SPIES LIKE US: A COMPARISON OF INFILTRATING NETWORKED TERRORIST ORGANIZATIONS VERSUS FOREIGN INTELLIGENCE SERVICES

A Thesis
Presented to the
Faculty of
San Diego State University

In Partial Fulfillment
of the Requirements for the Degree
Master of Science
in
Homeland Security

by
Edison H. Penaflor
Spring 2012
SAN DIEGO STATE UNIVERSITY

The Undersigned Faculty Committee Approves the

Thesis of Edison H. Penaflor:

Spies Like Us: A Comparison of Infiltrating Networked Terrorist Organizations

versus Foreign Intelligence Services

[Signatures]

Eric Frost, Chair
Homeland Security Program

Jeffrey McIlwain
Homeland Security Program

Patrick Papin
Department of Physics

12/9/20
Approval Date
Copyright © 2012
by
Edison H. Penaflor
All Rights Reserved
ABSTRACT OF THE THESIS

Spies Like Us: A Comparison of Infiltrating Networked Terrorist Organizations versus Foreign Intelligence Services
by
Edison H. Penaflor
Master of Science in Homeland Security
San Diego State University, 2012

During the cold war, the United States intelligence community was focused on addressing a specific intelligence threat: spies. One of the ways U.S. intelligence agencies alleviated this threat was by penetrating the adversary’s Foreign Intelligence Services. They learned that this was the most effective way in countering the threat. After September 11, the intelligence community focused on addressing a new threat: al-Qaida, a networked based terrorist organization. Traditional counterterrorism tools are insufficient in addressing the new threat.

The U.S. government is willing to bring to bear every tool at its disposal including the penetration of terrorist organizations. This thesis compares the infiltration of terrorist organizations versus Foreign Intelligence Services. It also discusses why terrorist organizations are much more difficult to penetrate and which methods that were previously employed against Foreign Intelligence Services are ineffective. This will enable the reader to realize that penetrating terrorist organizations require a different mentality as well as a tailored approach. Applying these conclusions will allow for more effective penetrations of terrorist organizations and minimal loss of life.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ABSTRACT</td>
<td>iv</td>
</tr>
<tr>
<td>2 ACKNOWLEDGEMENTS</td>
<td>vi</td>
</tr>
<tr>
<td><strong>CHAPTER</strong></td>
<td></td>
</tr>
<tr>
<td>1 INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>2 BACKGROUND</td>
<td>3</td>
</tr>
<tr>
<td>Fourth Generation Warfare</td>
<td>3</td>
</tr>
<tr>
<td>Hierarchy versus Networked Organizations</td>
<td>4</td>
</tr>
<tr>
<td>Al-Qaida Organizational Structure</td>
<td>5</td>
</tr>
<tr>
<td>3 HUMINT</td>
<td>8</td>
</tr>
<tr>
<td>Definitions</td>
<td>8</td>
</tr>
<tr>
<td>Importance</td>
<td>11</td>
</tr>
<tr>
<td>4 GENERAL DIFFERENCES</td>
<td>15</td>
</tr>
<tr>
<td>Recruitment</td>
<td>16</td>
</tr>
<tr>
<td>Motivations</td>
<td>23</td>
</tr>
<tr>
<td>5 CHALLENGES</td>
<td>29</td>
</tr>
<tr>
<td>6 CASE STUDY</td>
<td>39</td>
</tr>
<tr>
<td>7 RECOMMENDATIONS</td>
<td>47</td>
</tr>
<tr>
<td>Recruitment Position</td>
<td>47</td>
</tr>
<tr>
<td>Agent Types</td>
<td>48</td>
</tr>
<tr>
<td>Potential Agents</td>
<td>50</td>
</tr>
<tr>
<td>Access Agents</td>
<td>53</td>
</tr>
<tr>
<td>Agent Motivations</td>
<td>54</td>
</tr>
<tr>
<td>Collaboration with Allies</td>
<td>56</td>
</tr>
<tr>
<td>Conclusion</td>
<td>57</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>60</td>
</tr>
</tbody>
</table>
ACKNOWLEDGEMENTS

This thesis would not have been possible without my parents Edgardo and Annette. They believe that I can accomplish every endeavor I pursue. Their support enabled me to complete this thesis.

Lastly, I am grateful to Dr. Eric Frost and Dr. Jeffrey McIlwain. They are always there to provide support to their students.
CHAPTER 1

INTRODUCTION

The cold war represented an era where the battle lines between the two adversaries were in the realm of espionage. The United States’ intelligence agency, the CIA, was in constant battle with its adversary, the Soviet Union’s KGB. The main threat during this era was enemy spies. One of the ways to deal with the threat was to recruit an agent within the Foreign Intelligence Service (FIS) and learn the identity of its spies from within. September 11, 2001, represents the beginning of a new era where the United States has new adversaries: networked based terrorist organizations, more specifically al-Qaida. Terrorists are now the main threat. With the emergence of the new threat, the CIA now puts extra attention on using a tool that was effective in a previous era.

The purpose of this thesis is to explore the differences between attempting to infiltrate terrorist organizations versus Foreign Intelligence Services. This thesis examines if the CIA should simply adopt a copy and paste approach and employ the same strategies used against a previous adversary. This thesis will aim to answer the following questions:

1. Why are penetrating terrorist organizations different from Foreign Intelligence Services?
2. Why is it more difficult to penetrate terrorist organizations?
3. Which strategies would be effective against the new threat?

The 9/11 commission concluded that the events of that fateful day were due to various intelligence failures. The commission concluded as well that U.S. government agencies should move away from relying on technical means of intelligence collection and increase the capability of human intelligence collection. A successful penetration of a terrorist organization presents an invaluable human source of intelligence. The purpose of this thesis is to open the reader’s eyes to the mentality required in order to successfully infiltrate a terrorist organization. It is also to convey to the reader that a tailored approach is necessary which would allow for a more effective intelligence gathering on organizations considered impenetrable from human intelligence.
This thesis is derived from both primary and secondary source documents. The 9/11 commission report and other government reports served as a basis for determining the importance and the need for human intelligence. Former CIA employees such as Marc Sageman and Frederick Hitz provided the insights into which strategies they believe will and will not work against al-Qaida. This thesis also draws heavily on the interviews of the famous al-Qaida double agent, Humam Khalil Abu-Mulal al-Balawi, and his wife, Defne Bayrak. The interviews provided insight on the mentality of a terrorist espionage agent. The most significant limitation of this scholarly endeavor is the classified nature of the topic. Successful and unsuccessful penetration cases are publicly distributed on a limited basis because of the intelligence agencies’ goal of protecting its sources and methods.

Chapter Two of this thesis discusses networked terrorist organizations as a threat. It discusses the organizational structure of al-Qaida and its characteristics that affect the United States’ ability to collect intelligence. Chapter Three discusses the value of intelligence in counter terrorism and why penetration in particular is important. Chapter Four compares the general characteristics of terrorist groups and Foreign Intelligence Services as they relate to infiltration. It includes a comparison of the recruitment process for each group. It also includes a comparison of the motivational elements of spies versus terrorists. Chapter Five discusses the reasons why it’s more difficult to infiltrate terrorist organizations. Chapter Six discusses the case of al-Balawi, the extremist turned spy, turned terrorist. There are specific elements of the case that show the differences and the difficulties associated with penetrating terrorist groups. Chapter Seven discusses some recommendations that intelligence agencies may implement in order to alleviate the challenges discussed in Chapter five.

Although the title of this thesis is the penetration of networked terrorist organizations in general, the main object of this study is the terrorist organization al-Qaida. Al-Qaida’s organizational structure, employment of terrorism and the diverse Islamic cultural background of its members are the factors why it was chosen. Likewise, though the comparison is to Foreign Intelligence Services in general, the main object is the Soviet Union’s intelligence agencies namely the GRU and the KGB, now known as SVR. This thesis was written from the perspective of a friendly intelligence agency, mainly the CIA, due to the overseas nature of their mission and because the National Clandestine Service (NCS) is part of the CIA. The NCS presides over all human intelligence activity by the United States.
CHAPTER 2

BACKGROUND

This chapter discusses the new threat that the United States government and its intelligence agencies face. This chapter also discusses some of the characteristics of networked based terrorist organizations as they apply to penetration activities and why it is important to penetrate terrorist organizations.

