering these questions is the best way to analyze the Intelligence Community's response because it breaks down insider threats, and IC responses, to their raw elements. Only once these ideas have been decomposed can they be built back up in a complete picture of all actions taken to counter this developing threat. By answering the first question (What is an insider threat?), the author will show that with as many organizations as there are in the IC's Counterintelligence Community there are as many different definitions of insider threats. Given that disparity the author will present the best definition possible to press forward with analysis of insider threats. The second question (Where do insider threats come from?) is designed to give analysis in how individuals who were once loyal to the United States can betray their country. This will be important to understand because the first part of understanding how to counter a threat is identifying where it came from. The third question (How have these threats impacted the Department of Defense and National Intelligence Agencies?), will establish the basic structure that the IC has been forced to develop to cope with insiders. This will help the reader to understand the dramatic impact that threats have on the development of policy and organizations within the IC. The fourth question (How have the different insider threat groups increased the IC's ability to target insider threats?) will highlight the recent changes that have been taken across the IC to enhance cooperation in the fight against insider threats. Finally the last question (What changes are still needed to help combat the insider threat?) will reveal the necessary steps that the author feels the IC should

take to repair weaknesses uncovered in the analysis of the systems revealed answering the first four questions. Each of the first four questions will attempt to develop the insider threat and the IC response while the final question is designed to assess what is still needed.

With such emphasis placed on insider threats by the President of the United States, the preservation and proper employment of a multitude of new research currently underway is vitally important to our national security. The findings of this thesis will build upon topics addressed by many different research initiatives and operational organizations to offer some new insights.

Of particular note, the Computer Emergency Response Team (CERT®) Program at Carnegie Mellon University has been chartered by the United States government to provide research, analysis, and recommendations of insider threat-related topics to the Office of the National Counterintelligence Executive (NCIX) and the Intelligence Community (IC) [1]. In addition to CERT®, the Department of Defense and the Defense Personnel Security Research Office have conducted studies relating to insider threat program analysis, threat prevention, and past threat assessments. This research will provide useful insight into case studies and proven problems and advantages of insider threat programs.

This paper will use many different types of sources to answer the proposed thesis questions. Current literature will be very important, and will be used to capture academic and

[1] The CERT® Program is a federally funded program that was established to conduct research, provide findings and recommendations, and facilitate communication among community experts regarding cyber security. It has, since its inception, been tasked with the additional mission, "*To enable effective insider threat programs by performing research, modeling, analysis, and outreach to define socio-technical best practices, so that organizations are better able to deter, detect, and respond to evolving Insider Threats.*" This change of mission has allowed them to become the government's leader on insider threat research. (The CERT Insider Threat Center, "Mission" http://www.cert.org/insider_threat/, 05 June 2012.)

theoretical understandings of insider threats throughout the analysis. However, literature alone cannot provide all the details for the effectiveness of policy. For this thesis, literature will serve as a good supplement to integrate interviews with current members of the IC working on insider threat issues. Such a vast range of sources is necessary because a true understanding of how the IC has identified and responded to the insider threat can only be garnered through a study of the written policies and real-world practices. Given the disparity that often exists in government between what is written on paper and what is practiced in application, interviews with IC officials will fill the gaps regarding what actually happens[2]. Discussions with these individuals will provide the best look into "real-world" practices versus the required practices on paper. Lastly, subject matter experts will also be able to provide some insights into those practices that have aided them in the field and could best become formal policy.

As with all studies in Intelligence, there will be some limitations to the depth of the research covered in this paper. The main limitation for this paper will center on the nature of the subject, counterintelligence, and the amount of available research. When discussing Counterintelligence, the availability of details and programs is often very obscure. The reason for this abstruse nature is because Counterintelligence organizations are established to protect America's secrets. Defense missions like this will generally restrict the amount of information publicly available so as to not compromise strategic visions and specific tactics.

[2] This author will be implementing qualitative research methods, to include contributions of relevant subject matter experts, such as the Co-Director of the Joint Insider Threat Task Force, a Community wide organization established by the President and tasked with enacting the National Insider Threat Policy, as well as representatives of the National Counterintelligence Executive's Office, and other members of the Counterintelligence Community some of who have been working in the CI field for in excess of 30 years. Counterintelligence Special Agent-in-training allows me access to individuals who have been working in the CI field for some in excess of 30 years.

Lastly, before beginning any analysis, this author, a Counterintelligence Special Agent, realizes that all people are susceptible to their own personal biases. Richards J. Heuer, a veteran of over 45 years in the CIA and author of *Psychology of Intelligence Analysis*, says that one's personal biases are the mental shortcuts that human beings take to help them come to the conclusions that they draw. Serving in the field, while having its benefits, also leaves this author susceptible to bias of analyzing his own parent organization. In additions to the author's bias as a CI agent, the application of research and interviews from SME's within the CI field will provide the potential for personal biases to be voiced rather than honest assessments. To avoid both of these biases, a substantial amount of literature, doctrine, and public policy will be referenced to provide a better technical understanding and to keep personal opinions out of the narrative. Understanding these biases and how the human mind operates will better allow the author to remain objective regarding the analysis within this paper, and to look for biases placed on given the presented ideas and policies. After all, the essence of good analysis is "how to make judgments and reach conclusions, not just about the judgments and conclusions themselves[3]."

This thesis is one that will focus on a threat that until recently has not been a chief priority of the IC. Wars in Iraq and Afghanistan have fixed intelligence officials on one theater of the world with a level of policy paralysis not seen since the Cold War[4]. As the United States withdraws from nearly thirteen years of fighting abroad and the IC begins the reorganization process, officials will soon realize that such an intense focus on the wars

[3] Heuer, Richards J. "Psychology of Intelligence Analysis." Center for the Study of Intelligence: Washington DC, Central Intelligence Agency, 1999.

[4] Policy paralysis refers to the fixation that US Intelligence has placed on current threats. Policy Paralysis leads the IC to remain fixed on one issue and miss all other developing or current threats.

overseas have left us vulnerable to the "wars" being fought on our home soil. This study will provide a new way of looking at threats that are very difficult to identify, how some very minor changes can greatly improve successes in preventing insiders from becoming threats, and how to build upon current proven success for greater community-wide successes in the future.

The reason that this is so important is because of the potential damage these types of insiders can cause. Nidal Hassan, the Fort Hood shooter and an insider threat, entered the Reverse Soldier Readiness Processing Center at Fort Hood, Texas and killed 13 American service members[5]. Bradley Manning, an Army Private with a Top Secret clearance and an insider threat, published over 700,000 classified documents to Wikileaks[6]. Which as Michelle Van Cleve, former head of U.S. counterintelligence under President George W. Bush, writes ultimately "had repercussions across the world, breaching confidences, embarrassing friends and allies, undermining US credibility, putting the lives of American soldiers and Afghan informants in danger and operations at risk[7]."

In summary, a myriad of research is beginning to be conducted on insider threats, but this threat is constantly evolving. Until the United States creates a way permanently to prevent insider threats, research will be needed to identify the latest developing trends and techniques to combat them. Failure to stay up to date with these threats is not an option as

---

[5] Joseph Lieberman. *A Ticking Time Bomb: Counterterrorism Lessons From The U.S. Government's Failure To Prevent The Fort Hood Attack.* U.S. Senate Committee on Homeland Security and Governmental Affairs, http://www.hsgac.senate.gov//imo/media/doc/Fort_Hood/FortHood Report.pdf?attempt=2, Washington D.C., February 2007, pg. 7.

[6] Included in these were Combat Strategies, State Department cables, and terrorism detainee assessments.

[7] Michelle Van Cleave, "Myth, Paradox & The Obligations Of Leadership: Edward Snowden, Bradley Manning and the Next Leak," Center for Security Policy, Occasional Paper Series. September 2013.

one mistake could be the difference between a foiled attack or the next Bradley Manning or Nadal Hassan.

Chapter 1: What is an Insider Threat?

Our planet is home to over 190 different countries, all with unique economic, political, and religious goals[8]. The one commonality among them all is a desire for self-preservation. No matter the size, big or small, all countries strive for continued existence and will do whatever they can to protect themselves from the many threats they face. Tactics employed by nations in the pursuit of political power have varied over time with the evolution in weapons, technology, and national interests. One tactic that has been prevalent throughout history, however, is the use of insiders, or insider threats[9].

The term "insider threat" is a buzzword; it is used to refer to a specific threat that the United States faces from its enemies. The term has been used in many different studies including those conducted by the CERT Program, the National Infrastructure Advisory Council, the White House, the Congressional Review Service, and the RAND Corporation[10]. Each of these studies gives a slightly different definition of an insider threat, and each has used that definition to fashion the arguments proposed in their studies. Of the many studies that have been conducted looking at insider threats, the National Infrastructure Advisory Council has one of the best definitions, which defines an insider threat as, "one or more individuals with the access and/or inside knowledge of a company, organization, or

[8] This number will differ depending on the constant change of the nation.

[9] One of the earliest accounts of an insider threat is from the Battle of Thermopylae in 480 BC when Ephialtes of Trachisas went to Xerxes and betrayed his fellow Greeks telling the Persian Army how to flank the Greek position, thus defeating the Spartan forces. (Terry Crowdy, *The Enemy Within A History Of Spies, Spymasters And Espionage*, (London: Osprey Publishing, 2014)).

[10] The CERT Program alters their definition of insider threats to focus more on the aspects of threats to Cyber Security and information systems. The White House, the Congressional Research Service, and RAND have very generic definitions that are lacking in specifics.

enterprise that would allow them to exploit the vulnerabilities of that entity's security systems, services, products, or facilities with the intent to cause harm[11]." While this is one of the best definitions, it does not quite sum up an insider threat; it is missing one essential element, a foreign nexus.

One important fact to keep in mind when defining an insider threat is who is responsible for combatting them. The answer is the Counterintelligence Community under the direction of the National Counterintelligence Executive, one of the offices in the Office for the Director of National Intelligence. As laid out in the President's 2009 National Counterintelligence Strategy, the CI Community is responsible for "detecting insider threats." By giving CI jurisdiction over insider threats, the Director of National Intelligence has essentially made them a CI issue, which means an insider threat must meet the qualifications of a Counterintelligence crime. Executive Order 12333 describes Counterintelligence as, "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities[12]." The essential elements of this definition are the crimes and the foreign nexus.

The foreign nexus is significant, because without that tie, these would not be CI crimes; they would be domestic crimes outside of the CI mission. This is a point that has been of contention in the United States Intelligence Community for several years when

[11] Thomas Noonan and Edmund Archuleta, "The Insider Threat to Critical Infrastructures." *The National Infrastructure Advisory Council Report.* April 2008.

[12] Ronald Reagan, "Executive Order 12333—US Federal Intelligence Activities." December 1981.

arguing who has jurisdiction over domestic terrorism. The important thing to note is that domestic terrorism "involves violence against the civilian population or infrastructure of a nation—often but not always by citizens of that nation and often with the intent to intimidate, coerce, or influence national policy[13]." This definition shows that in fact all violent insider threats are domestic terrorists; it does not however mean that all domestic terrorists are insider threats. This is important to clarify because one of the main missions of Counterintelligence is exploitation of our foreign enemies. A domestic terrorist without foreign ties offers nothing to Counterintelligence agents. So while the FBI is likely to handle both cases the methods that they use to investigate them will differ. Keeping this in mind can better help define exactly what an insider threat is.

For the purpose of this study, an insider threat is a traitor. These are individuals with placement and access to critical infrastructures, military units, and the government and their supporting agencies, who have turned against and targeted their parent organization aiding a foreign power or international terrorist organization[14]. This definition of insider threats explains why the CI community has adapted over the years to meet the coming challenges presented by insider threats. It also takes into account the necessary foreign nexus in addition

[13] RAND. "Domestic Terrorism." http://www.rand.org/topics/domestic-terrorism.html, 01 December 2013.

[14] Insiders can also target businesses and other areas of the economic sector, but this paper will look more to the traditional insider threats presented to the Counterintelligence Community rather than domestic law enforcement. Aiding a foreign power is used in US Code Title 18, Chapter 37- Espionage. Section 798- Disclosure of Classified Information. (Nicholas Catrantzos, "No Dark Corners: Defending Against Insider Threats to Critical Infrastructures" Naval Post-Graduate School, September 2009).

to the specific crimes that CI is responsible for investigating. Ultimately, these crimes are designed to harming our national security in several ways[15].

The harm inflicted by insider threats may take on various forms of crimes. There are insider threats that will commit acts of espionage, terrorist actions, or acts of economic and cyber sabotage. Ultimately, these are all insider threats, but for the Counterintelligence community, the chief concerns lie in the two main types of crimes—espionage/intelligence crimes and terrorist actions. These are the threats that the Counterintelligence community seeks to stamp out and from which they derive their principal mission, which is protecting the state and helping it to survive.