FOURTH GENERATION WARFARE

There are different theories to describe the new era of conflict that we are experiencing in the world today. Lind and Hammes describe it as fourth generation warfare.\(^1\) However one describes the current conflicts in which the United States is involved, the underlying principles remain the same: state versus non-state actor, use of asymmetric warfare including terrorism, centralized versus decentralized organization, and use of information operations especially media outlets.\(^2\) The organizational structure of a non-state actor can be either hierarchical or networked.\(^3\)

This thesis will focus on infiltration of networked organizations and will use hierarchical organizations as a basis of comparison.

Before examining the organizational structure of a non-state actor, we must first look into the tactics that they use in order to pursue their goals. One of the tactics non-state actors use is terrorism. Terrorism, as defined by Bruce Hoffman, “is the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political


change.”\textsuperscript{4} The use of terrorism is significant because it will present problems in terms of a successful infiltration. The next chapter will closely examine the elements that make successfully penetrating a networked based terrorist organization difficult.

**Hierarchy versus Networked Organizations**

Networked organizations have advantages over hierarchical organizations despite having less manpower and resources. According to Arquilla and Ronfeldt, “hierarchies have a difficult time fighting networks.”\textsuperscript{5} Some of the examples used were the Drug Trafficking Organizations in Columbia, religious revivalist movement in Algeria and the Zapatista movement in Mexico. A networked organization’s shared principles, interests and goals determine the group’s effectiveness. The organization must share deeply in either doctrine or ideology in order for it to be effective. This allows for each member to think alike and for decentralized execution of their missions as well.\textsuperscript{6} “In addition to ideological training, al-Qaida provided these associate groups with military expertise, religious-political indoctrination and terrorist-guerilla training, thereby significantly improving their guerrilla and terrorist capabilities.”\textsuperscript{7} Considering that networked based terrorist organizations have an advantage over hierarchical organizations, their ability to execute without central authority and the possibility of acquiring weapons of mass destruction, it is crucial that the United States use all available means necessary, including penetration, to mitigate this threat.

In terms of counterintelligence (CI), Gleghorn argues that networked based organizations have no advantage over hierarchical organizations. “Whether the organizations that pose a threat to the U.S. are networked, hierarchical or some hybrid form, and regardless of whether they are state or non-state entities, the task at hand for counterintelligence does not change.”\textsuperscript{8} This is true in counterintelligence as a whole. Whether an individual’s motive

\textsuperscript{4} Hoffman, Bruce. *Inside Terrorism.* (New York: Columbia UP, 2006), 40.

\textsuperscript{5} John Arquilla and David Ronfeldt. *Networks and Netwars: The Future of Terror, Crime and Militancy* (Santa Monica: RAND, 2001), 15.

\textsuperscript{6} Ibid., 15.


is to inflict casualties or to collect intelligence, it is CI’s goal to prevent these individuals from accomplishing their mission. Chapter two discusses that counterintelligence has many aspects and the penetration of organizations is only one of them.

**AL-QAIDA ORGANIZATIONAL STRUCTURE**

Before the successful penetration of a transnational non-state actor can be accomplished, a close examination of its organizational structure must be done first. Al-Qaida and several transnational terrorist groups are organized in networks. Within this network, there are different groups each of which has its own function. The first group in al-Qaida is the core group. The core group includes senior leadership, organizational commanders, and their trusted associates. This group is built on close personal relationships.  

The second group is the structural cells. Structural cells provide “specialized” functions for al-Qaida. Functions such as military operations, terrorist operations, fundraising, financial management, technology support, intelligence, political and psychological operations support, etc. Because of their respective functions, they are required to be in a more “urbanized and globalized environment.” Structural cells embedded into society are knowledge-base specific. The relationship between the support cells and the core group is described as “the core group acting like a token-ring network topology.”

Another group in a network type terrorist organization is the operational cells. Each cell has a commander. The commander and each member are “comcon” - completely and continually connected. The commander makes contact with individuals outside of the cell, such as the core group or support cells. External contacts are kept to a minimum. The individuals in operational cells are observed during their training by the core group. This

---


10 Ibid., 9.
serves as their “vetting” process and protects their organization from potential moles.\textsuperscript{11} Each cell can have two to fifteen members.\textsuperscript{12}

And finally, terrorist organizations that are network based also have what is labeled as support networks. Al-Qaida mainly uses support networks for their source of technology, fundraising and for other financial activities. They can be either unaware of their support to al-Qaida by means of secondary/tertiary networks,\textsuperscript{13} or they can be sympathizers that do not commit terrorist acts but provide financial, logistical, political and legal support.\textsuperscript{14}

After examining the different types of groups present in a networked terrorist organization, the ties between the groups must be examined as well. J. A. Rodriguez, in his social network analysis on the March 11, 2004, Madrid bombings, concluded that there were three kinds of ties that connected the terrorists together:

1. Binding ties: kinship, friendship, personal contacts.
2. Repeated interaction in particular settings: The Telephone Calling Shop, living together.
3. Reliability ties: Al Qaida relations, training in Afghanistan and Pakistan, participation in the War in Chechnya, involvement in terrorist actions prior to March 11th (such as an action against the Spanish consulate in Casablanca in 2003, or the Sept 11th attacks), and membership in Al Qaida.\textsuperscript{15}

How the groups communicate with each other is also a significant characteristic of a networked terrorist organization. Ayman al-Zawahiri heavily influenced the structure of an al-Qaida cell. The network is based on the model of the Islamic group of Egypt and the Egyptian Islamic Jihad. Special mission cells such as the cells from 9/11 and the Los Angeles airport millennium attack have an agent handler that coordinates the mission.\textsuperscript{16}

\begin{itemize}
\item[\textsuperscript{11}] Ibid., 9.
\item[\textsuperscript{12}] Gunaratna, \textit{Inside Al Qaeda}, 97.
\item[\textsuperscript{13}] “Decision Support Systems, Inc.,“Hunting the Sleepers,” 10.
\item[\textsuperscript{15}] J. A. Rodriquez, “The March 11th Terrorist Network: In its Weakness Lies its Strength,” (lecture, XXV International Sunbelt Conference, Redondo Beach, CA, February 2005).
\item[\textsuperscript{16}] Gunaratna, \textit{Inside Al Qaeda}, 97.
\end{itemize}
Al-Qaida uses a four tier courier system which includes their leadership. Osama Bin Laden’s location was found through the successful efforts of U.S. intelligence in tracking Abu Ahmed al-Kuwaiti, Bin Laden’s personal courier.\textsuperscript{17} Al-Qaida leadership minimizes their communications through cell phones, satellite phones and emails due to being monitored by Foreign Intelligence Services.\textsuperscript{18}

Al-Qaida’s courier system is so sophisticated that there are different networks for each type of message passed to other groups. There is an administrative courier network, an operational courier network, a media courier network and a final courier network. Senior leadership uses the final courier network for communicating with each other. The trusted couriers have the ability to memorize the messages verbatim which adds more security. Al-Qaida’s courier system and the network sophistication increases the importance of Human Intelligence (HUMINT) in the intelligence collection on networked terrorist groups and demonstrates the limits of other intelligence disciplines such as Signals Intelligence (SIGINT) and Imagery Intelligence (IMINT).\textsuperscript{19}


\textsuperscript{18} Seth G. Jones and Martin C. Libicki, \textit{How Terrorist Groups End: Lessons for Countering Al Qa’ida.} (Santa Monica: RAND, 2008), 129.

\textsuperscript{19} Ibid., 130.
CHAPTER 3

HUMINT

The previous chapter examines the characteristics of a networked based terrorist organization such as al-Qaida. This chapter examines the significance of a weapon that the United States is not properly utilizing: penetration. But before examining the significance of penetration, this thesis will distinguish some of the terms in intelligence so that the role of penetration can be better understood.

DEFINITIONS

The use of individuals is necessary in order to penetrate a terrorist organization. With that requirement, infiltration automatically falls under the realm of HUMINT. HUMINT is the intelligence collected from human sources.\textsuperscript{20} The sources could be friendly, hostile or neutral, and they may or may not know that they are providing information to a friendly or hostile intelligence organization. Some examples include: Advisors, military attachés, espionage sources, Non-Governmental Organizations, prisoners of war, and routine patrolling by friendly forces. This thesis focuses on espionage sources.

Espionage is only one part of HUMINT. Espionage or spying involves individuals obtaining information that is considered secret or confidential without the permission of the holder of the information. Because a spy’s mission is to obtain information without permission, it is generally clandestine in nature. Clandestine means that their actions are unnoticed by the other party. This chapter analyzes the importance of intelligence received from espionage sources. The human sources could be agents planted in the terrorist organization, defectors from the organization or special recruits from the organization’s

social or logistical frameworks.  

Counterintelligence (CI) is another discipline of intelligence that deals with terrorism. Counterintelligence, as practiced by most states, is the effort to protect their secrets, to prevent themselves from being manipulated, and (sometimes) to exploit the intelligence activities of others for their own benefit. Executive Order 12333, which outlined the powers and responsibilities of U.S. intelligence agencies, defines it as: “Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs.” It is the CI’s mission to prevent unauthorized individuals from either conducting espionage or terrorist attacks.

Counterespionage (CE) is the sub-discipline of counterintelligence which specifically deals with catching spies. The Army defines it as the “aspect of counterintelligence designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities.” Espionage describes the operations that U.S. agencies conduct to try to penetrate terrorist organizations. Counterespionage, on the other hand, describes the operations that U.S. agencies conduct to catch terrorists trying to penetrate U.S. agencies.

There are two types of counterintelligence operations: defensive counterintelligence and offensive counterintelligence. Defensive counterintelligence operations are aimed at one’s own organization in order to look for weaknesses that can be used by either a spy or a

---

22 Roy Godson, Dirty Tricks or Trump Cards: U.S. Covert Action & Counterintelligence. (New Brunswick: Transaction, 2001), 2.
terrorist. On the other hand, offensive counterintelligence operations are more aggressive and are “aimed at neutralizing or exploiting the activities of hostile intelligence service or terrorists.”\textsuperscript{25} Organizations performing offensive counterintelligence operations also attempt to infiltrate adversarial organizations for the purpose of disrupting the enemy’s activities.

Counterterrorism is another mission of U.S. intelligence agencies. It is defined by the military as “Operations that include the offensive measures taken to prevent, deter, preempt, and respond to terrorism.”\textsuperscript{26} By its strict definition, the penetration of terrorist organizations falls under counterterrorism. However, most of the operations that require the infiltration of either Foreign Intelligence Services (FIS) or terrorist organizations fall under either HUMINT or counterintelligence.

For the purpose of this thesis, it is acknowledged that the mission of penetrating terrorist organizations is technically a counterterrorism mission, but it is usually conducted by U.S. intelligence agencies that perform HUMINT and counterintelligence missions. The difference with an infiltration of an FIS or a terrorist organization between a HUMINT and a counterintelligence mission lies in the purpose of their penetration. HUMINT operations seek to understand an FIS or terrorist organization’s interest or intentions while counterintelligence operations seek to disrupt the FIS or terrorist organization’s activities by either neutralizing or manipulating their operations.\textsuperscript{27}

For the next chapters, the infiltration of FIS or terrorist organizations referred to in this thesis falls under the mission of counterintelligence. Disrupting a terrorist attack or a leak of intelligence that can cause serious damage to the United States has precedence over the mission of learning an adversary’s interest. “The other side of the CI coin—counterespionage—has one purpose which transcends all others in importance:


\textsuperscript{27} Gleghorn, “Exposing the Seams,”11.
While this thesis will mainly discuss the penetration of terrorist groups through the mission of counterintelligence, it should be noted that the analysis and findings in this thesis can be applied to penetration through the mission of HUMINT also known as “positive” intelligence.

**IMPORTANCE**

Now that the roles that different intelligence disciplines play in the infiltration of terrorist groups are better understood, this thesis will discuss the significance of the intelligence received from a successful penetration of a terrorist organization. Intelligence in general is significant in the fight against terrorism. Seth Jones and Martin Libicki conducted a study of 648 terrorist groups that existed between 1968 and 2006. They concluded that terrorist organizations ended for two reasons:

1. 43 percent of the time, members decided to adopt non-violent tactics and join the political process; and
2. 40 percent of the time, local police and intelligence agencies arrested or killed key members of the group.29

Clearly, intelligence is a vital resource in combating terrorism. “The prerequisite for a successful counter-terrorism response is the highest caliber intelligence gathering, analysis, co-ordination, and dissemination.”30 Having good intelligence also allows more flexibility in the political actions the U.S. government can take in the fight against terrorism. “The better your intelligence, the more you can diminish or limit the force of the other weapons you employ against terrorism.”31

The importance of HUMINT in the realm of intelligence cannot be overstated. Specifically, human sources in the fight against terrorism are extremely valuable. “The traditional and emerging transnational (Tier A) threats demand a reinvigorated application of

---


30 G. Davidson Smith, *Combating Terrorism* (London: Routledge, 1990), 150.

human intelligence.” As it was mentioned in the last chapter, networked terrorist organizations are becoming increasingly aware of the U.S. government’s ability in collecting intelligence using technical means. In contrast, the terrorists have developed a courier system and minimized the use of electronics as a means of communication. With the decreasing effectiveness of SIGINT and IMINT in the war against terrorism, this proportionally increases the importance of HUMINT.

Intelligence contributes significantly in counterterrorism operations. David Charters divides the contribution of intelligence into three categories: warning intelligence, operational intelligence, and criminal-punitive intelligence. The goal of early warning intelligence is to provide the appropriate law enforcement or intelligence agency with the time to prepare the possible targets in order to prevent the attack from succeeding. Operational intelligence provides agencies the information needed to identify and locate terrorist organizations and their support networks. Operational intelligence “allow[s] them to plan operational measures against the terrorists.” Criminal-punitive intelligence is the intelligence needed in order to prosecute the terrorists in court.

The three categories described by Charters can be achieved through the successful penetration of a networked based organization. A well placed source will be able to provide early warning intelligence. The individual can warn the appropriate security force once he/she learns of the group’s intentions. However, there are some issues and concerns regarding using a source for early warning intelligence. There is a possibility that the identity of the source might be compromised. The concerns regarding the infiltration of terrorist groups will be discussed in the next chapter.

A successful penetration will also be able to provide operational intelligence. The source can provide the identity of the members of the organization as well as their location. The agency handling the source can then use the intelligence to conduct offensive operations against the group. The source’s ability would depend on the success of the infiltration and the

---

terrorist group’s organizational structure. In the case of al-Qaida, even with a successful penetration, there would be limited operational intelligence that can be provided because of its networked structure. Even if the source has successfully infiltrated the operational cell, his/her ability to provide intelligence on other cells and the core group would be limited.³⁴

Finally, an infiltration of a terrorist group could also provide criminal-punitive intelligence. Unfortunately in the case of al-Qaida, there is sufficient intelligence to prosecute the leadership without an inside source. This situation is unfortunate because it presents the challenge that terrorist groups present against intelligence agencies. A terrorist organization is not usually in their radar until after they have successfully attacked a target. A successful infiltration’s criminal-punitive value would be dependent on the source’s ability to determine the group’s intentions and have the ability to provide sufficient intelligence to prosecute the organization prior to a successful attack occurring.³⁵

Similar to HUMINT’s significance in intelligence, penetration of an adversarial organization is valuable in intelligence as well. The first reason it is important is that there is no way for the enemy’s organization to prevent it completely. As we have learned in the cases of Aldrich Ames and Robert Hanssen, even organizations that have robust security are vulnerable to penetration. As long as people are involved, there is no defense against penetration. Another reason is because it will provide U.S. intelligence agencies the adversary’s intentions and actions. “The only way to be sure that an enemy has been contained is to know his plans in advance and in detail.”³⁶

Another reason penetration is important in intelligence and specifically in counterintelligence is that this is the only way to find out if our own organizations have been penetrated. If a terrorist organization has been infiltrated, the individual inside will have access to the group’s intelligence. He/she can then pass the information to our intelligence agencies and from there, the agencies can determine if the terrorist organization has successfully penetrated U.S. intelligence agencies. Counter-espionage operations heavily rely

³⁴ Ibid., 230-233.
³⁵ Ibid., 230-233.
³⁶ Matschulat, “Coordination and Cooperation in Intelligence.”
on penetrations. “Conducting CE without the aid of penetrations is like fighting in the dark. Conducting CE with penetrations can be like shooting fish in a barrel.”37

37 Ibid.
CHAPTER 4

GENERAL DIFFERENCES

After examining, in the previous chapter, the role and significance of the infiltration of terrorist groups in the fight against terrorism, this chapter will now compare and contrast Foreign Intelligence Services (FIS) and networked terrorist groups. This chapter will analyze the recruitment process for both FIS and terrorist groups. A thorough understanding of the recruitment process will provide a good basis to understand how terrorist groups are infiltrated. This chapter will also examine the motivations for both spies and terrorists. The difference in the motivation of spies and terrorists provides a glimpse into the differences in the infiltration of FIS and terrorist groups.