The survival instinct of states is what has led to some of the largest and most technologically advanced countries in history to search out and find their enemy's, and even closest friend's "secrets." The "secrets" of states are often the inner workings of their government, military, and industrial sectors. These can offer insights into the political and military technologies, strategies, and plans that help aid their competitiveness and survival. Acquiring this information provides states with advantages over their adversaries because it is what Sun Tzu says "enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men," and to "win without striking" It gives states what he calls foreknowledge[16]. This foreknowledge not only reveals to leaders how to array their defenses, when enemies might strike, or how they can defeat their enemy, even if outnumbered and outgunned, but it can also reveal how they might interact with other states

[15] Robert M. Bryant, "The National Counterintelligence Strategy of the United States of America." Office of the National Counterintelligence Executive, 2009.

[16] Sun Tzu, *The Art of War*, (Filiquarian, 2006) pg.65-68.

to best set themselves up for survival. In essence, foreknowledge gives leaders what they need to make the best decisions for their countries, What Sun Tzu calls foreknowledge, we call intelligence.

Intelligence is many things. It is the process through which we evaluate information. It is the product that we produce from analysis. And it is the organization that collects and analyzes the information[17]. Beyond all of that, intelligence is a tool. It gives decision makers the necessary information to make the best-informed decisions. Clausewitz refers to intelligence as the complete understanding of another nation's character, institutions, and state of affairs. This, he states, will help the policy maker understand and formulate an assessment of another country's most likely course of action[18]. When a nation's intelligence is uncovered by another country, suddenly the latter state's advantage is lost. And, assuming that country does not know about its loss, its enemy now has the advantage, for they understand the other nation's weaknesses and can change their strategies, move forces, and reallocate resources to get an edge on its blinded foe. How does this happen? How can one country get access to such closely guarded secrets? The oldest and most reliable method is betrayal by traitors.

Betrayal of one's own country by handing over intelligence, or spying, is not a new tactic. For as long as states have existed, they have spied on one another. It is part of human nature. In fact, Sun Tzu says the best way to acquire intelligence is "from the enemy himself,

[17] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*. (4th ed. Washington, DC: CQ Press, 2009), pg. 1.

[18] Carl von Clausewitz, *On War.* (ed. and trans. Michael Howard and Peter Paret, Princeton, NJ: Princeton University Press, 1976), Book 1, Chapter 6.

through spies"[19]. The reasons that individuals become spies vary and include ideological differences within their governments, religious ideals, and money, to name a few. Regardless of their reasons, states that take advantage of the disloyalty and other weaknesses of their enemy's countrymen can often find a wealth of intelligence that will assure continued survival as a state.

Spies, however, are not the only intelligence insiders; another type of intelligence insider is the "leaker." Individuals such as Bradley Manning, who release or leak national defense information and classified material, have a more obscure foreign nexus, but they are just as guilty of giving information to the enemy as those that hand it to them directly. Under United States Code Title 18, Chapter 37, Espionage, there are multiple Sections that discuss the crimes of espionage[20]. These crimes, while each addressing a different aspect of espionage, all convey that any individual who lawfully has "possession of, access to, control over, or is entrusted with information" which reasonable belief would suggest could be used "to the advantage of any foreign nation" has committed espionage[21]. By taking Defense information and publishing it on the internet, Bradley Manning was making information publicly available to Foreign Intelligence Security Service (FISS). So while he may not have

[19] Sun Tzu, pg. 65.

[20] Crimes falling under Title 18 Chapter 37, § 793. Gathering, transmitting or losing defense information; § 794. Gathering or delivering defense information to aid foreign government, § 795. Photographing and sketching defense installations, § 796. Use of aircraft for photographing defense installations, § 797. Publication and sale of photographs of defense installations, § 798. Disclosure of classified information, § 798A. Temporary extension of section 794, § 799. Violation of regulations of National Aeronautics and Space Administration

[21] Quotation is extracted from Section 793, Gathering transmitting or losing defense information, however the language used in Section 793 is very similar to the other sections of Chapter 37. "To the advantage of a foreign nation" is an expression used in all description of espionage crimes and is specific to no singular Section of Chapter 37. (United States Government Printing Office, "United States Code, Title 18, Chapter 37: Espionage and Censorship", December 2012).

met with a handler, there is reasonable belief that by his publishing that information, a foreign power could use the information to their benefit. This foreign nexus, while not as direct as spying, is what makes leakers just as much of an insider threat. Additionally, this type of insider is potentially more problematic than a spy because they can commit their acts of espionage while hiding behind the computer screen. This modern day technological shield acts as a protection for the insider and makes finding their identification very difficult.

Betrayals are not just related to stealing information. They often result in unexpected attacks. Antoine-Henri Jomini writes, "Advantage should be taken of all opportunities for surprising an adversary," because taking an enemy by surprise enables a force to attack before the other can "make preparations for an attack[22]." What better way to surprise one's enemy than to have a traitor willing to conduct that attack, or to provide critical information that facilitates a military, terrorist, or other strike?

Those willing to kill their own countrymen, like those willing to steal their country's secrets, are often driven by deep ideological differences with their own country, making them susceptible to the recruitment efforts of foreign powers. Clausewitz reminds us that "War is an act of force, and there is no logical limit to the application of that force[23]." By persuading the people within a country to attack their own, an enemy can create the many "minor incidents" that no leader can "really foresee to lower the general level of performance so that

[22] Antoine Henri Jomini, *The Art Of War*. (A new ed. Westport, Conn.: Greenwood Press, 1971), Chapter 6 Article XXXIV.

[23] Clausewitz, Book 1 Chapter 1 Section 3.

one always falls short of the intended goals[24]." The world is not comprised entirely of large states with comparable military capabilities. There are small states that would never be able to compete on a conventional scale. For them, attacks conducted by dissident insiders allow them to level the playing field. This sudden equalizer can bring the most powerful countries to their knees by targeting the homeland, which damages much more than infrastructure. It damages the very psyche and morale of the population.

Often, the psychological damage that is done can be more destructive than the actual physical damage. In the history of the United States no insider attack has yet achieved its stated objectives[25]. However, these attacks drive serious debates within the target country as to what current policies should be. A key problem is that such attacks give international terrorist organizations propaganda to further their cause. In a time of fourth- generation warfare, where international perception becomes paramount in effective foreign relations, the terrorist and other actions taken by insider threats give direct support to an enemy and make it appear even stronger than it is[26]. Ultimately, the enemy can exploit this perception to give them real advantages. This struggle against fourth-generation threats has led the United States to all corners of the globe searching out and killing the members of these parent terrorist organizations hoping to end the terrorist and insider threats to the United States.

---

[24] Clausewitz refers to these minor incidents as the "frictions" of war, or the things that leaders cannot anticipate, war in reality, that will prevent them from executing theirs plans and strategies, or the "war on paper." (Clausewitz, Book 1 Chapter 1 Section 7)

[25] Actual insider attacks such as the Little Rock Recruiting Station Shootings, Fort Hood Shooting, and Boston Marathon Bombing never accomplished their mission, but they have furthered support for international terrorist organizations and promoted their mission of fighting the United States.

[26] The modern era of warfare, in which battle lines are blurred and there is little difference between a civilian and a military target. Terrorism is one of the main tactics used and hence insider threats the ultimate attack mechanism. (William Lind et al., "The Changing Face of War: Into the Fourth Generation" *Marine Corps Gazette*. October 1989).

Unfortunately, much of the US effort has been devoted to fighting threats abroad, while domestic ones fall to the wayside. Throughout the past 75 years, the United States government has become preoccupied with a single kind of warfare however, the world is not such a black and white place, and most of our enemies will not fight a conventional, symmetric war with the United States. At any given time the threats that are present to a nation are vast, leaving US policy directed at one fight lacking on other fronts. During World War II, the preoccupation of US policy makers became so wrapped up with the fight against Fascism that the government for the large part missed the many deep penetrations the Soviet Union had made in the United States government[27]. Five years later, once the fighting had quelled and the United States moved out of a state of "hot war" in Europe, the government quickly discovered the many Soviet penetrations and the US as the Cold War began. This conflict lasted for over forty years and resulted in a sort of policy paralysis that caused the United States to miss the rise of terrorism and violent Islamic extremists as well as insider threats. Finally in the years preceding September 2001, policy again went "hot" with the fight against radical Islamic terrorists. What has been missed since then? Jennifer Sims, professor at John Hopkins University, thinks we have fallen victim to insider threats because our preoccupation with Muslim extremist groups (another form of policy paralysis) has left us open and vulnerable. She believes while we have been away fighting our wars, the Chinese and others have made massive gains by exploiting and exporting our military and economic secrets, often with the help of insiders. This trend needs to come to an end, and as the United

[27] During World War II Soviet spies penetrated upper levels at the State Dept. (Alger Hiss), the Manhattan Project (Klaus Fuchs and the Rosenburgs), and even the Executive Office (Lauchlin Currie, Executive Assistant to President Roosevelt) (Christopher Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*, (Basic Books: 1999)).

States looks to pull back its troop presence in the Middle East, policymakers must once again set their sights on what they have missed[28].

[28] Jennifer Sims and Burton Gerber, *Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence,* (Georgetown University Press: 2008), pg. 3-4.

Chapter 2: The Origin of Insider Threats

There are many different reasons why people become insider threats. Often, it is because of a disenchantment with the government. In other cases, it is because they become trapped in (or even blackmailed into) a series of bad decisions and see traitorous activity as the only way out[29]. Whatever reasons people have for betraying their country, understanding why once good citizens go down these alternate paths is important to determining how to counter them. In fact, the ideal situation would be to reach these individuals before they begin the path toward betrayal[30].

Although there are several explanations for the changes in psyche of the insider threat, there are two distinct models for understanding insider threat psychology, the Spy Lifecycle and the Radicalization Model[31]. These are good starting points for describing the shift in the thought process that leads loyal human beings to become attackers and spies. The most important aspect of these models, and something that is necessary to understand them, is how they define insider threat psychology.

It is human nature to have predispositions. These are our personal habits that may make us susceptible to negative influences. In the case of insider threats, these influences may be Foreign Intelligence and Security Services (FISS) and International Terrorist

[29] Some additional reasons are personal greed, exacting revenge, coercion and compromise, ego and excitement, and many more. One important note, approximately 65 percent of all insiders come from within the native born population, leaving 35 percent as naturalized citizens.

[30] This will be one of the key recommendations for Chapter 4.

[31] The Radicalization Model is used to show the Radicalization Process and the turning of a violent insider. The Spy Lifecycle shows the process that is taken by Foreign Intelligence and Security Services (FISS) to turn an intelligence insider.

Organizations (ITO). The goal of these groups is to discover character flaws in people of potential interest and exploit them. In identifying a potential insider threat, FISS and ITO search for people with the right predispositions and enough weaknesses or outright problems to make them vulnerable. These vulnerabilities can help our enemies to harness any political uncertainty, organizational dissent, dual loyalty, or character flaws to manipulate their target[32]. These flaws may be very obvious or not, but what everyone should be aware of is that there are a series of associated indicators that may reveal dispositions. The major predispositions can be broken down into four areas: loyalties and ties, social and professional problems, financial problems, and mental health disorders[33].

Loyalties and ties refer to more than people placing their hands on their heart and saying the pledge of allegiance. Loyalties and ties refer to whom or what they owe their loyalty, to what degree they believe in their country and its government, and what can test or even break their loyalty. Since 1990, insider espionage threats have indicated that over 58 percent of insider spies had foreign relatives and friends overseas and 50 percent had foreign

[32] Richard J. Heuer, "The Insider Espionage Threat", Research on Mitigating the Insider Threats to Information Systems, RAND Corporation, Monterey, CA: Defense Personnel Security Research Center, 2000.

[33] The current way of looking at insider threats is as a series of indicators that may show if a person is a potential insider threat, but there are no means of associating the indicators. By breaking down the indicators and giving them a larger predisposition, I am illuminating the main problem. Coworkers may not feel that their colleague is committing espionage, but they may realize he has work problems. Helping get past the initial denial of "They would never do that" can help others to realize just what actual issues might be at stake and may help prevent problems from developing into insider threats. This idea will be discussed about more in depth in Chapter 4.

professional connections[34]. This illustrates just how vulnerable those individuals were to influence and exploitation by our adversaries.