The first and most significant difference between an FIS and a transnational terrorist organization is the group’s objective. An FIS’s main purpose is to collect intelligence. Intelligence agents may be ordered to perform other activities as well such as sabotage and assassinations. However, intelligence agents collect intelligence first and foremost. Their main concern is to protect sources and methods. Their philosophy is to get the most benefit for their home country.  

The main purpose of a terrorist group, on the other hand, is to use violence to undermine their adversary. Members of terrorist groups may conduct other missions such as collecting intelligence; however, all their activities will culminate in an attack or a series of attacks. Their philosophy is to inflict the most damage to their adversary.  

The differences in their respective objectives are closely tied to their intelligence collection practices. The intelligence requirements of terrorist groups are perishable. This means that the intelligence that they require to conduct their attack is more often likely to change. Most of the intelligence activities of terrorist groups are directed against their

adversary’s physical security. There is always the likelihood that the security procedures will be changed in response to new threats. Moreover, there is always the possibility that the group’s intentions might be discovered, in which case the intelligence is useless.\textsuperscript{40} 

In contrast, for an FIS the value of a source is more towards the long term. Their intelligence requirement is to learn the adversary’s intentions. It is in the intelligence agency’s best interest to continue to learn their adversary’s thoughts and intentions. The possibility also exists that the source can be compromised such as the case with terrorist groups, which is why it is the intelligence service’s first priority to protect their sources and methods. \textsuperscript{41}

**RECRUITMENT**

The next step in comparing and contrasting Foreign Intelligence Services and transnational terrorist groups is to analyze the recruiting process employed by each group. In order to properly understand the effectiveness of cold war espionage tradecraft applied to transnational terrorist groups, the terms and definitions must be identified first. The focus will be on the definitions of the individuals involved in espionage.

Starting from the broadest term, an individual that obtains intelligence for an intelligence service is called either an agent or an asset. The term agent is normally used for individuals that are more involved in the espionage process. They are either in high positions within the government or military, or they are involved in deception activities. The agents involved in deception activities will be discussed further in this chapter. Agents can be considered either witting or unwitting, and in some cases, willing or unwilling. The term asset is generally used for individuals that have limited access to the adversary’s plans and intentions.\textsuperscript{42}

In the United States, the individuals that recruit and manage agents are called case officers. They are also referred to as agent handlers. These individuals are the intelligence

\textsuperscript{40} Gleghorn, “Exposing the Seams,” 37.


officers that work for their respective country’s intelligence services. Case officers conduct collection activities as well; however, their primary purpose is to manage human agents and human intelligence networks.\(^{43}\)

Once a case officer recruits an agent, there are different ways the agent can be classified. The first type is the mole. A mole is a type of agent that is recruited prior to gaining access to valuable intelligence. In our case, a mole is originally loyal to the United States before joining either a terrorist group or a Foreign Intelligence Service. Because moles collect intelligence, they are agents. However, not all agents are considered moles.\(^{44}\)

Sleepers are moles as well. “‘Sleepers’ are covert operatives, individuals or ‘cells’ (small, compartmentalized groups) infiltrated into a target country and community, waiting for a time or the signal to strike. Sleepers represent a key weakness in Western society, but something that also provides strength—individuals are generally trusted until a reason is demonstrated that such an assessment is flawed.”\(^{45}\) For espionage, a sleeper mole is defined as one “who may enter a service, possibly at a young age, but definitely not reporting or doing anything that would attract suspicion, until reaching a senior position.”\(^{46}\) The term sleeper is widely used both in referring to terrorists and spies.

Another type of agent is the defector. Defectors are individuals who decide to leave their own organizations and provide intelligence to the United States. What distinguishes defectors from moles are that moles start out with loyalty to the United States before gaining access to valuable intelligence, while defectors already have access to valuable intelligence before making the decision to change their loyalty to the U.S. A defector in place is an individual with access to intelligence when he or she decides to change his or her loyalty. But instead of leaving their home country organization, they are convinced to stay in the organization and continue providing intelligence to the United States.\(^{47}\)

\(^{43}\) Ibid., 13.

\(^{44}\) Ibid., 29.


\(^{46}\) IPB USA, \textit{U.S. Military Intelligence Handbook}, 29.

\(^{47}\) Ibid., 29.
As part of counterintelligence operations, moles are discovered within the organization. Instead of prosecuting some of these individuals, they are convinced to switch loyalties. They are either asked to spy for the United States instead or provide erroneous intelligence to the adversary group. These individuals are labeled double agents. To take it further, when double agents are discovered, and convinced to change loyalties, they are labeled triple agents. The rule of thumb is that when an agent switches loyalty once, he or she is called a double agent. If he or she switches loyalty twice, the term triple agent is used and so on and so forth. 48

A significant difference between terrorist groups and Foreign Intelligence Services is the need for recruits. Terrorist groups constantly need recruits. Groups would keep their recruitment process ongoing because of attrition from counterterrorism forces. They would eventually lose members from kinetic operations, detainment, or from desertion. Terrorist groups may also need to recruit because they lack the resources and manpower to accomplish their political or religious goals. Terrorist groups that use suicide attacks as a tactic would regularly require recruits even if they are successful in their missions. Whether terrorist groups have to recruit to replenish their manpower or to expand their operations or support base, this presents a vulnerability that can be exploited. Terrorist groups are susceptible to recruiting an agent that works for an intelligence agency. 49

FIS, on the other hand, do not recruit as much because they do not experience as much turnover as terrorist groups. Other intelligence disciplines could be able to compensate for the reduction of HUMINT. However, the other intelligence disciplines would not be able to eliminate the need for HUMINT. 50 United States intelligence prior to 9/11 relied heavily on technical intelligence collection. This was during the time when spies such as Robert Hanssen and Aldrich Ames were discovered. There was an overall feeling of skepticism


50 Jeffrey Richelson, The U.S. Intelligence Community (Boulder: Westview, 1999), 257.
towards human sources. Unfortunately, the intelligence community learned the hard way that the need for Human Intelligence cannot be eliminated.

Besides having other intelligence disciplines to pick up the slack, another reason FIS do not require as many recruits is because of the attrition rates. Counterintelligence organizations are constantly searching for spies much like counterterrorism organizations are searching for terrorists; however, by the nature of the tactic that each group uses to accomplish its goal, the attrition rate is much higher for terrorist groups. Terrorist groups, by definition, use terrorism to accomplish their goals. Terrorism uses fear as a result of violence to accomplish political goals. The success of their mission depends heavily on recognition of the terrorist attacks. This makes the group visible to counterterrorism forces. On the other hand, espionage, by definition, requires clandestine activity. Their purpose is to collect intelligence without detection by counterintelligence agencies. A successful suicide bomber would have to be replaced right away, while a successful agent would never have to be replaced.

In order to fully understand the recruitment process for both groups and to examine the potential for infiltration, this thesis will now look into the recruitment qualifications for both terrorist groups and FIS. According to the al-Qaida training manual, the following are the necessary qualifications and characteristics for the organization’s members: Islam, commitment to ideology, maturity, sacrifice, listening and obedience, keeping secrets and concealing information, free of illness, patience, tranquility and "unflappability," intelligence and insight, caution and prudence, truthfulness and counsel, ability to observe and analyze, ability to act, and to change positions and conceal oneself.\footnote{\cite{al_qaida_manual}}

Victor Suvorov described the Main Intelligence Directorate (GRU) conditions for agent recruitment:

A candidate for recruitment must fulfill the following conditions: he must have agent potential that is he must be in the position to provide information of real use to the GRU, either to steal or copy secrets, to communicate secret information by word of mouth, or to recruit new agents. There must exist motives by means of which he may be recruited — displeasure with the regime or other political

\footnote{\cite{al_qaida_manual}}
motives, personal financial problems, or private motives like a desire for revenge on somebody or secret crimes which he is trying to hide. It is desirable that he be sympathetic to communism without being a communist. Communist parties everywhere have been compromised to a certain extent by their contacts with the KGB and the GRU, and it is always recommended that agents recruited from communist parties should leave the party.\(^5^2\)

The qualification requirements for both groups can be essentially divided into two categories: the recruit’s ability to accomplish the mission and the recruit’s adherence to the group’s control or guidance. Al-Qaida’s qualifications are geared towards the recruit’s ability to be a successful sleeper agent. Characteristics such as patience, tranquility, caution and ability to act, change positions and conceal oneself, are all crucial for a successful sleeper agent. On the other hand, access to vital information and the ability to pass the information is essential for an espionage agent. The difference in the qualifications is that for terrorist organizations, the ability to accomplish the mission is more internal. That means that the qualities listed above are based on the individual’s personal abilities. On the other hand, the ability of an espionage agent is more dependent on their position in the government or military. As long as the agent can practice sufficient operational security, the agent’s ability to accomplish the mission will not be dependent on the individual’s personal ability. Both groups list qualities that are essential to keep the agent or terrorist in line with the organization’s objectives. The difference is that for al-Qaida, the recruit must already be a firm believer in the ideology. For a Foreign Intelligence Service, the motives for the recruit to spy on their own country must just be present. It is not necessary for the recruit to have loyalty to the foreign country to start the recruiting process. Another difference between the two groups in recruiting qualifications is the formal membership in the ideology. For al-Qaida it is required for the recruit to be a Muslim. On the other hand, the GRU prefer that the recruit is not a member of a Communist party.