One of the most easily exploitable weaknesses is a person's loyalties. Everybody is born into a family, tribe, state, or country, with each of these different groups giving a person their individual identity. Often, people are born with a loyalty to many of those groups at the same time. In such cases, people are said to have dual loyalties. Dual loyalties are not uncommon and many people have them[35]. The exploitable weakness here occurs when FISS and ITO challenge these dual loyalties and split a person's allegiances. The split of an insider threat's loyalties leaves them owing allegiance to another state, group, or country. It is this "divided loyalty" that leaves insiders willing to harm their fellow citizens[36]. Divided loyalties are a real problem and account for 57 percent of all insider espionage threats[37]. As for violent insider threats, anyone that would conduct an attack in the name of an ITO displays symptoms of a divided loyalty, perhaps not for another country, but to the ITO.

It is extremely difficult to identify someone with divided loyalties due to the often-secretive nature of the division, or the inability to decipher a divided and dual loyalty. Some of the best indicators of potential divided loyalties include subversive language, expressed desire to harm fellow citizens, sending money and support overseas, and advocating loyalty

[34] Katherine L. Herbig, "Changes in Espionage by Americans: 1947-2007", Defense Personal Security Research Center, Technical Report 08-05, March 2008.

[35] Herbig, Changes in Espionage.

[36] Heuer, The Insider Espionage Threat.

[37] Herbig, Changes in Espionage.

to a foreign interest[38]. While on paper these may seem ease to identify, they are difficult to see. The difficulty in identifying these indicators is what makes the second part of this predisposition so important. Cultural ties play a vital role in identifying what a person's true loyalties are.

As previously stated, it may not be easy to identify someone's loyalties at first glance. Keeping that in mind, individuals with foreign and cultural ties may be susceptible to FISS and ITO exploitation. Indicators of foreign and cultural ties include foreign friends and family, foreign assets, sudden religious conversion, donations overseas, and regular and unreported foreign travel[39]. The reason that these indicators could be signs of an insider threat is because they show ties to an outside country or ITO. These ties, which for many are innocuous, are to the insiders the crucial connection to the foreign nexus that drives their operations[40].

When one considers how an insider threat must have a foreign nexus, identifying foreign connections becomes paramount. For spies, foreign connections are difficult to identify because of the training they may have received. Additionally, often the only connection that they may have is a single "handler"[41]. Often, the support network that violent insiders have is nothing more than email correspondence overseas, and violent literature, like Inspire the official magazine of al-Qaeda, for violent extremists. Nidal Hassan, the Fort Hood

[38] Department of the Army. *Threat Awareness and Reporting Program*, (AR 381-12), October 2010.

[39] Department of the Navy. "Espionage Indicators." NCIS Publications, March 2013.

[40] Department of the Army. AR 381-12.

[41] The liaison person between a spy and the foreign country they work for is known as the handler.

shooter, relied on email communications with Anwar Al-Awlaki, the operations head of Al-Qaeda in the Arabian Peninsula, for "guidance" before his attack[42]. At other times, communication can occur through individuals and spiritual leaders in the United States with connections overseas. Ryan Anderson, the Inland Island Jihad plotter, and the New York Synagogue plotter, James Cromitie, relied primarily on contacts they believed to be associated with ITOs[43]. Lastly, the support may be direct as with the cases of Faisal Shahzad, the failed Times Square bomber, and groups like the Lackawanna Six, in which the would-be attackers actually traveled overseas to Pakistan and Afghanistan where they were trained in terrorist tactics in hopes of attacking the US upon their return. No matter what the connections are, it often will be very difficult to see the foreign connections that some individuals have, which is why understanding the other predispositions is crucial.

Poor decision-making ability, the second major predisposition, reveals the common exploitable weaknesses found in the decisions people make in everyday life. The decisions people make are what define how a person lives his or her life. Poor decision-making can

[42] CICENTRE, "DOMESTIC TERRORISM CASE: Nidal Malik Hasan", http://www. cicentre.com/?HASAN_Nidal,15 February 2014.

[43] Ryan Anderson attempted to give secrets to AQ on how to destroy American tanks and "kill American soldiers." (CICENTRE. "DOMESTIC TERRORISM/ESPIONAGE CASE: Ryan Anderson", http://www.ci centre.com/?page=ANDERSON_Ryan, 15 February 2014). The Island Jihad Plotters were a group of individuals from California who attempted to reach out to AQ and Taliban before scheduling to travel to Afghanistan to conduct Jihad (CI CENTRE, "DOMESTIC TERRORISM CASE: Inland Empire Jihad Plot",

http://www. cicentre.com/?Inland_Empire, 15 February 2014). James Cromitie believed he was communicating with terrorists in Afghanistan who would help him attack Americans at synagogues in the Bronx (CICENTRE, "DOMESTIC TERRORISM CASE: James Cromitie", http://www.cicentre.com/? CROMITIE_James, 15 February 2014). All three of these cases were failures because the "AQ" representatives were actually FBI agents.

often result in both social and professional problems. Together, these illustrate the effects of poor decision-making and help us to understand how some people become insider threats[44].

Social problems can hinder people in making good decisions in their personal lives, specifically outside of the office and away from work. A few examples of common social problems and indicators associated with insider threats are gambling, drug and alcohol abuse, and adultery[45]. The reason that these behaviors can be indicators of espionage is because they leave the individual vulnerable. As with any bad behavior, there are always consequences. People who lack the ability to make wise decisions leave themselves open to the efforts of FISS and ITOs who may try to blackmail them based on the knowledge of their bad decisions. In an effort to protect themselves, some people may become vulnerable to recruitment. Also, social problems are an indicator that people may have internal conflicts in their lives that lead them to make these decisions. Drugs and alcohol, which are well-known coping mechanisms, may be what the person needs to deal with the stress of living a double life[46]. Lastly, these social problems often result in debt.[47] The need for money may be what the person needs to agree to engage in active spying or attacks[48].

Professional problems are those that involve decisions and actions made in people's professional lives, while working. There are two main types of professional problems:

---

[44] Steven R Band, Dawn Cappelli, Lynn F. Fischer, Andrew P. Moore, Eric D. Shaw, and Randall F. Trzeciak "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis" CERT Program, December 2006.

[45] Department of the Army 381-12.

[46] The Spy Lifecycle shows how insiders may feel lost, isolated, and alone which leads them feeling inadequate. For some people, the only way to deal with these feelings is through alcohol and drugs.

[47] Herbig, Changes in Espionage

[48] Discussed more in depth later on in Chapter 2.

unprofessional behavior and breaches in security. Together, they demonstrate common issues that are exhibited in the workplace, where, due to the nature of the threat, a large percentage of insiders are actively operating[49].

Unprofessional behavior shows the value that people place in their work and the poor decisions they make when interacting with others. The insider-threat indicators associated with unprofessional behaviors include fighting with coworkers and expressed violent intent[50]. Those who fight coworkers and express violent intent show clearly that they do not fear harming others and they maintain negative animosities towards their work. It is this disgruntled attitude that FISS and ITOs can seize upon as a motive to swing potential insiders. Statistically, this is a huge problem since 97% of insider threats came to the attention of their supervisors because employees displayed symptoms of unprofessional behaviors; 58% indicated intent to cause harm and 20% directly threatened to harm others[51]. The good news is that with such a common indicator, this should provide one of the better tools for understanding and identifying threats.

Lastly, operational security violations are important because 100 percent of insiders commit security violations. Whether it is soliciting information from others, attempting to gain access to information outside of their need-to-know, or copying and stealing classified information, all insiders commit security violations[52]. Someone who routinely violates

[49] Herbig, Changes in Espionage.

[50] Department of the Army 381-12.

[51] Band, Comparing Insider IT.

[52] Department of the Army 381-12.

security protocols may become the perfect target for those looking to get past security measures when targeting America[53].

The third major predisposition is financial problems. During the Cold War, spying for money was the most common reason for espionage, but that is no longer true today. In the past 20 years, the number of people spying for money has dropped to approximately 7%. Money often is considered a contributing factor, but since 2000, there have only been a few cases where it was the sole reason for someone's betrayal[54].

Money can be a problem because of how it seemingly makes the world go around. As was already discussed, poor decision-making can result in FISS and ITO offering to pay off debts, however, there are other reasons someone could be monetarily motivated. Some people with large credit card debts may be looking for some way to get free of debt. Other individuals simply want to have a lifestyle that is beyond their means and will do anything to get it. Monetary indicators of insider threats include paying off substantial debt and living beyond one's means[55]. These could be signs of repayment for insider action. Whatever the reason, money will always remain a motive to some degree.

The last area is mental health. This is much rarer than the other two predispositions but is just as important. According to the Defense Personnel and Security Research Center (PERSEREC) study in 2008, of the then 11 cases of insider threats since September 11, 2001, four involved cases in which the subject exhibited mental health problems. Such a weakness

[53] Band, Comparing Insider IT.

[54] Ibid.

[55] Department of the Army 381-12

is definitely a contributing factor to how FISS and ITO recruit insiders[56]. Those with access to information who have mental health problems could be turned against their country either wittingly or unwittingly with very little say otherwise.

The important thing to realize about predispositions is that everyone has them; human beings are not without fault. The mere presence of negative indicators does not necessarily mean that someone is an insider threat. What it does mean, though, is that while these ties alone may not be indicators, the negative behavior could develop into the slight hold that FISS and ITO's need to develop an insider. The ways in which these weaknesses are exploited are what make up the Spy Lifecycle and the Radicalization Model. As stated previously, these models are the potential paths that people can go down that lead to their development as insiders.

The Radicalization Model depicts the development that violent insider threats go through on their pathway to violent attacks. The Spy Lifecycle model displays the common thought processes that spies go through before deciding to hand over America's secrets. These two models serve as excellent guides for explaining the psychology of their piece of the insider threat, and together they show many similarities that can lead to better understanding of both spies and violent attackers.

The Radicalization Model is that of the violent extremist. This model shows the thought process and the step-by-step contortion of thought that occurs in those who go from being a normal person to disgruntled insider to violent killer. This model was first "created" by an independent study in the New York Police Department. Prior to that, the Radicalization

[56] Band, Comparing Insider IT.

Model was merely a loosely grouped set of indicators that suggested terrorist activity. The NYPD identified the psychological path that extremist Muslims take. This study was based on case studies of past terrorists. While considered to be the definitive "process of radicalization," it looks strictly at radicalization from the standpoint of Takfiri Muslims[57]. This paper will look at the Radicalization Model a little differently and incorporate multiple views of it, tying in additional insights from those who do not necessarily agree with it[58]. One key distinction to make is that radicalization is not limited to Muslims alone. This paper will break the model down into four phases: Pre-Radicalization, Indoctrination, Planning, and Action.

During the Pre-Radicalization phase, the future insider threat is living a normal life. They usually have "ordinary jobs" and live normal lives. During this phase of their life, they will go to school, have families, and perhaps go to church. Their life is no different than many of those in the world today[59].

The second phase, identification, usually involves the first signs of stress. This is where the individual begins to feel the pressures of the outside world more clearly. Perhaps there are people at work who harass him daily, or perhaps the reforms of the government go

[57] Mitchell D. Silber and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, New York City: NYPD Intelligence Division, 2007.

[58] The NYPD Report on Radicalization addresses radicalization following "Salafist" Muslims, however al-Qaeda (the reports intended model) is a follower of the Takfiri ideas. Takfiri Muslims split away from the Salafist ideas becoming more radicalized than their offshoot sister organization in the late 1990's. (Bruce Livesey, "The Salifist Movement," Frontline, PBS. http://www.pbs.org/wgbh/pages/frontline/shows/front /special/sala.html.)

[59] Ibid.

against his religious convictions[60]. These triggers make the individual begin to feel dissent[61]. This dissent starts out small, perhaps as a simple disagreement or upset, but it grows. Soon, these disinterested individuals feel like they need someone that understands them. All too often, the people left to fill these shoes are members of ITOs. Leaders in these groups now begin to take the often young and malleable minds of their targets and lead them into thinking that if they killed just a few people, the government would see how wrong its policies are regarding a given issue[62]. Once the individual has reached out to others, the grooming is furthered, and the ITOs continue to mold and shape his picture of reality. Their reality is shaped by "cliques" which "define a certain social reality for the ever more intimate friends, and facilitates the development of a shared collective social identity and strong emotional feelings for the group[63]." The end of this phase is marked by the complete transference of thought from the possibility that some people should die to efforts to get the disaffected person to conduct an attack. The most important part of this phase involves the signs explored in the first part of this chapter. Due to the emergent nature of these extremist beliefs, the individual will show the most indicators including, but not limited to, expressing

[60] Tomas Precht, "Home Grown Terrorism and Islamist Radicalization in Europe", Danish Ministry of Justice, Dec. 2007.

[61] Additional triggers: Economic (loss of a job, blocked mobility), Social (alienation, discrimination, racism), Political (global conflict), personal (death in family).

[62] Silber & Bhatt, Radicalization.

[63] Daveed Gartenstein-Ross and Laura Grossman, *Homegrown Terrorists in the U.S. and U.K.*, FDD Center for Terrorism and Research, April 2009. (Quote from Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century* (Philadelphia: University of Pennsylvania Press, 2008)).

hatred towards American society and culture, advocating support for ITOs, advocating violence to achieve goals, or communicating with and funding extremist organizations[64].

The third phase, indoctrination, is the planning phase. During this phase of Radicalization, the insider is beginning to purchase the necessary items for conducting the attack. At this point, he has already decided that he is going to kill Americans. All he needs are the supplies and the location. During this phase, there are fewer indicators visible to the outside. Some will be plain to see, including buying weapons, buying bomb-making materials, traveling to a training camp, target selection and reconnaissance, and final construction of a bomb[65].

The fourth and final stage is the action phase. During this phase, the insider finally launches an attack. By the time the insider has made it to this phase of the cycle, the hope of preventing the attack is very limited and the only indicator left is the attack itself.

Together these four steps take a seemingly normal individual and transform him into a homegrown terrorist. The process is slow and often does not happen overnight, but that is one of the things that makes identification so difficult. Each of the steps along the way has several indicators during which outside forces can attempt to change the course of that individual's life. If those steps are not altered, then it is a victory for the enemy.

The second model that breaks down the psychology of the insider threat is the Spy Lifecycle. This model shows that there are commonalities between the different thought

[64] Department of the Army 381-12.

[65] Precht, Homegrown.

processes that many spies go thru before deciding to hand over their secrets. The complete Spy Lifecycle, as created by Dr. David Charney, was developed through an in-depth investigation of case studies and psychological interviews with convicted spies. The model itself follows the life of a spy from his pre-spying days thru the "brooding in jail" phase[66]. This paper will only look at the phases up to active spying because that is what helps develop the psychological mindset of the insider spy. These thought processes are just as twisted as those of the Radicalization Model and the results can be just as deadly.

The first phase of the Spy Lifecycle is the sensitizing stage. During this phase, the future insider spy is growing up. The insider will live a seemingly normal life, but usually there are influences that will mentally scar him, perhaps an absentee or abusive parent, maybe a failed love life, or even a troubled childhood as the son of immigrants. For most, these influences will be simply a memory; for the insider spy they often play a much deeper role in defining who they are and remain on their mind forever[67]. Typically, the only indicators that would manifest themselves at this point are individual flaws and weaknesses.

The second stage, the stress and spiral stage, is characterized by more life challenges. The challenges experienced in this phase are not the same as the ones the person experienced growing up. Perhaps the insider loses a child or spouse during birth, maybe his spouse is cheating on him, or maybe he even begins to have problems with people in the office based on race or ethnic background. Regardless, the effects of this stage will stress the insider to the

[66] David L Charney, "True Psychology of the Insider Spy: Insights on the Profession", *Intelligence Journal of the U.S. Intelligence Studies*, Fall/Winter 2010.

[67] Ibid.

highest degree[68]. This phase is marked by a change in behavior of the insider. Like the first phase, the only indicators that would manifest themselves at this point are the individual's character flaws and weaknesses.

The third phase, known as the crisis and resolution phase, occurs when the insider just cannot take the stress anymore. The external problems of life are affecting his work and family life; perhaps he is getting negative reviews at work and maybe his wife has left him. The stress felt at this point is at its worst. Many people turn to alcohol and drugs to cope with the problems, but this leads to discipline problems at work. Full of upset and anger, the insider begins to pass blame for his problems to the organization where he works. He begins to think about how he might get "payback." Slowly, during this phase, it becomes evident that the insider is changing. The insider will look for acceptance and support wherever he can find it. Perhaps he finds a group of people from the land of his parents who offer to help him out. It is the last part of this phase when he decides maybe he can alleviate his problems by spying that he will spy for money and with enough money everything will be alright[69]. This phase is characterized by serious personal and professional problems in the life of the insider. These problems may not always be visible since many individuals are good at compartmentalizing their lives so that they do not outwardly show their true emotions. This might be when the decision-making problems, both social and professional, manifest themselves most clearly with a possible a turn to drugs and alcohol[70].

[68] Ibid.

[69] Ibid.

[70] Ibid.

The final stage that this paper will look at is the post-recruitment (or volunteer) phase. The Spy Lifecycle does not end there; it actually consists of six more phases that cover regrets, denial, dormancy, acceptance of fate, arrest, and jail time. These phases though do not add anything of value to the understanding of the insider spy and his earliest thought process. During this fourth phase of the cycle, the insider spy is actively conducting his espionage. The money is coming in and the information is flowing. During this phase, the most significant indicators of espionage will be visible because the spy is actively conducting espionage[71]. This phase will often be characterized by new foreign contacts and travel, disregard for security, unusual work behavior and undue interest in sensitive or classified projects, and financial relief and living beyond one's means. These common indicators of espionage will most likely be visible, although identifying them now only helps to catch the active spy, not prevent the damage he does to national security[72].

These models each show a twisted pathway that leads to betrayal, but the most important thing to note is the similarities that exist between the models. While models attempt to take data and find a common ground, as pointed out in NAIC's report, models do not show a guaranteed path. Nonetheless, it is important to look at the "models" because while 9 times out of 10 the person that exhibits these habits will not develop into an insider threat, there is the potential. What this chapter has shown thus far is that there are many different behavioral weaknesses that leave individuals susceptible to exploitation by FISS and ITOs. The exploitation of these individuals can lead them down a pathway towards betrayal. Once someone is on this path, it does not mean they will become an insider. There

[71] Ibid.

[72] Department of the Army 381-12.

is still time for intervention. The further down the path they go, the less intervention is possible, and the less influence it will have.

Together, each of these models provides a good insight as to how insiders betray, but what do they have in common? The answer, remarkably, is that they have a great deal in common. The crimes may be different, but the psychological thought processes are very similar.

The first commonality is that during the first stage of both models the insider lives a seemingly normal life. There are ups and downs, but nothing is too far out of the ordinary. The spy may have additional stressors early in life, but otherwise the early stages are quite similar. This first stage simply underscores that as similar as the two types of potential insiders are at this point, they are not much different than the rest of people in their society. What really sets them apart is how they handle their problems. During the second stage of both models, we begin to see the indicators that point towards a shift in psychology. The stresses on the individual increase, and in the radicalization model, at least, the perceived or real persecution is just too much and the thought process goes from "I dislike the people" to "I want to work with others to hurt them." This is the same as the thought process for the spy in the third stage, where the answer to his problems seems to be in the infliction of damage to those that he once called his countrymen. The final similarity is that for the Radicalization Model, the third and fourth phases are about prepping for the attack and attacking. Phase four for the spy is when all the activity occurs.

All the models are very similar and they cast a new way of analyzing insider threats. They are not scientific and they are not fact. What they are is an attempt to explain a strange

and unknown psychology. Understanding why insiders become insiders is critical because the psychology of their behavior is what helps those who study them to understand the threat[73]. Without understanding the threat, there is no way that one can hope to defeat it. The great advances in the last 13 years, since September 11, 2001, show just how much the Intelligence Community has applied its collective efforts to understanding the insider threat. This new understanding of basic psychology indicates that the IC is adapting well to the changing threats. The only thing left to do now is to begin incorporating this understanding into regular training and defense mechanisms.

[73] Thomas Noonan and Edmund Archuleta, "Insider Threat to Critical Infrastructure", *The National Infrastructure Advisory Council Final Report and Recommendations*, April 2008.

Chapter 3: The Current CI Community and Approaches to Insider Threats

A threat as atypical as that posed by an insider presents a certain challenge for any defense plan. Ultimately, insider threats find their roots in spying and sabotage, two activities already addressed as being as old as organized states and best handled by Counterintelligence. Defeating these two types of attacks has required a special plan, organized and designed to target threats from the strategic, operational, and tactical levels[74].

The terms strategic, operational, and tactical are words primarily used to describe levels of decision making in the military during war. Given the ongoing fight against insiders, and the danger posed by them, military terms in this sense are appropriate to define the "battle plans" necessary for the fight. The strategic level resides at the national level where policymakers make decisions that affect long-term national goals and strategies. This would be where strategy is crafted and where battle plans are developed for all of the different threats that the people and their government face. The operational level refers to different "theaters of war" for the fight and the different organizations that operate in each. At this level, different organizations have specific goals driven by the larger strategy in the fight against the common threat. Finally, there is the tactical level, where the CI "engagements" and "battles" are fought. At this level, individual "combatants" such as field

[74] This chapter will identify the three distinct levels of decision making, but the majority of emphasis will be on analysis of the strategic level. While the operational and tactical level is where the detective work and active protection methods like routine background checks, psychological testing, interviews, work history reviews, and financial reporting occur, the strategic level is where the high level policies are developed. Additionally, this paper will focus on the strategic level because of the vast number of agencies and differing priorities at the operational and tactical levels, which make a thorough analysis impossible within the scope of this work.

agents and analysts do their part to produce success in the larger struggle[75]. Using this framework, the United States has responded to the insider threat in much the same way that the US government responds to other threats.

At the strategic level, insider threats are under the purview of the Intelligence Community (IC)[76]. More specifically, when it comes to solving problems, often the best method is to target those enemies who, according to intelligence sources, would target us. That is what Counterintelligence seeks to do. Agents seek to exploit the weaknesses of those who target them to gain knowledge on the very mechanisms that their enemies are hoping to use to harm Americans. Once this objective has been met, CI is left to exploit its captured and compromised sources for actionable intelligence. This type of operation does many things for the Intelligence Community. It not only stops the threat, but it exploits the extensive network setup to support the insider and it gets inside the enemy's state of mind to illuminate how he thinks and operates, what his tools are, and what his weaknesses are[77]. As previously stated, the IC is tasked with collecting, analyzing, and producing intelligence, but

[75] USAF College of Aerospace Doctrine, Research, and Education. "Three Levels of War." *Air and Space Power Mentoring Guide*, (Vol. 1, Maxwell AFB, AL: Air University Press, 1997).

[76] The IC is composed of 17 different agencies whose duty it is to collect, analyze, and distribute intelligence products to policymakers in Washington. In charge of the IC is the Director of National Intelligence (DNI). The DNI is primarily responsible for directing the actions of the Community and ensuring a unity of effort. The IC operates in a system following a basic cycle. The easiest way to interpret the Intelligence Cycle is to look at it as a loop in which information enters the system, moves through the cycle, and eventually releases new information, starting the loop over again. Kent argues that the intelligence process is a cycle in which intelligence, as a product, is consumed by policymakers, who give feedback to the Intelligence Community for future collection and direction. While this is a very simplified definition, it captures the essential elements of the process. The very nature of the feedback loop implies that guidance is given in the beginning, and again at the end to keep the cycle going. Since the mission of the IC is to provide intelligence for the policy maker, it is the policy community's role to provide the guidance on where to collect intelligence. In the case of the Insider Threat, the threat has always been present, but often policy has been more focused on other threats. (Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, (4th ed., CQ Press, Washington DC 2009)).

[77] Office of the National Counterintelligence Executive. "What is Counterintelligence?" http://www.ncix.gov/ about/ about.php, 01 March 2014.

CI is responsible for a very special aspect, the enemy's perspective. For CI, the idea that the best defense is a good offense against insider threats reigns supreme. In this sense, the key is exploitation. By exploiting insider threats, we can begin to establish what FISS and ITO structures look like in the United States, which ultimately supports the end goal of force protection, and stopping the insider threat. For instance, had we understood fully the connection between Anwar Awlaki and Nidal Hassan prior to the Fort Hood shooting, what are the chances the Texas massacre could have been prevented[78]? That is what the mission is about—protection—and it has evolved through the years to make Counterintelligence what it is today.

At the strategic level, the National Counterintelligence Executive (NCIX) is tasked with providing leadership, prioritization, and guidance of the IC's CI organizations. This guidance extends to all matters of CI from operations to collections[79]. Each of the agencies in the IC and CI Community has an important part to play in countering the insider threat, but the CI Community as a whole is what establishes the common operating picture and provides a unity of effort when it comes to countering the insider threat at the operational and tactical levels.

At the operational level within the Intelligence Community, there are nearly a dozen different organizations that conduct Counterintelligence. The United States Army has US Army Counterintelligence, the Navy has the Naval Criminal Investigative Service (NCIS),

[78] William H Webster, "Final Report of the William H Webster Commission on the Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas, on November 5, 2009." Federal Bureau of Investigation Press Releases. 19 July 2012.