There is also a significant difference in the recruiting process between terrorist organizations and FIS. Recruitment in terrorist organizations is described as a bottom-up process. It begins way before contact with the terrorist organization. Recruiting begins with

contact with family and friends. “About 75 percent of mujahedin had preexisting social bonds to members already involved in the global jihad or decided to join the jihad as a group with friends or relatives.” Mosques also play a big role in the social ties prior to recruitment. The friendship bonds are usually formed in Mosques when members interact with each other and see they have similar Islamic ideology. Tribal and family connections are significant in exclusion from membership as well. Al-Qaida has traditionally avoided Algerian recruits because they believed that the Algerian intelligence has infiltrated the terrorist groups in the country.

Once the group becomes a “bunch of guys,” they now look to join jihad. The group looks for someone, preferably someone they know, that has ties to a terrorist organization. The individual that has ties to a terrorist organization then arranges for the group to meet and train with the organization. The group of friends will be evaluated by members of the organization to determine if they could be tasked with future operations. Al-Qaida is selective when it comes to their recruitment. Only 15 to 20 percent of prospective Muslim recruits are selected to go to Afghanistan for training.

Contrary to the terrorist recruitment process, Foreign Intelligence Services prefer to initiate the recruitment process. They prefer to recruit agents that they have targeted for selection and scouted instead of recruiting agent “walk-ins.” The recruitment process discussed in this chapter will be primarily based on the GRU. However, the CIA employs the same process. The process of recruiting espionage agents is called the recruitment cycle.

The first step of the recruitment cycle is called spotting. Spotting is the step in which potential recruits are identified. The case officer will try to make contact to obtain basic information so that analysts can extract information about the potential recruit from their

---

54 Whitlock, “After a Decade at War With West.”
55 Sageman, *Understanding Terror Networks*, 70.
databases. Spotting typically occurs during embassy functions, conferences and other normal activities.\(^{57}\)

Once an individual has been identified as a potential recruit, the FIS will learn everything they can about him or her. This step in the process is called assessing. Intelligence agencies will try to evaluate the potential recruit’s ability to provide valuable intelligence. They will conduct background checks and surveillance so that they can learn the potential recruit’s daily routine. Based on the information gathered on the potential recruit, the FIS will assess his/her vulnerabilities. They will determine the motivations they can use to convince the recruit to spy for them. The potential recruit having financial problems would be an example. Intelligence agencies will compare the recruit’s possible value to the risks associated in making the recruitment pitch.\(^{58}\)

After identifying a vulnerability that the FIS can use against the potential recruit, they will now “cultivate” the perceived vulnerability. This step in the process is called development. If the individual has financial problems, he/she will now experience a string of “bad luck” that will exacerbate the problems. The case officer can contact the potential recruit before or after the development process begins. After establishing contact with the potential agent, the case officer will decide when to make the pitch and which approach to use. The two types of approach that intelligence agencies use are the gradual and the crash approach. The crash approach is when the officer makes the recruitment pitch right away with minimum contact.\(^{59}\)

For the gradual approach, the case officer will start the recruitment step of the cycle by offering gifts for small favors. The favors will be small and insignificant at first. This is just to establish the relationship between the agent and case officer. The case officer just wants the agent to get used to being asked for favors while being compensated. The compensation will be disproportional at first. The value of the information the agent provides is not worth the money that he is being paid for. Eventually the case officer will ask for

\(^{57}\) Ibid.
\(^{58}\) Ibid.
\(^{59}\) Suvorov, “Agent Recruiting.”
unauthorized information and force the agent to comply. The intelligence officer can threaten to report the agent that he has been providing information to a foreign intelligence agency.\textsuperscript{60}

Hundreds of people every year walk into the Soviet/Russian embassies offering information or services. Most of the time, the information that is offered to them is useless. Sometimes, the walk-in is just a reporter looking to write a story. There is also a possibility that the walk-in is an officer of an adversarial intelligence agency who is trying to identify the intelligence officers in the embassy. A walk-in recruit that actually has value would drop off material that shows his/her access with instructions on how to contact him/her at a later time. The embassy turns them down and tells them, “This is a diplomatic representation and not an espionage centre. Be so kind as to leave the building or we will call the police.”\textsuperscript{61}

The root difference in the recruitment process between terrorist groups and FIS lies in their attitudes towards walk-ins. For terrorist groups, walk-ins are the preferred method of recruitment. It is the recruit that initiates contact with the organization. For FIS, the organization prefers to initiate the contact. They view walk-ins with skepticism. In fact, officers that worked for the Soviet Union know the living conditions in their country and view a person that willingly offers their services for a communist country with disgust. On the other hand, terrorist organizations more than welcome volunteers and praise them in public.

**Motivations**

Part of the recruitment process for an espionage agent, as previously discussed, is to determine the agent’s potential motivations for spying. The common theory used to describe motivations for spying is the acronym MICE. MICE stands for Money, Ideology, Coercion and Ego. This thesis will use seven motivations for espionage, an expanded version of MICE: ideology, money, revenge, blackmail, friendship, ethnic or religious solidarity, and love of espionage for its own sake. A single motivation can be enough to convince an agent to spy on their country. However, agents that commit espionage usually have a combination

\textsuperscript{60} Suvorov, “Agent Recruiting.”

\textsuperscript{61} Ibid.
of motivations. One motivation is the primary reason, and the other motivations would be secondary.62

Ideology is the set of ideas that constitutes one's goals, expectations, and actions. During the cold war, the competing ideologies were Soviet communism versus Western capitalism. Agents that spied for the Soviet Union during the cold war believed in communism. Agents that spied for Western countries disagreed with communism. One thing that must be pointed out is that even if the potential recruit agrees with a foreign power’s ideology, it doesn’t automatically mean that individual will spy against their own country. “There is a considerable gap between commitment to an ideology, even one that espouses the violent overthrow of a government to which one owes allegiance, and the commitment actually to spy under the direction and control of a foreign power.”63

Money is the most misunderstood of all the motivations. Inexperienced case officers believe that agents commit espionage for a foreign country in exchange for money as part of a financial transaction. Some case officers believe that they are purchasing the intelligence from the agents. In reality, case officers are selling a lifestyle. In the case of Robert Hanssen, he gave secrets to the Soviet Union so that his kids could go to private school. In that example, the officers were selling private school in exchange for Hanssen’s services.

Frederick Hitz described money as a motivation for spying:

It is the essential lubricant of this clandestine form of commerce. If the truth be known, most intelligence services prefer it that way. They consider it a fee for services rendered, without the complications of faith in a given system or ideology. It is less messy.64

Like any other company, intelligence agencies have to deal with disgruntled employees. Intelligence officers spy for other countries as an act of revenge for various reasons such as being passed over for promotion and being wrongfully terminated. These officers believe that they are not properly recognized for their abilities and they commit espionage as a means of retribution. Robert Hanssen was the poster boy for espionage as

---

63 Ibid., 26.
64 Ibid., 34.
revenge. He was an FBI Special Agent that worked in the Counterintelligence division. Although he was knowledgeable in Information Technology, he was never included in the FBI’s inner circle. Psychiatrists who interviewed him believed that he spied as a means to show his wife and his father that he would amount to something. Hanssen never believed in communism and his payment was disproportionate to the value of the intelligence that he was providing.\textsuperscript{65}

Western intelligence agencies typically stay away from using coercion as a tool to convince recruits to spy for them. This is not because of moral reasons but simply because U.S. and British intelligence agencies have learned that coercion doesn’t work. On the other hand, the former Soviet Union used blackmail as a means to motivate agents effectively. Coercion was effective for the former Soviet Union because once a western government or military personnel is engaged in extramarital relationships, their career is practically over. In contrast, if government or military personnel for the Soviet Union are engaged in extramarital relationships, it does not have a negative effect on their careers. Former Soviet Union Intelligence agencies use female recruits called “swallows” to seduce American personnel. Western personnel working in overseas assignments are lonely and isolated and typically vulnerable to seduction.\textsuperscript{66}