[79] Office of the National Counterintelligence Executive. "About the NCIX: Our Mission". http://www.ncix.gov/ about/ about.php, 01 March 2014.

the Air Force has the Office of Special Investigations (OSI), and there are even CI elements in the Departments of State, Energy, and Justice. This vast array of Counterintelligence bodies means that there are many different entities each led by different parent organizations, and each with different priorities. Providing the unity of effort to lead these groups is a struggle for the NCIX and one that often conflicts with higher-level goals. The reason for these difficulties is that each of the different organizations in the Counterintelligence Community has a specific goal and purpose. Two examples of these differences are the Department of State and the Department of Energy. In the State Department, counterintelligence agents are worried about threats to diplomatic missions[80]. Meanwhile, in the Department of Energy, agents are focused on the threat to Nuclear Technology[81]. Each agency is concerned with its own most-serious insider threats and has long had systems in place to counter the insider threat as its analysts see them.

Finally, at the tactical level, individual agents for the different organizations are on the streets daily, confronting the threat, and catching the "bad guys." This final level, however, is not just agents. It also includes the general public. Due to the threat posed by insiders, the person best suited to catch insider threats before or during their acts is the person sitting to their right or left, their friends, coworkers, or neighbors. Because an insider by definition is no different in appearance than any other person, a knowledge and understanding of the threats, by the general population, is very important. Countering this

[80] United States Department of State, "Counterintelligence Investigations", http:// www.state.gov/m/ds/ terrorism/c8653.htm, 10 March 2014.

[81] United States Department of Energy, "Office of Intelligence and Counterintelligence," http://energy.gov/ office-intelligence-and-counterintelligence, 10 March 2014.

threat is not one where the agents can do all of the work. Every person must do his or her part to help.

Assigning Counterintelligence assets the primary responsibility for countering insider threats, as the 2009 National Strategy did, focuses their collection, analysis, and dissemination efforts against those targets that seek to exploit America's weaknesses[82]. Understanding this mission and its importance, the CI Community has adapted substantially over the years to meet the evolving threats. The current CI Community is largely reflective of the necessity for organization and standardization when it comes to handling insider threats. The changes of the past 20 years are some of the most important in the fight against insider threats and are what define the current CI Community's structure and strategy.

In 1994, the first extensive reforms to the Counterintelligence Community came about in response to the arrest and subsequent conviction of Aldrich Ames of espionage. Ames was convicted in 1994 of having spied for the Soviet Union for nearly nine years. Considered the deadliest spy in American history, Ames handed over 25 American spies, two of the most productive collections programs, and nearly 100 other operations that were the crown jewels of the American intelligence effort against the Soviet Union during the Cold War[83]. The reason that Ames got away with spying was not because he was a great spy. Ames was, in fact, quite the opposite. The reason that Ames got away with it was because the Counterintelligence system had shortcomings. These problems, identified in great detail by

[82] The Counterintelligence Community does this because of the opportunities that CI has above and beyond a law-enforcement-only strategy. Inherently, the mission of CI is different than that of traditional law enforcement, or even traditional intelligence collection, which gives CI agents a unique perspective when it comes to countering threats.

[83] Pete Earley, *Confessions of a Spy: The Real Story of Aldrich Ames*, (New York: G.P. Putnam's Sons, 1997).

the Senate Select Committee for Intelligence, brought to light systemic errors in how CI in the CIA and FBI shared information, conducted investigations, and cooperated when it came to handling potential insiders[84]. Additionally, lackadaisical security practices at the operational level allowed Ames to commit what the Senate Select Committee on Intelligence called "the most egregious level of espionage ever seen[85]."

Based on its assessment of these errors, Congress passed the National Counterintelligence Reform Act of 1994. This law was designed to change the institutional errors outlined by the Senate Select Committee and create a structure that would promote a more unified Counterintelligence Community. The key aspect of this law was the creation of the National Counterintelligence Center (NCIC). The NCIC was designed to develop a national counterintelligence policy and create a national program for counteracting foreign threats[86]. The problem was that it did not do this. The NCIC did not present unified national policy that was capable of "unifying" the different Counterintelligence offices. Thus, the institutional problems that should have been fixed following the Ames case continued, allowing Robert Hanssen, who began spying even before Ames, to continue his activities until February of 2001.

As with all such failures, following the conviction of Robert Hanssen, policy makers again directed "fixes" to the Counterintelligence Community. In 2002, Congress passed the

[84] Senate Select Committee on Intelligence, "An Assessment of the Aldrich H. Ames Espionage Case and its Implications for U.S. Intelligence", (US Government Printing Office: Washington DC, November 1994).

[85] Ibid.

[86] United States Congress, "National Counterintelligence Reform Act of 1994", Senator Slade Gorton, May 1994.

Counterintelligence Enhancement Act of 2002, which brought about the creation of the NCIX, and the National Counterintelligence Policy Board[87]. Together, these two organizations were tasked with tying the community together and providing guidance, leadership, and oversight in US Counterintelligence. The NCIX would accomplish this mission by producing the annual National Counterintelligence Strategy[88]. This strategy, which would set forth priorities for the community, would be based on information from the National Threat Identification and Prioritization Assessment (NTIPA)[89]. However, this was not enough. More changes were needed as was highlighted in 2005 when the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction said that US Counterintelligence was "fractured, myopic, and only marginally effective[90]." This understanding would lead to further changes and improvements in the NCIX and in US Counterintelligence; the change that was needed was to address insider threats specifically.

One of the key tenets with regards to the establishment of the NCIX was the ability to standardize the approach taken by myriad CI organizations to counter the "insider threat." The answer to this problem would come in 2009 with the newly created Insider Threat Advisory Group (ITAG) and, in 2011, with the National Insider Threat Task Force (NITTF).

[87] This law would formalize Presidential Decision Directive 75, issued by President William Jefferson Clinton, which proposed the NCIX position.

[88] United States Congress, "Counterintelligence Enhancement Act of 2002", November 2002.

[89] Representatives from the FBI, CIA, Department of Justice, and Department of Defense draft the NTIPA annually. (John Fox, Jr. and Michael Warner, "Counterintelligence", *Vaults Mirrors, and Masks*, ed. Jennifer Sims and Burton Gerber, (Washington D.C.: Georgetown University Press, 2009)).

[90] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States,* (Washington D.C.: Government Printing Office, 2005).

These two organizations would help draft policy, implement standards, and continuously assess the implementation of a National Insider Threat Policy.

The ITAG was established in the 2009 National Counterintelligence Strategy. The role, as laid out in that strategy, was to define, the organizations that counter insider threats, the "best practices" from these organizations, and make a uniform policy from which to counter insider threats[91]. Despite the ITAG's very vague role, Gene Barlow, of the NCIX office, clarified the ITAG's purpose stating that it would be a committee composed of members from across the IC that meets to create a unified policy, derived from the successes (or best practices) of other organizations, for defeating insider threats[92]. All organizations in the IC would have a role to play by contributing their best practices, and eventually adapting to future recommendations proposed by the ITAG. Additionally, the ITAG recommended creating another organization to help with the implementation and standardization of the new policy. This new organization would be the National Insider Threat Task Force[93].

Following the formation of the ITAG, in 2011, President Barack Obama released Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information[94]." This executive order incorporated the initial assessments of the ITAG, officially created the NITTF, and

[91] Office of the Counterintelligence Executive, "The National Counterintelligence Strategy of the United States of America," 2009.

[92] Gene Barlow, Office of the National Counterintelligence Executive, Interview: December 20, 2013, Topic: National Insider Threat Task Force and Insider Threat Working Group.

[93] Ibid.

[94] Barack Obama, "Executive Order 13587: Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 2011.

established a timeline for publishing the National Policy. The role of the NITTF, as described in EO 13587, was to finish the development of the National Insider Threat Policy and to ensure its implementation within one year[95].

The NITTF continues to this day to undergo refinement. According to George Stukenbracker, the co-director of the NITTF, its current mission is to outline the National Policy for training, establish minimum standards for insider threat programs, conduct command inspections of insider threat programs to ensure compliance, recommend improvements to organizational insider threat programs, and give country-specific threat briefs for the IC[96]. This mission gives them the unique ability to conduct oversight across the CI Community and continually realign the community's approach to insider threats. Comprised of officials from across the community, the NITTF will be able to provide new perspectives that CI specialists in the Department of Defense, Justice, or State may not see based on their institutional mission.

The creation of the NITTF was one of the biggest changes in the CI Community during the past 20 years and is already beginning to show signs of success. The group's formation, and drafting, of a National Insider Threat Policy is a huge step from previous organizations, which were "formed," but never did anything. This new National Policy will sync all of the different CI organizations and ensure a united message across the community designed at targeting the tactical-level decision makers. What this does, effectively, is turn all

[95] Ibid.

[96] George Stukenbracker, Co-director of the NITTF, Federal Bureau of Investigations, Indirect Interview Conducted: December 20, 2013, Topic: Joint Insider Threat Task Force and Counterintelligence Working Groups.

those who work in the IC into "sensors" for insider threats. Secondly, by requiring that training match a national standard, all IC personnel will receive consistency of training objectives and a standard message across the IC. The result of this has been crucial, increased reporting, and increased sensitivity to potential threats. Additionally, the creation of the NITTF has led to the drafting of new organizational-level training standards and policies in many CI organizations[97]. One example is the Army. The old "insider threat" manual, AR 381-12: Subversions and Espionage Directed Against the United States Army, has since been re-written. The new AR 381-12: Threat Awareness and Reporting Program, written in 2010, was very important because it began to incorporate protection against terrorist and extremist organizations, something the older document did not address[98].

The last and largest NITTF benefit to the IC is a new collection of country threat briefings and threat analyses they produce. These briefings will be created by the NITTF and used as apart of regular threat briefings to IC personnel traveling outside the United States. The analysis will be conducted by IC analysts and given from the NITTF to IC agencies regularly to ensure that there is a clear, coherent, and current threat analysis for every country in the world. These provide government agencies a general CI threat picture. This information is important because it gives leaders in the Army, Navy, Air Force, or one of the 17 intelligence agencies information on threats that will be seen by all organizations. This is a good starting point for deeper analysis by the CI Community on their mission-specific threats. By forcing the CI Community to operate together and create unified policies,

[97] In the past year, the Air Force, Navy, and DIA have all drafted new Insider Threat programs, which conform to the new standards of the NITTF. The Army devised their training in 2011.

[98] Department of the Army, *Army Regulation 381-12, Threat Awareness and Reporting Program*, 1993.

different perspectives of CI will drive future changes. Continual adaptation means increased awareness of and sensitivity to emerging threats, which in turn equates to greater success.

The Counterintelligence Community has come a long way from its beginnings. It has changed and adapted over the years to meet the challenges it has faced. The NITTF and the ITAG are very useful additions to the CI Community, but will they accomplish their goals? The unified policy now in its second year is already making strides to fix problems, but there are still changes to be made. These will not be easy, as is the case with most reform, whether it is with the Intelligence Community as a whole or just the CI Community.

Chapter 4: The Reform Process

Given the many insider threat-related challenges the CI Community faces, the United States has done a great deal to confront this dangerous enemy. Nonetheless, the CI Community must make additional changes due to weaknesses in the current legislative processes, organizational interactions, and other issues involved in this effort [99]. As addressed in Chapter 3, the structure of the CI Community has adapted over the years, but the sad reality is that these changes happened largely as a result of failures in the system and knee-jerk reactions designed to address specific instances of failure[100]. Even then, the changes that do occur often do not come easily and are the result of extensive reform processes throughout the IC. The ever-present threat posed by insiders means that the US CI Community must routinely evaluate the process it operates under and look to better itself. Our CI specialists must address a range of persistent vulnerabilities to help strengthen the American security apparatus. The problem is that substantive reform is often very difficult to accomplish in the IC, and subsequently the CI Community, for two reasons. First, intelligence reform is usually more politically motivated than it is focused on, and motivated by, the need for substantive change[101]. Second, since the IC is a tool of the policy makers, who ultimately oversee these organizations, this often means that the people making decisions for the IC have little to no

[99] As stated previously in Chapter 3 this paper will focus on the Strategic Level improvements in the IC and CI Community because of the number of agencies and vast organizational differences at the Operational and Tactical Level.

[100] The 1994 reorganization and 2002 Reorganization were the result of the arrests of Aldrich Ames and Robert Hanssen respectively.

[101] Amy Zegart, "September 11 and the Adaptation Failure of U.S. Intelligence Agencies," *International Security*, Spring 2005, pg. 98.

real understanding of the Intelligence process[102]. As Chapter 3 demonstrated, there were multiple reforms over the past 20 years that have helped mold the CI Community into an organization that could fight the insider threat. These changes however, were not the result of planned reform, they were reactionary movements to larger community failures that allowed insiders like Ames, Hanssen, and Hassan to exist. Politicians do not like huge failures for political reasons, so large high-profile events act as ”motivation” for change, and to show their constituents that they are making things better[103].