Once an individual that has access to valuable information has sexual relations with a foreigner, he is subject to blackmail. Western personnel working in a foreign country must report any contact with foreigners and are subject to dismissal or reassignment. This is especially true for married individuals. Intelligence agencies have learned that contact with foreigners present a significant security risk and must be avoided. An example of “honeypot” recruitment was Irvin Scarbeck. He was a U.S. Diplomat working at the U.S. Embassy in Poland. He was involved in an affair with a Polish woman. The Polish intelligence took pictures of Scarbeck in a compromising situation and used the pictures to blackmail him into providing information.\textsuperscript{67}

\textsuperscript{65} Ibid., 43.
\textsuperscript{67} Frank J. A. Rafalko, Post World War II to Closing the 20th Century (1-435), Vol. 3 of A Counterintelligence Reader (Washington, DC: Office of the National Counterintelligence Executive, 2004),
Espionage motivated by friendship relies on existing relationships between the case officer and the potential recruit. Case officers can take advantage of their relationship with the potential agent and can ask the agent for favors. Friendship is a significant contributor when recruiting intelligence officers of another country. Case officers meet with known intelligence officers from an adversarial agency and they give each other intelligence in a *quid pro quo* relationship. The temptation for recruitment based on this relationship becomes strong.  

Sometimes the previously mentioned reasons are insufficient to explain an agent’s motivation for committing espionage. Agents sometimes commit espionage due to the excitement that goes along with it. Robert Hanssen hated his FBI colleagues and needed money to send his children to private school. Frederick Hitz believed that Hanssen continued his espionage activities because he felt “invincible.” When Hanssen was part of the FBI’s counterintelligence division, he was tasked with finding the mole that compromised agents during 1985 and 1986. In fact, he was the mole. Hanssen believed he was smarter than his colleagues and enjoyed the position that he was in. When he was captured, he said, “What took you so long?”  

Espionage for the sake of spying is one of the less documented motivations but it is nevertheless significant in the recruitment process. Frederick Hitz believed that the potential recruit’s reception of the game of espionage is a significant prerequisite to their recruitment.

> [O]ne of the qualities the CIA must be looking for in its pursuit of individuals prepared to betray their friends, family, professional associates, and country to spy for us is a relish for the game of espionage itself. More than (or in addition to) money, sex, ideology, friendship, revenge, or ethnic solidarity, a potential spy must be comfortable in the duplicitous role-playing and manipulation of people that spying often demands.  

There is an enormous amount of stress that goes along with betraying one’s country, and it is important that the agent is able to handle it.

---

68 Hitz, *Why Spy?*, 60.
69 Ibid., 76.
70 Ibid., 76.
According to Decision Support Systems Inc., these are the motivational elements of al-Qaida based on propaganda, media releases and interviews:

- **Survival.** Many individuals in the region feel threatened by U.S. dominance—force projection, financial, cultural, technical, etc. Responding with a ‘fight-or-flight’ mechanism, there are few places to run in the modern globalized civilization, so ‘fight’ remains essential (from their view) for survival.

- **Target the social contract.** The freedoms and culture of the U.S. are abhorrent to Al-Qaida—spiritually ‘bankrupt.’

- **Opportunistic.** The vulnerabilities are there, as are the opportunities. Any chance to attack can be seized upon.

- **‘Shared suffering.’** Social ties in the region, refugee camps, failed economies, and various conflicts draw the individuals together. You fight because you need to, it’s expected of you, and your ‘brothers’ depend on you. Tightly coupled cells also undergo ‘continual enrollment’—reinforcement of membership and obligation. While initially brought together through ‘voluntary association,’ once engaged in a cell they are trapped and it would be shameful to disengage.

- **Spiritual interpretation, ‘purity’ of purpose.** Religious belief or necessity dictates that such activities and operations, up to and including death of self and others, is an obligation and will be rewarded.

- **Revenge.** Only one or two degrees of separation are between any individual (living) and one of the victims of the regional chaos that has been progressing for decades. Terry Anderson’s (former hostage) “train of history” is a good metaphor—you’re in a train car because of what was done to you by the occupants of the previous car, and your actions will populate the next car, and so on.

- **Ego, symbolism.** Striking out at perceived authority is ego-reinforcing. Highly visible or high-profile targets provide the ‘greatest return’ in attention.

- **Being taken seriously.** Threats without action are ignored—violence wins a seat at the table. This is why force projection is essential for opposition groups. Escalation of Al-Qaida terrorist actions may be linked to a lack of negotiation or being afforded a ‘voice’ in political matters. Declaration of ‘war’ on Al-Qaida and bin Laden accomplish establishment of parity—they’re now an equivalent of a State power, the primary priority of the top nations.

- **Demonstration of power.** Proof of capabilities, but more importantly, the shift in ‘will’ of the opposition force. For an individual, suicide in such an operation provides control—selection of the time, place, and situation of one’s death.

- **Appease existing and attract new support.** Political support, financial support, new recruiting, etc., increase after an operation (more so when it’s successful)

- **Action is the message.** ‘Brand’ Bin Laden. As per the initial discussion regarding organizational motivation, Al-Qaida wants the U.S. out of the region, and hates the symbols and substance it represents.
• Face. Authority needs to be exercised. This may not be internally relevant in Al-Qaida, but it positions Bin Laden and associates more significantly in regional affairs.

• Destiny, calling. Pronouncements, fatwa, declarations of jihad, etc., appeal to those wishing simple answers to return to a simpler world.

• Shift relative strength. The U.S. is perceived as weaker post 11 Sept. 2001—the air of ‘invulnerability’ has been stripped away, regardless of military force projection.

• Lure. Trapping the U.S. into a response improves Al-Qaida’s position, including the potential destabilization of regimes to their benefit (a nuclear-equipped Pakistan, religious sites in troubled Saudi Arabia, financially teetering Lebanon, etc.)

The key difference between the motivations of terrorists and spies is that for spies, the motivations are essentially “life improvements.” Their lives are not dependent on action. The decision is solely based on having more to gain compared to the risks involved in their mind. For terrorists, the motivations are more survival based. There is essentially no decision involved. At which case the risks and consequences involved become insignificant because they view the situation as bleak and view violent action as the only choice to make.

---

CHAPTER 5

CHALLENGES

Infiltrating an adversarial group is difficult, whether it is a Foreign Intelligence Service or an Islamic terrorist group. It is particularly difficult to penetrate a terrorist group. This chapter will examine the reasons why it is more difficult to penetrate terrorist groups in relation to FIS.

The first reason why penetrating terrorist groups is difficult is the requirement to commit terrorist acts as part of the recruitment process. This requirement makes inserting a mole inside a terrorist organization extremely difficult. As written in a U.S. Department of State Bulletin in July 1988, “Penetrating terrorist groups—placing an agent on the inside—is enormously difficult. Terrorist organizations are secretive by nature; some accept as members only people with a given ethnic, religious, or even family background. Even then, the "entry fee" to join can be very high. For example, Sendero Luminoso, one of the world's most highly disciplined and dangerous terrorist groups, operating in Peru, requires that before being allowed into the group, an aspiring new member establish his or her credentials by first killing a judge or policeman. Only after that will their application for membership be considered. Obviously, this makes placing agents in such a group difficult or impossible. And in the case of the United States anyway, illegal.”

In contrast, the recruiting requirements by FIS are much more lenient compared to terrorist groups. If an agent objects to a particular activity, intelligence services generally accept the condition as long as the agent continues to provide valuable intelligence. An excellent example is Robert Hanssen. Hanssen refused to meet in person with his Soviet/Russian handlers. Instead, Hanssen passed intelligence and received payment through “dead drops.” Hanssen would leave packages in marked public places where his Soviet/Russian handlers would pick them up and vice versa. Robert Hanssen also requested a

---

specific handler, Victor Cherkashin. Cherkashin was picked by Hanssen because of his reputation for taking care of his agents.\textsuperscript{73}

Another reason it is difficult to penetrate terrorist groups is that it is sometimes necessary to hire criminals and terrorists as sources. In order for the CIA to hire an informant with a criminal record, they would need to file a report with the Department of Justice. It is up to the Department of Justice to approve the request. Because of this requirement, case officers typically stay away from potential agents that may have committed terrorist acts in the past and aim for agents that will provide less valuable intelligence but have a clean record. Members of terrorist organizations usually affiliate with other individuals that have performed illegal activities in the past. If case officers do not target these individuals for recruitment, it is like fighting with one hand tied behind your back.\textsuperscript{74}

This requirement applies to recruiting foreign intelligence officers as well. However, officers of an FIS typically stay away from recruiting individuals with criminal and terrorist activities. Because of the clandestine nature of their mission, intelligence officers are required to keep a low profile. Terrorist activities would prevent intelligence officers from staying undetected. The pool of individuals that case officers can target for recruiting against an adversary Foreign Intelligence Service is much larger compared to a terrorist organization.