Policymakers drive the intelligence cycle. As the driving force, they should continually evaluate the systems in place, judging their effectiveness and adapting them as need be[104]. Unfortunately, this is often not the priority of those in the policy community[105]. The absolute certainty of the need for reforms in the CI Community begs the question, why have major substantive reforms not happened yet[106]? The answer to this question relates to the challenges that intelligence reform faces: time, concession of power, and consensus.

Time is a valuable commodity and one that has a dramatic impact on the actions of people everywhere. Whether it is rushing to meet a deadline or hanging on for the long run, time seems to dictate our lives, and this idea could not be truer for both the IC and the policy

[102] Richard K Betts, *Enemies of Intelligence: Knowledge and Power in American National Security,* (New York: Columbia University Press, 2007), pg. 3.

[103] Ibid pg. 2-3.

[104] Mark M Lowenthal, *Intelligence: From Secrets to Policy,* (Washington DC: CQ Press, 2000), pg. 65.

[105] Ibid pg. 57.

[106] Substantive reform that is not a knee-jerk reaction is the key. Yes, there have been “major reforms,” but those were only in response to failures, and initially they did little to address institutional failures as shown in Chapter 3.

community. The reason that time is such a significant challenge to reform has to do with the nature of the IC and CI communities, the policy community, and the dramatically different understandings they have of time.

First, in the IC there has traditionally been less sense of time-urgency, because before 9/11 intelligence was seen mostly as a long-run game, an endurance race. The challenges posed by agile extremist organizations have forced the IC to face a new paradigm in this arena. However, when it comes to collecting, analyzing, and exploiting so much information from the enemy, whether that is an insider threat, a nation-state he spies for, or an ITO supporting him, the operations tend to last for years. As intelligence professionals see it, steady analysis not rushed by political pressure is the key to success. Conversely, in Congress and the White House, politicians are rushed to make their mark by showing their constituents what they have accomplished. In this sense, they often view intelligence as a tool to gain large results in a short period of time. With the two operating under a different time frame there are bound to be confrontations[107].

The second and most important way that time holds back reform is in the reform process itself. Given that reform will be drafted and incorporated by the policy community, the US Congress cannot simply "change." Rather, there have to be bills written, voted on, debated, passed, and signed into law. This all takes time—a very long time. To make matters worse, it is the legislature's right to conduct an investigation into failures, or reasons for

[107] Loch Johnson and James Wirtz, *Strategic Intelligence: Windows into a Secret World*. (Roxbury Publishing Company, Los Angeles, 2004), pg. 222.

reform[108]. As Berkowitz states, "Commissions take months to convene, staff, and complete their work. Experience shows that commissions require, on average, a year or two to report their results—and even more time to declassify their reports so they can be released for public discussion. During this time, any passion officials might have had for fixing intelligence ebbs and the public's attention wanders to other matters." Just one example of this is the September 11th Commission, which was formed a year after the attacks, releasing results two years later, and passing changes through Congress 10 months later[109]. The problem here is that the IC has its most fervent reform supporters immediately after the failure, as was the case with Ames, Hanssen, and Manning, yet as time drags on, the supporters of reform begin to become busy with other things, and the intended reforms do not come to fruition[110].

The next major barrier to reform is cession of power, because giving up power is not what any agency, or leader, wants to do[111]. This desire to maintain power often results in nothing more than long debates and very weak results, if any at all. An example of this is clear within the IC. In 2002, with the creation of the position of the NCIX, the Counterintelligence Enhancement Act of 2002 tasked the NCIX with developing the annual National CI Strategy. Developing this strategy would be based on the NTIPA as stated in Chapter 3. The problem is that the NTIPA and the CI Strategy are not based on the Director

[108] Bruce Berkowitz, "Intelligence Reform: Less is More," *Hoover Digest*, (Hoover Institution, Stanford University, April 2004).

[109] Ibid.

[110] Ames led to the 1994 legislation, Hanssen the 2002 legislation, and Manning the 2011 Executive Order.

[111] Ibid pg. 100

of National Intelligence's National Intelligence Strategy (NIS), nor does the NIS say anything about CI[112]. This is because with the creation of the NCIX in 2002, it was given the power of drafting the CI Strategy, while the DNI, created in 2004, does not have the power to "develop" any part of the CI strategy. This is one area where a small cession of power and cooperation between organizations could go a long way to unifying the role that the DNI has within the IC[113]. This tight hold on the CI Community has had drastic consequences for the office of the DNI, which was originally designed to provide leadership and guidance for all of the IC, but left weak and limited.

Like time, consensus is a chief barrier to reform for the IC and policy community because of how the intelligence cycle works. However, consensus is probably the most important barrier because of the ways in which it can affect other barriers to reform. One of the key ways in which consensus is a challenge to reform has to do with the fact that consensus implies that both sides come to an agreement. As Berkowitz discusses, political compromise allows opponents to sabotage the creation of any new agency from the start by simply not agreeing to certain aspects of potential future laws[114]. This truly is a hurdle for reform because while politicians, and heads of agencies, can come with hands outstretched under the banner of reform, a "nay" vote or even language inserted into a bill that passes through the legislature can destroy consensus and weaken any real reforms.

---

[112] This remains a problem because the DNI has the power to allocate money to different priorities as outlined in the NIS. The NCIX develops the budget for CI programs based on the National CI Strategy and then must work with the DNI for funding that budget.

[113] Jennifer Sims, "Democracies and Counterintelligence," *Vaults Mirrors, and Masks*, ed. Jennifer Sims and Burton Gerber) Washington D.C.: Georgetown University Press, 2009), pg. 4.

[114] Berkowitz, Intelligence Reform.

Another major barrier to consensus is the secret nature of the IC. The reality is that the majority of the work that the IC does is classified, which can be a problem for the policy community. The reason this level of secrecy is such a major issue is that members of the policy community do not normally have the clearance to see all the information necessary to make proper decisions about CI or any other reforms. This lack of information basically leaves the IC asking Congress to go along with their plans with a minimum amount of information and understanding of what the plans actually are[115]. In this way a call to reform without all the necessary components is not asking for consensus, but rather asking for acceptance by the few who have access to the intelligence, which in the case of the Senate is a Select Committee of 15 individuals and in the House, 21 individuals.

Finally, for the proper cession of power there must be consensus on the level of gains or losses, which can end up being a problem, especially for agencies or individuals not wishing to lose power. For example, when the office of the Director of National Intelligence was created, the policy makers and the Department of Defense never could gain consensus as to the level of power the DNI would have, and the result of this was a DNI with very little power[116].

Ultimately, time, power struggles, and consensus will remain barriers to reform and until those barriers are overcome, the IC, the CI Community, and the policy community will continue to experience problems like those already seen. This continuing failure will waste

[115] Michael V. Hayden, "The State of the Craft: Is Intelligence Reform Working?" World Affairs, September/October 2010.

[116] Zegart, pg.100.

time and effort—time that is already in short supply and could be used to stop insiders instead of allowing them to continue damaging the United States.

In light of these challenges and the problems that still exist, we must evaluate the kinds of changes required for the continued fight against insider threats. As has been previously mentioned, this work focuses on reform efforts at the strategic level for three reasons. First, top-down reform is critical when it comes to addressing an enemy like the insider threat where a unified approach is needed. Second, reform suggestions for individual agencies look too deeply at specific tactics. Addressing weaknesses would have very real security implications due to the nature of the sensitivity of the mission. Finally, the sheer number of differences between the different operational agencies and their different mission sets would inundate researchers and not allow adequate analysis of weaknesses at any other level.

In order properly to look at each problem, this work will first define the problem within the CI Community that interested parties must address. Next, it will outline steps for proper implementation of the reforms. Inherent to this is how implementation will address the aforementioned barriers to reform. Lastly, for each reform effort this work will offer some evaluation criteria, which may be used to identify strengths/successes or weaknesses of the reform efforts.

Before presenting recommendations, understanding what type of reform is best for the IC is essential to ensuring the best changes. Sweeping reform efforts generally do not work. Often, in the effort to "fix problems" policy makers will make massive and

revolutionary changes[117]. These risk throwing out the good organizational structures, procedures, and systems in place along with the bad ones. The changes proposed in this work are intended to limit the "pendulum swings" that Richard Betts refers to, and to offer minor corrections that will benefit CI in its continued missions to stamp out insider threats[118].

Lastly, one important issue to highlight for evaluation is that intelligence reform evaluations are difficult to assess due to the nature of intelligence. By definition, intelligence helps to inform. Good intelligence may help to inform leaders of decisions needed to prevent negative outcomes. In this case, decisions made will yield little to no "visible" result. However, when intelligence does not inform, and disaster occurs, policy makers will tend to say there was a failure in intelligence[119]. Failures are always visible, and the IC is almost always held accountable. The root of this problem rests in the fact that the only true success is 100-percent success[120]. The next time a spy is caught or a violent extremist blows himself and American citizens up, policy makers will begin looking at the system as a failure. The reason this is seen as a failure is because of the misunderstanding of what intelligence is and what it does. Intelligence is not predictive and it cannot catch 100 percent of the problems, especially when it comes to insider threats. As with all things in this world, everyone and everything has a say, to include our enemies, for every action that we take our enemies can be expected to take two. Knowing this, policy makers must understand that there will always

[117] Betts, pg. 2.

[118] Betts, pg. 18.

[119] John Hollister Hedley, "Learning from Intelligence Failures," *International Journal of Intelligence and Counterintelligence*, Volume 18, Number 3, 2005, pg. 436.

[120] Paul Pillar, *Intelligence and US Foreign Policy,* (New York: Columbia University Press, 2011), pg. 8-9.

be uncertainty in intelligence and that "failure" is not necessarily failure there is always more that is accomplished that is never seen[121].

The first improvement that is needed is the establishment of a common definition of an insider threat. Currently, there are over 15 different definitions as outlined in the NCIX's Official Terms & Definitions of Interest List[122]. Such a broad list of definitions leaves many questions in the minds of the different IC agencies as to what an insider threat is, and who has jurisdiction regarding collection, analysis, and apprehension. Most importantly, the definition in the 2012 National Policy lacks any sort of tie to a foreign nexus[123]. This vague language creates confusion as to who has jurisdiction over potential insiders. According to the policy definition, CI would have been responsible for identifying and handling any threat, to include domestic law enforcement cases. The problem is that if these threats are American citizens, not working for extremist organizations or foreign nations, then CI does not have jurisdiction as assigned in EO 12333[124]. This current lack of specificity can cause confusion when it comes to handling insider threats, because over utilization of CI and LE on areas outside of their jurisdiction leaves them both over-exerted and stretched thin[125]. Furthermore,

---

[121] Betts, pg. 11.

[122] Office of the National Counterintelligence Executive. *Terms & Definitions of interest for Counterintelligence Professionals.* October 2013.

[123] National Insider Threat Task Force. *National Insider Threat Policy.* Issued by President Barack Obama, November 2012.

[124] Additionally, the General Provisions of the National Insider Threat Policy specifically state that this policy shall not be construed to supersede or change the Requirements of EO 12333.

[125] Ernesto Londoño, "Pentagon Grapples to Understand how yet Another Insider Threat went Undeterred." *New York Times*, 03 April 2014, http://www.washingtonpost.com/world/national-security/pentagon-grapples-to-understand-how-yet-another-insider-threat-went-undeterred/2014/04/03/6cf43b3a-bafc-11e3-9a05-c739f29ccb08_story.html, 05 April 2014.

establishing a definition will be difficult with as many different and divergent definitions as we already have throughout the government. As was mentioned, consensus is important and right now there is none. Changing this will require the NITTF to build common ground and push past the differences. The important thing to remember is that words have meanings and, as the 2009 NIS states, insider threats are the priority for CI[126]. An open-ended definition will tax a stressed organization. Specificity allows work to be spread across the spectrum of CI and Law Enforcement cases and thus increase the amount of success.

Chapter 1 of this paper outlined the author's definition of an insider threat as "an individual with placement and access to critical infrastructures, military units, and the government and their supporting agencies who have allegedly turned against and targeted their parent organization, thus aiding a foreign power or international terrorist organization." This definition is based on a conglomeration of multiple different definitions used across the IC. It encompasses all of the critical elements of the threat and leaves no question in the minds of the different agencies as to who has jurisdiction. Simply adopting a new definition does not mean that "jurisdiction battles" will be solved. Inherent to any definition is the constant need for cooperation amongst the different organizations of CI and in the case of uncertainty, to allow for joint investigations and the sharing of potentially valuable information between the different disciplines[127].

[126] Director of National Intelligence, "The National Intelligence Strategy of the United States of America," August 2009.

[127] Valuable information that involves unknown nexus would be important to both law enforcement and Counterintelligence. Additionally any information that has foreign ties, such as recruitment methods and future attacks would be important to both LE and CI due to the different levels of protection they can offer at different levels.

Evaluation will be more than just the success or failure of a standard definition. The definition itself will be tied to a broader evaluation of the National Threat Policy. Accordingly, the ITAG and the JITTF would be primarily responsible for the evaluation of current policies. In order to do this, an evaluation of classified and unclassified reporting and investigations, at the national level, will identify increases in reporting, opening of investigations, opening of joint investigations, prosecutions, and operations conducted. An increase in these numbers would be a strong indication that programs are working, at least in the short-term. This data would be compiled and presented by the NCIX to the DNI and policy makers as an indicator of the change that is occurring with new policies. Granted this information would not be shown to all policy makers, but there are representatives in Congress and the White House that would be privy to this information, and that serve as representatives for the broader policy community[128].

The second improvement needed is that the CI Community should realign insider threat training to focus toward preventing threats, not simply identifying them. The National Insider Threat Policy includes a set of "Minimum Standards for Executive Branch Insider Threat Programs." These minimum standards are the current guidelines promulgated by the executive branch, the NCIX, and the JITTF regarding Insider Threat Programs[129]. The programs' standards have addressed many of the issues relating to insider threats except one key issue: prevention. The minimum standards read more like a list of training for

[128] The National Security Council, Senate Select Committee on Intelligence, and the House Select Committee on Intelligence are just a few of the groups that would important to keep informed on the developments of recent changes in policy.

[129] National Insider Threat Task Force. *National Insider Threat Policy: Minimum Standards for Executive Branch Insider Threat Programs.* Issued by President Barack Obama, November 2012.

identification of a current threat, and less like a set of preventative measures. Identifying threats is useful, but the problem with insider threats is that they are often unidentifiable; more is needed in the form of prevention. The major problem with passing changes such as these is, once again, the problem of time. As previously stated, policy makers like to see fast results. Preventative measures will not get nearly the same results as fast as identification. Focusing training on identification can give quantifiable numbers to policy makers about how successful a program has been by catching bad guys. One can hope that politics is not all that is at play when it comes to determining how these programs are organized, but these changes will need to be made quickly because the longer they wait the longer the system goes without preventative measures.

Not much needs to be added to current CI training, but an understanding of the basic threat psychology, as addressed in Chapter 2, should be a part of the Minimum Standards. A key element of this "preventative measure" is the provision of information regarding where developing threats can seek assistance, how coworkers can report suspected problems for assistance, and how supervisors can refer to assistance. These insights would be crucial both for impacting the potential downward spiral and the apprehension of an individual. The one major outlet that exists is in Employee Assistance Programs (EAPs).

As stated in EO 12968, all individuals working for agencies with access to classified information are eligible to use EAPs for "assistance concerning issues that may affect their eligibility for access to classified information, such as financial matters, mental health, or substance abuse." Essentially EAPs are counseling services for those in the IC who need an

extra support structure to get personal help[130]. The problem is that often there is a stigma placed on anyone for using these services. The proper use of these programs is crucial for serving this preventative measure and should be included in training as a healthy outlet free of judgment or damage to one's career.

One thing that the Spy cycle and the Radicalization cycle both underscored was that in the earliest stages of the development of an insider threat, there was a need for help. The spy found that help in the solace of a foreign intelligence service, while the future violent extremist found it in the support network of an international terrorist organization. By focusing training on identification at the later stages of development, we are skipping an important step in the progression of an insider threat. Ignoring the early stages does nothing to prevent those potential future threats sitting on the edge of right and wrong from making bad choices. By adding to the current training a focus of earlier detection then the potential to remove the future insiders from their support structure and offer them a healthy outlet is possible. Additionally, teaching this training to everyone will turn personnel into sensors for future threats, not just current ones[131].

The best way of evaluating change would be through the use of the individual agencies' EAPs. These would continue to offer their counseling services as usual; nothing would change except for how they report the raw number of appointments and referrals each week. The visits, while confidential, would remain secret, but the number of meeting and

[130] President William J Clinton. *Executive Order 12968: Access to Classified Information.* August 1995.

[131] Defense Human Resources Activity. *Understanding and Helping People with Personal Problems: Employee Assistance Programs,* http://www.dhra.mil/perserec/osg/eap/intro.htm#Understanding %20and%20Helping, 30 March 2014.

referrals would be reportable. These reports could be crucial to evaluating the effectiveness, results could be gleaned from: the amount of internal reporting, scheduled visits to EAPs, and new clients meeting with EAPs. This information would show an increase or decrease in what an EAP deems a "potential threat," which then could be gathered and presented to policy makers as indicators of the effectiveness of programs and to illustrate the internal changes occurring because of new policies.

The third change is the NCIX and DNI should draft the National CI Strategy together and base priorities off the NIPF with the NTIPA serving as a supplement, not the primary factor. In 2002, Congress passed the Counterintelligence Enhancement Act of 2002, which brought about the creation of the NCIX and the National Counterintelligence Policy Board[132]. Together, these two organizations were tasked with tying the community together and providing guidance, leadership, and oversight to US Counterintelligence despite not having actual control over the agencies and offices accomplishing the mission[133]. The NCIX manages to accomplish this by producing the annual National Counterintelligence Strategy[134]. This strategy, which draws priorities for the community, is based on information from the National Threat Identification and Prioritization Assessment (NTIPA)[135]. The problem with this production system is that the NTIPA is drafted separately from the

[132] This law would formalize Presidential Decision Directive 75, issued by President William Jefferson Clinton, which proposed the NCIX position.

[133] Lowenthal pg. 161

[134] United States Congress. *Counterintelligence Enhancement Act of 2002*, November 2002.

[135] The NTIPA is drafted annually by representatives from the FBI, CIA, Department of Justice, and Department of Defense.

National Intelligence Priorities Framework (NIPF)[136]. This is a problem because the NIPF is the DNI's list of official priorities for the IC, drawn from policy maker, diplomatic, and defense priorities[137]. When the two documents are drafted separately, there is little to tie the two together, and the system will remain a disconnected and fractured bureaucratic mess. To complicate matters, the DNI, whose position was created in 2004, is tasked with providing priorities and guidance to the IC, yet based on the 2002 Counterintelligence Enhancement Act the DNI has no say on the priorities at play for the CI strategy. In essence, the DNI has no control over one of its own subordinate offices. The only control that the DNI does have is over the spending of the NCIX. However, since the NCIX does not have any budgetary control over the subordinate CI offices in the IC, this control is even limited[138]. This is a major challenge to cession of power, and one that is controlled by law. In order to change this, policy makers will have to become involved, and as mentioned earlier, time is never on the side of the reform process.

The NTIPA, while it has merit, needs to be more closely tied to the NIPF. Without this connection, the Intelligence Cycle is broken and CI elements are conducting their mission independent of their "consumers" needs. The problem with this as the Intelligence Cycle highlighted the role of intelligence as support the policy maker by providing the best information to make informed strategic decisions. By creating the National CI strategy in a vacuum from the NIPF the NCIX the oversight that is presented by policy makers in lost and

[136] What becomes the National Intelligence Strategy from the DNI.

[137] Sims, pg. 2.

[138] Lowenthal, pg. 161.

there are competing priorities within the IC, which result in lost effort[139]. To fix the problem, Congress will need to pass an amendment to the CI Enhancement Act of 2002 making the CI strategy the product of the NCIX based on the NTIPA and the NIPF. By doing this, the DNI will finally have control over the NCIX, one of its subordinate offices.

Evaluating the effectiveness of this reform would be difficult to do from outside the IC and CI Community, but the regular coordination would be reflective of a better synchronization of priorities. Additionally, this reform would do more for the policy makers by ensuring that those groups that collect for them are meeting their expectations. That being said, the evaluation would be conducted annually by the Senate and House Select Committee on Intelligence who have the clearances to understand the intricate details of collection efforts, how effective they have been, and to what degree the CI and IC threats are synchronized.

The final improvement is to give the NTIPA more IC representation and less LE influence. As previously discussed in Improvement 3, the National CI Strategy is based on information collected from the NTIPA. Representatives from the FBI, CIA, Department of Justice, and Department of Defense draft the NTIPA, as a document, annually. The problem with this document is that it is drafted from a predominantly law-enforcement (LE) and defense-oriented perspective which skews priorities and only loosely aligns them to policy makers' objectives[140]. Due to the mission of CI outlined in Chapter 3, intelligence and CI like to exploit, whereas LE focuses on neutralization, the priorities need to be established from an

[139] Ibid pg. 57.

[140] Sims, pg. 2

intelligence centric view[141]. Using a predominantly LE organization to create the priorities for an Intelligence organization is flawed and begs for underutilization of intelligence assets[142]. The problem with changing this system is that the LE organizations are not going to be as interested in ceding the power they have in the NTIPA and so any sort of battles for power will take time away from potential reform—time that is and always will be crucial. This is in no way an indictment of the closeness of the IC, CI, and LE professions because ultimately, should a threat present itself, there needs to be a close working relationship since any case could potentially move between CI and LE as it develops[143].

Fixing these problems will require the NCIX to alter the makeup of NTIPA. In order for this to happen, Congress would have to pass legislation, and that takes time for a group that often does not generally do things fast. Assuming that such a bill passes, the next best step would be for the DNI to reorganize the NTIPA to include members from all across the IC. Reorganizing as such would allow their meetings to be focused on collaboration of threats and discussions about how to handle them.

It is worth repeating that evaluating the effectiveness of this reform would be difficult because intelligence failures, whether real or perceived, are highly visible, but the successes

[141] CI is given priority because while handling an insider threat is inherently a crime, the nature of that crime yields greater benefit to intelligence, intelligence is better equipped to handle a insider spy backed by a foreign government, media coverage that may follow LE cases damages intelligence operations, and intelligence is used to running longer operations sometimes taking years. (William E Odom, *Fixing US Intelligence,* (Yale University Press, 2003), pg. 177)

[142] Odom, *Fixing US Intelligence,* Yale University Press, 2003, pg. 177.

[143] One reason that this is so important in insider threat cases is because by nature of the incident, a crime has been committed. Law Enforcement at some point will need to be involved if prosecution is ever needed at which point CI and LE forces will need to have been working closely to identify the best time to neutralize the threat. (Odom, pg. 175)

are not. Consequently, the best metric would probably be an analysis of the NTIPA's priorities to see what amount of influence LE agencies have exerted as opposed to those in the IC. Comparing past years' priorities to current ones will show the natural progression of frame of thought that those drafting the NTIPA had.

These four changes, while not dramatic, offer insights into a few things that the IC can do to fix the "fractured" systems in the CI Community. They maintain that there are valuable systems in the IC and that the "changes" should not be so dramatic as to throw out potentially good processes. The insider threat is too important to be tossed aside because of political inconveniences, only to be looked at when there have been failures. The increase in insider activity in the past few years is an indication that policy makers and the IC should place serious consideration on what needs to happen to the insider threat framework. It is sad that it must come down to the loss of some of the nation's most important secrets for this to happen, so we must continue to work toward meaningful reform.

Conclusion

As this paper has shown, in the years since the end of the Cold War, the United States has spent nearly 13 years fighting international terrorism. The efforts spent overseas were a part of a larger mission to protect the American people and ensure global peace stability. The problem is that while the United States was fixated on the fight against al-Qaeda, foreign governments and international terrorist organizations were reorganizing, targeting the weaknesses that remained on the US homeland. Many governments took this as an opportunity to exploit weak intelligence security, through the use of spies. Additionally, terrorists, who had been stopped overseas, set their sights on America and began working with US citizens to conduct their attacks. These two threats, the American terrorist and the American spy, comprise what is known collectively as insider threats. This is not a new threat, it is one that is as old as nation-states, but it is one that is once again becoming a chief concern for policy makers as America's wars come to an end and a renewed focus is placed on internal security. This paper has sought to answer one main question: How successful has the United States Intelligence Community (IC) been in responding to the increase of insider threats? As the last four chapters have shown, given the nature of Intelligence work, a clear evaluation is not possible for operational successes and failures. As was previously stated, the purpose of intelligence is to inform leaders of current situations and to provide them with the best understanding of policy actions. When intelligence does not fully inform, and bad policies are made, the results are often dramatic and result in policy makers blaming intelligence for these failures. Additionally, any correct decisions made will yield little to no "visible" results of success. What is apparent is that the United States has made many strategic reforms needed to better posture the IC to defeat the Insider Threat. These reforms

have been strategic successes by altering IC structures and organizations. These reforms are addressing insider threats from the top down for the first time in history and have been very beneficial to the strategic makeup of the CI Community. What effect these changes will have on the operational level is yet to be seen, and will in fact not be realized for several years. Despite these successful changes there are still reforms that are needed to bolster previous actions. This assessment is based on the answers to the 5 sub-questions that each chapter looked at in detail.