It is also difficult to penetrate networked based terrorist groups due to their organization. As discussed in Chapter 2, al-Qaida and other networked terrorist groups are designed for survivability. They are designed so that elimination of any member or cell does not destroy the whole organization. This scheme is also effective in preventing a successful infiltration of the group. The core is difficult to penetrate by design. The operational cells, even if successfully penetrated are compartmentalized so the negative effects to the organization are minimized. The article by Decision Support Systems, Inc., illustrated the difficulty in penetrating the terrorist group al-Qaida. The article stated, “Islamic organizations are better thought of as building from an internal core outward…. it’s built on close personal relationships. This group is, of necessity, socially embedded (tightly coupled


\textsuperscript{74} Hitz, \textit{Why Spy}, 165.
to the point of lost flexibility), as well as location and context embedded.”75 The article further discusses the difficulty in penetration:

Trust inside Al-Qaida is role based—who, the domain, the degree. This will prevent easy penetration of the network. Turning members will require detailed understanding of their original motives for membership, with considerable psychological effort taken to ‘convert’ an individual. Walk-ins are particularly unlikely out of the core group; pressure may force structural support cells out of the network or into cooperation, but with limited benefits; operational cells will be compartmentalized but will give glimpses into capabilities and some organizational elements. 76

As far as organizational structure is concerned, networked terrorist groups and Foreign Intelligence Services are similar. FIS, in order to protect their sources and methods, practice compartmentalization. Also, the agents are organized into networks in order to prevent the detection of the case officer and other case officers that are also targeting the host county. Both groups, though networked, have hierarchical characteristics. Al-Qaida showed its hierarchical characteristics when Ayman al-Zawahiri wrote a letter to Abu Musab al-Zarqawi, the leader of al-Qaida in Iraq (AQI). In the letter, Zawahiri asked Zarqawi to stop the killing of civilians during the Iraq insurgency. “Therefore, the mujahed movement must avoid any action that the masses do not understand or approve.”77 By trying to influence Zarqawi’s operations in Iraq, Zawahiri perceives himself in a higher status in the organization therefore implying hierarchy in the organization.

The difference in the organization is in each group’s respective intelligence consumer. An FIS must pass its intelligence to either members of the government or the military or else the intelligence is useless. This is part of the intelligence cycle known as dissemination. In contrast, an operational cell that collects intelligence does not need to pass the intelligence to other members of the network. The cell can use the intelligence in order to

76 Ibid., 13.
conduct their attack. The elimination of outside consumers makes the detection and penetration of terrorist cells extremely difficult in contrast to Foreign Intelligence Services.\textsuperscript{78}

Risk aversion also plays a significant role in making the infiltration of terrorist groups more difficult. Risk aversion is not only part of Western intelligence culture, it is a significant part of Western culture overall. Every life in Western civilization is important, is deemed worthy of saving.\textsuperscript{79} Counterintelligence agencies engage in deception and manipulation activities in order to disrupt the activities of adversary intelligence agencies. The deception activities typically involve sacrifices. Counterintelligence agencies allow known spies to access some vital information in order for the adversary intelligence agency to believe that they were successful in their infiltration. Then, the counterintelligence agency can choose to either try to discover the spies’ handlers or keep feeding the spies useless and wrong intelligence.

The record of U.S. counterintelligence, especially counterespionage, shows that most CI has been based on tolerating some level of loss—extremely grave loss in the case of some long-serving, well-placed spies—that, once discovered, triggers intensive investigations, prosecutions, and countermeasures to repair and limit damage. It is now intolerable in the face of a global war and the steady growth of intelligence operations directed against the United States and its interests.\textsuperscript{80} If an intelligence or a counterterrorism agency allows a terrorist group to continue their activities, it could result in a significant number of lives lost. Western society would find that unacceptable.

The complication of risk aversion is also evident in the protection of agents. The protection of sources has always been the priority of intelligence agencies. Future agents will be reluctant to trust an intelligence agency if the agency earns a reputation for not protecting their agents. “If the word got out that the DO didn’t protect its agents, no one would ever spy


for the CIA again.”81 The risk versus reward calculus in determining whether or not to use intelligence at the risk of the source has always existed in intelligence.

In terrorism, the complications are even greater because not using the intelligence might result in the loss of lives. Former head of the Mossad, Meir Dagan, referred to this complication as “the limited shelf-life of the intelligence source.” He further explained that “the very act of using the intelligence information received, both to prevent intended terrorist attacks and to plan and carry out offensive counter-terrorist actions, presents the tangible danger that the intelligence source will be exposed by counter-intelligence agencies or by the terrorist organization itself.” An example that Dagan gave was,

If intelligence information is received that someone intends to commit a terrorist attack against a particular target, and based on this the terrorist is subsequently arrested, or road blocks are placed along the way to the target and security measures are beefed up at the target itself, then this signals to the organization that its intentions were exposed and the enemy managed to place an intelligence source inside the organization.82

Dagan concluded that, “any operational action that is based on concrete intelligence information involves a risk to the intelligence source himself.”83

American perception in the Middle East is an obstacle for the United States regarding foreign policy in the region. Sam Huntington discusses the reasons in his book Clash of Civilizations. Basically, American perception in the Middle East is negative due to U.S. military presence in Iraq and Afghanistan, U.S. support for Israel, U.S. role in economic globalization and also the perception that Americans are insensitive to Islamic culture. In the Cold war, American capitalism is the alternative to Soviet communism. Many individuals in the Eastern Bloc countries did not agree with communism. Some of these individuals decided to change their loyalty and spy for the West. The U.S. was perceived as the good guys in comparison to the Soviets. However, “This time we are the bad guys.”84

---


83 Ibid., 52.

84 Hitz, Why Spy?, 137.
This negative perception is especially evident in the U.S. efforts to recruit agents in our counterterrorism efforts. This is the most significant hurdle that case officers must go through in order to successfully penetrate terrorist groups. The negative perception of the U.S. in the Middle East effectively eliminates one of the motivations for espionage: Ideology. Even if potential recruits disagree with terrorism enough to compel them to take action, they would be reluctant to support the United States if they perceive Americans negatively.

Another reason it is more difficult to penetrate terrorist groups in comparison to Foreign Intelligence Services is because of the terrorists’ radicalization process. In 2008, the British Intelligence Service MI-5 estimated that it took roughly an average of 18 months for an individual to become radicalized enough to conduct an attack. During the radicalization process, it is difficult to identify the groups and the members of the groups. Domestically, it is more difficult for the FBI because they need probable cause before the group can be under surveillance. Before they can be under surveillance, some members of the group during the radicalization process become frustrated and form a separate group that will resort to violence. These members will be closely knit and go “underground” which makes it extra difficult to infiltrate.85

The process of transforming from a radical extremist group to a terrorist group makes it difficult to identify the groups that need to be penetrated. First, intelligence needs to find the radical groups. Then it needs to assess which ones have the potential to become violent. Then try to determine the members’ vulnerabilities. On the other hand, Foreign Intelligence Services have a set method of placing their agents within our borders. FIS either uses diplomatic covers or companies that they created. “It is a far more challenging puzzle than looking at a cadre of Soviet or Chinese officials and trying to determine who the intelligence officers are, and then assessing their vulnerabilities. For the most part, we are still in the position of trying to figure out who and where the bad guys are.” 86


Another problem that inhibits the penetration of terrorist groups is within the CIA’s recruitment doctrine. F. W. Rustmann, Jr. described this problem:

[O]ne of the most important courses taught to new operations officers at “The Farm” – the CIA’s secret training facility – is “The Recruitment Cycle.” It’s a basic “how-to” course describing the steps and techniques required to induce the in-place defection of new sources of intelligence. The recruitment cycle involves four distinct phases: spotting, assessing, developing, and delivering the final recruitment pitch.

When a CIA case officer targets an international terrorist organization for penetration, the first step is to examine its membership. The profile of today’s international bomb planting terrorist is an Arab male between the ages of 17 and 24, raised in the strict Muslim faith in a small rural Middle Eastern town, who harbors a deep hatred of the U.S. and a fanatical willingness to martyr himself in the name of Allah. He is highly suspicious of foreigners, has few if any foreign language skills, and shuns anyone who is not of his faith, clan and heritage.