Chapter 1 provided a more in-depth description of an insider threat. It did so in an effort to identify the best definition and to demonstrate that there is a certain amount of disparity in the IC about the definition of an insider threat. In this discussion, greater detail and understanding of the different types of insider threats revealed just how similar the threats really are. This Chapter was essential to provide the reader a complete understanding of what the threat is and why the threat exists.

Building on this definitional effort, Chapter 2 looked at the theoretical process by which people become insider threats. This chapter sought to answer where insider threats come from and highlighted the many studies that have been conducted recently focusing on insider threat psychology. Identifying the answer to this question relied heavily on the psychological aspects of insider threats and explaining why some people decide to betray their country. While the goals of the two types of threats may be different, the "radicalization"/"spy lifecycle" processes are very similar. Additionally, this chapter is significant because it reveals various key considerations that must be understood when determining how to deal with insider threats. Chief among these considerations is understanding how insider threats develop. Understanding an insider threat's origins offers

insights into possible preventative measures that the CI Community can use to develop proactive policies.

Chapter 3 then showed the historical evolution of the insider threat structures and the current structures for countering insider threats. This chapter was designed to answer the next two questions: how insider threats have impacted the IC, and how Insider Threat Groups have helped the IC to target insider threats. This chapter described the unique challenges facing the IC and CI Community and how the CI mission is specially adapted to counter the insider threat. Furthermore, the reader should understand that the current insider threat structure is one that has been influenced by the past and changed several times over the last twenty years fixing weaknesses that allowed large scale damage like that of Aldrich Ames and Robert Hanssen. These reactions, while bringing about a largely bureaucratic mess, have resulted in a few potential good systems as well that have yet fully to show the IC their true capacity.

Finally, Chapter 4 acknowledges the positive changes that have occurred but also emphasizes the necessity for further reform. This final chapter answers the last question regarding what changes are still needed. Discussing reform impediments briefly, this chapter reveals how time, concession of power, and consensus were the key impediments to reform in the CI Community and its insider threat structures. This chapter explains that four simple changes could bring about significant difference in the CI community and greatly assist in the fight against insider threats. Based on material presented in the foregoing chapters, here are the key recommendations for policy makers:

1) Establishment of a common definition of an insider threat that encompasses all crucial elements of an insider threat.
2) Realign insider threat training to focus more to preventing threats, not simply identifying them.
3) The NCIX and DNI should draft the National CI Strategy together and base priorities off the NIPF with the NTIPA serving as a supplement, not the primary factor.
4) Increase IC representation and decrease LE influence in the NTIPA.

The changes that this paper offers are not revolutionary changes, they are minor changes that will help the system fight the insider threat. These first improvements can help develop the CI community to meet current and potentially future challenges. Following these changes if others are required, then they can be made then, but the most important thing to remember is in the search for the best reforms, do not cause additional damage where there once was none. The question now lies in what will happen. Will the identified problems come under substantive reform creating systems and structures that will best help to counter the threat, or will the desire and drive for reform waver as memories of Manning and Hassan become part of the distant past?

Bibliography

Amy Zegart, "September 11 and the Adaptation Failure of U.S. Intelligence Agencies," *International Security*, Spring 2005.

Antoine Henri Jomini, *The Art Of War,* Westport, Conn.: Greenwood Press, 1971.

1971.

Barack Obama, "Executive Order 13587: Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 2011.

Bruce Berkowitz, "Intelligence Reform: Less is More," *Hoover Digest*, April 30, 2004. Hoover Institution, Stanford University.

Bruce Livesey, "The Salifist Movement," Frontline, PBS. http://www.pbs.org/wgbh/pages/ frontline/shows/front /special/sala.html.

Carl von Clausewitz, *On War.* ed. and trans. Michael Howard and Peter Paret, Princeton, NJ: Princeton University Press, 1976.

Christopher Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*, Basic Books: 1999.

CI CENTRE, "DOMESTIC TERRORISM CASE: Inland Empire Jihad Plot", http://www. cicentre.com/?Inland_Empire, 15 February 2014.

CICENTRE, "DOMESTIC TERRORISM CASE: James Cromitie", http://www.cicentre. com/? CROMITIE_James, 15 February 2014.

CICENTRE, "DOMESTIC TERRORISM CASE: Nidal Malik Hasan", http://www.cicentre. com/?HASAN_Nidal, 15 February 2014.

CICENTRE. “DOMESTIC TERRORISM/ESPIONAGE CASE: Ryan Anderson”, http://www.cicentre. com/?page=ANDERSON_Ryan, 15 February 2014.

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

Daveed Gartenstein-Ross and Laura Grossman, *Homegrown Terrorists in the U.S. and U.K.*, FDD Center for Terrorism and Research, April 2009.

David L Charney, “True Psychology of the Insider Spy: Insights on the Profession”, *Intelligence Journal of the U.S. Intelligence Studies*, Fall/Winter 2010.

Defense Human Resources Activity. *Understanding and Helping People with Personal Problems: Employee Assistance Programs,* http://www.dhra.mil/perserec/osg/eap/ intro.htm#Understanding %20and%20Helping, 30 March 2014.

Department of Defense, “DOD Insider Threat Mitigation: Final Report of the Insider Threat Process Team,” April 24, 2000, http://www.c3i.osd.mil/org/sio/iptreport4_ 26dbl.doc.

Department of the Army, *Army Regulation 381-12, Threat Awareness and Reporting Program*, 1993.

Department of the Army. *Threat Awareness and Reporting Program*, (AR 381-12), October 2010.

Department of the Navy. “Espionage Indicators.” NCIS Publications, March 2013.

Director of National Intelligence, “The National Intelligence Strategy of the United States of America,” August 2009.

Eric D. Shaw, Lynn F. Fischer, & Andree E. Rose, “Insider Risk and Evaluation,” Technical Report 09-02, August 2009.

Ernesto Londoño, "Pentagon Grapples to Understand how yet Another Insider Threat went Undeterred." *New York Times*, 03 April 2014, http://www.washingtonpost.com/world/national-security/pentagon-grapples-to-understand-how-yet-another-insider-threat-went-undeterred/2014/04/03/6cf43b3a-bafc-11e3-9a05-c739f29ccb08_story.html, 05 April 2014.

Gene Barlow, Office of the National Counterintelligence Executive, Interview: December 20, 2013, Topic: National Insider Threat Task Force and Insider Threat Working Group.

George Silowash, Dawn Cappelli, Andrew Moore, Randall Trzeciak, Timothy J. Shimeall, & Lori Flynn, "Common Sense Guide to Mitigating Insider Threats," CERT Program Report, December 2012

George Stukenbracker, Co-director of the NITTF, Federal Bureau of Investigations, Indirect Interview Conducted: December 20, 2013, Topic: Joint Insider Threat Task Force and Counterintelligence Working Groups.

Jennifer E. Sims, *Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence*, Georgetown University Press, December 2008.

John Hollister Hedley, "Learning from Intelligence Failures," *International Journal of Intelligence and Counterintelligence*, Volume 18, Number 3, 2005, pg. 436.

Joseph Lieberman. *A Ticking Time Bomb: Counterterrorism Lessons From The U.S. Government's Failure To Prevent The Fort Hood Attack.* U.S. Senate Committee on Homeland Security and Governmental Affairs, http://www.hsgac.senate.gov/imo/media/doc/Fort_Hood/FortHood Report.pdf?attempt=2, Washington D.C., February 2007.

Katherine L. Herbig, “Changes in Espionage by Americans: 1947-2007”, Defense Personal Security Research Center, Technical Report 08-05, March 2008.

Loch K. Johnson & James Wirtz, *Strategic Intelligence: Windows into a Secret World,* Roxbury Publishing Company, Los Angeles, 2004.

Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century* Philadelphia: University of Pennsylvania Press, 2008

Mark M Lowenthal, *Intelligence: From Secrets to Policy,* Washington DC: CQ Press, 2000.

Michael V. Hayden, “The State of the Craft: Is Intelligence Reform Working?” World Affairs, September/October 2010.

Michelle Van Cleave, “Myth, Paradox & The Obligations Of Leadership: Edward Snowden, Bradley Manning and the Next Leak,” Center for Security Policy, Occasional Paper Series. September 2013.

Mitchell D. Silber and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, New York City: NYPD Intelligence Division, 2007.

National Insider Threat Task Force. *National Insider Threat Policy.* Issued by President Barack Obama, November 2012.

National Insider Threat Task Force. *National Insider Threat Policy: Minimum Standards for Executive Branch Insider Threat Programs.* Issued by President Barack Obama, November 2012.

Nicholas Catrantzos, “No Dark Corners: Defending Against Insider Threats to Critical Infrastructures” Naval Post-Graduate School, September 2009.

Office of the Counterintelligence Executive, "The National Counterintelligence Strategy of the United States of America," 2009.

Office of the National Counterintelligence Executive, "Understanding Counterintelligence Core Competencies: Volume 1," National Counterintelligence Executive Office, January 2006.

Office of the National Counterintelligence Executive. "About the NCIX: Our Mission". http://www.ncix.gov/about/ about.php, 01 March 2014.

Office of the National Counterintelligence Executive. "What is Counterintelligence?" http://www.ncix.gov/about/ about.php, 01 March 2014.

Office of the National Counterintelligence Executive. *Terms & Definitions of interest for Counterintelligence Professionals.* October 2013.

Paul Pillar, *Intelligence and US Foreign Policy,* New York: Columbia University Press, 2011.

Pete Earley, *Confessions of a Spy: The Real Story of Aldrich Ames*, New York: G.P. Putnam's Sons, 1997.

President William J Clinton. *Executive Order 12968: Access to Classified Information.* August 1995.

RAND. "Domestic Terrorism." http://www.rand.org/topics/domestic-terrorism.html, 01 December 2013.

Richard J. Heuer, "The Insider Espionage Threat", Research on Mitigating the Insider Threats to Information Systems, RAND Corporation, Monterey, CA: Defense Personnel Security Research Center, 2000.

Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security,* New York: Columbia University Press, 2007.

Richards J. Heuer Jr., "Psychology of Intelligence Analysis," Washington, D.C.: CIA Center for the Study of Intelligence, 1999.

Robert M. Bryant, "The National Counterintelligence Strategy of the United States of America." Office of the National Counterintelligence Executive, 2009.

Ronald Reagan, "Executive Order 12333—US Federal Intelligence Activities." December 1981.

Senate Select Committee on Intelligence, "An Assessment of the Aldrich H. Ames Espionage Case and its Implications for U.S. Intelligence", US Government Printing Office: Washington DC, November 1994.

Steven R Band, Dawn Cappelli, Lynn F. Fischer, Andrew P. Moore, Eric D. Shaw, and Randall F. Trzeciak "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis" CERT Program, December 2006.

Sun Tzu, *The Art of War*, Filiquarian, 2006.

Terry Crowdy, *The Enemy Within A History Of Spies, Spymasters And Espionage*, London: Osprey Publishing, 2014.

The CERT Insider Threat Center, "Mission," http://www.cert.org/insider_threat/ 05 June 2012.

Thomas Noonan and Edmund Archuleta, "Insider Threat to Critical Infrastructure", *The National Infrastructure Advisory Council Final Report and Recommendations*, April 2008.

Tomas Precht, “Home Grown Terrorism and Islamist Radicalization in Europe”, Danish Ministry of Justice, Dec. 2007.

United States Congress, “National Counterintelligence Reform Act of 1994”, Senator Slade Gorton, May 1994.

United States Congress, “Counterintelligence Enhancement Act of 2002,” November 2002.

United States Department of Energy, “Office of Intelligence and Counterintelligence,” http://energy.gov/ office-intelligence-and-counterintelligence, 10 March 2014.

United States Department of State, “Counterintelligence Investigations”, http:// www.state.gov/m/ds/ terrorism/c8653.htm, 10 March 2014.

United States Government Printing Office, “United States Code, Title 18, Chapter 37: Espionage and Censorship”, December 2012.

USAF College of Aerospace Doctrine, Research, and Education. “Three Levels of War.” *Air and Space Power Mentoring Guide*, Vol. 1, Maxwell AFB, AL: Air University Press, 1997.

William E. Odom, *Fixing US Intelligence,* Yale University Press, 2003.

William H Webster, “Final Report of the William H Webster Commission on the Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas, on November 5, 2009,” Federal Bureau of Investigation Press Releases, 19 July 2012.

William Lind, Keith Nightengale, John Schmitt, Joseph Sutton, & Gary I. Wilson, “The Changing Face of War: Into the Fourth Generation” *Marine Corps Gazette*. October 1989.