Furthermore, the terrorist doesn’t frequent any of the traditional agent spotting arenas for the CIA: He doesn’t hang out in bars or frequent upscale restaurants, is not to be found on the diplomatic circuit, nor on tennis courts or at cultural events, or at any of the other usual spots where CIA case officers would normally troll for prospective agents. The terrorist and the urbane case officer do not move in the same circles….

The CIA’s recruitment doctrine is not entirely germane when dealing with the terrorist target. The terrorist can’t be recruited if the CIA case officer is not in a position to spot, assess and develop him first. So the CIA case officer must step back and work through intermediaries, or access agents,… The gap between the urbane American case officer and the Arab militant is still too great to bridge in one step. So additional links in the chain, additional access agents, must be added, further distancing the CIA case officer from his target, and exponentially compounding the difficulty of the operation….

Then, assuming the CIA case officer is able to orchestrate such a daisy-chain, there is the problem of getting accurate and timely information up the chain to the case officer, and requirements down to the terrorist recruit.87

The agent recruitment cycle has been the standard in espionage for both sides. It remains the same for both groups. The difference is where the recruitment cycle takes place, both in terms of physical location and social networks. Case officers have physical access to the areas in the world where the potential recruits are located. In fact, the physical access to

---

potential recruits is much easier now than during the cold war. However, the case officers lack the sufficient cultural and language skills to be able to blend in their potential recruit’s surroundings. They can be where the potential recruits are, but they stick out like a sore thumb. This is true socially as well. Case officers have difficulty penetrating the social barriers in order to have access to potential recruits for terrorist organizations.\(^{88}\)

Another reason it is difficult to infiltrate terrorist groups is because of the incentive structure of the CIA agent recruitment. David Tucker stated in his editorial, “An important part of the explanation, perhaps the most important part, is rather simple. Directing an agent who is trying to penetrate an organization like al-Qaida is time-consuming work, requiring careful handling of the agent. CIA case officers are rewarded for recruiting agents. They are not rewarded for running them carefully. Thus the incentives of the CIA discourage case officers from undertaking the time-consuming work of running long-term penetrations.”\(^{89}\)

This factor affects the penetration operations against both Foreign Intelligence Services and networked terrorist groups, but it affects operations against terrorist groups more. This is because of the long process required to penetrate terrorist networks. Al-Qaida would not allow “walk-ins” into their core group, and their organization is structured so that the damage remains minimal if one of the cells were penetrated or destroyed. Their vetting process is constant and meticulous. Every action and behavior is watched and carefully analyzed.\(^{90}\)

Finally another factor why it is difficult to penetrate terrorist groups is due to the poor recruitment of case officers.\(^{91}\) All intelligence agencies in the United States constantly need native speakers of Middle Eastern languages. The Iraq Study Group discovered that out of a

---


thousand person embassy in Baghdad, only six are fluent in Arabic. Like the previous reason, this factor is also applicable to the operations against both Foreign Intelligence Services and terrorist groups. However, this reason is more impactful in the infiltration of terrorist groups. Because of current political, cultural, and religious issues with Western countries, intelligence operations in the Middle East are much more difficult. “Gone are the days of the agency’s early espionage operations in the Middle East when a seasoned intelligence officer could declare that the only language he needed to gain access was that of money.” Extra emphasis is needed to recruit individuals that can work through the cultural and language barriers in the areas of the world where terrorist groups operate.

September 11, 2001, is widely considered as the Pearl Harbor of the 21st century. The parallels are due to the lack of warning (perceived as intelligence failures), the significant loss of lives, and the attack occurring within the borders of the United States. After the attack on Pearl Harbor, there was a lack of trust against Japanese Americans. Americans of Japanese ancestry where relocated into refugee camps on the West Coast. Japanese Americans that volunteered to join the military were generally not allowed to participate in the Pacific theater. However, German and Italian Americans were allowed to participate in the European theater during World War II. A comparable situation now exists for Americans with Middle Eastern descent in the intelligence field. The intelligence agencies are reluctant to give clearances because Arab Americans have relatives that still reside in areas in the Middle East where terrorist recruitment takes place. “There appears to be an underlying mistrust of Muslim Americans or Arab Americans in the national security area.”

On the contrary, this should make Arab Americans attractive to intelligence agencies. Terrorist groups are tied by social bonds with family and close friends. Case officers that

---


95 Hitz, *Why Spy?*, 68.
have social ties with the family and friends of terrorist members will have more success in recruiting valuable agents. The reluctance to trust Muslim Americans leads to the problem of not having enough case officers that can break through the cultural and language barrier. It also leads to the problem of not being able to recruit Americans that are in the best position to recruit agents.
CHAPTER 6

CASE STUDY

Humam Khalil Abu-Mulal al-Balawi was a Palestinian born in Kuwait. He grew up in a middle class family in which his father was an educator. Things were going well for the al-Balawi family until Saddam Hussein’s invasion of Kuwait in 1990. After Desert Storm, the Kuwaitis expelled 300,000 Jordanians because of Jordan’s support for Iraq. Humam al-Balawi and his family returned to Jordan, losing most of their possessions. Al-Balawi graduated from Amman High School with honors after which he decided to study medicine at Istanbul University in Turkey. While in Turkey, al-Balawi frequented internet chat rooms to study Turkish. This is how he met his wife Defne Bayrak. Bayrak is a Turkish journalist and translator. They decided to live in Jordan with their two children. One of al-Balawi’s future goals was to further study medicine in Turkey or in the United States.96

On the outside, al-Balawi seemed like an ordinary physician who works at a clinic in Zarqa, Jordan, treating children. Beneath the exterior, al-Balawi goes by the pen name Abu Dujana al-Khurasani. Abu Dujana is a frequent contributor to Islamist extremist websites. At one point, he was believed to be the moderator of al-Hesbah, an online forum directly tied to al-Qaida. He would post pictures and videos of American troops being killed. Abu Dujana became a popular personality in jihadist forums. He wrote, “My words will drink of my blood.” 97

According to his wife, the major catalyst in al-Balawi’s extremist views was the U.S. invasion of Iraq in 2003. Al-Balawi spent hours in online jihad forums under his pen name Abu Dujana. His views became even more radicalized after the 2008 Israeli-Gaza conflict. As a Palestinian, he identified with the victims in the war, particularly the children. He signed up with a group of physicians who wanted to travel to the Gaza strip and offer

---

96 Finn and Warrick, “In Afghanistan Attack.”
97 Ibid.
medical services. However, they were unable to travel to Palestine thus depriving al-Balawi, and more importantly his alter ego Abu Dujana, the means to directly support jihad.98

Based on an interview of Defne Bayrak, the opportunity for jihad did not present itself until the arrest of al-Balawi by General Intelligence Directorate also known as the GID. The GID is Jordan’s intelligence service which is a close ally of the United States. The GID learned of Abu Dujana’s true identity and tracked him down to Amman, Jordan. The GID arrested al-Balawi in the middle of the night and interrogated him. They released him after three days which was unusual. After his release, al-Balawi told his wife that he was going to Pakistan to further study medicine. He abandoned his goals of studying in Turkey or in the U.S.99

While under the custody of the GID, one of the intelligence officers that interrogated al-Balawi was Capt. Sharif Ali bin Zeid. Bin Zeid was a ten-year veteran of the intelligence service and also a distant cousin of the King of Jordan. Bin Zeid developed a relationship with al-Balawi in which he convinced him to work for the GID. Bin Zeid convinced him to travel to Pakistan and to infiltrate al-Qaida or any other terrorist group. Bin Zeid kept contact with al-Balawi during his time in Pakistan, after which al-Balawi provided proof of access to Ayman al-Zawahiri, al-Qaida’s number two leader at the time. He detailed medical information on al-Zawahiri verified by CIA analysts in Langley, Virginia.100

Due to the magnitude of the intelligence provided, the CIA decided to step in and meet al-Balawi. The CIA made a decision to debrief him and to train him in order to provide the location of al-Zawahiri. They arranged to meet him at the CIA base in Khost, Afghanistan. He entered the base, but instead of providing intelligence, al-Balawi detonated his suicide vest. His suicide attack killed seven CIA personnel and also his Jordanian handler,


99 Ibid.

100 Finn and Warrick, “In Afghanistan Attack.”
bin Zeid. This was the worst loss in CIA history since the 1983 bombing of the Beirut embassy.\footnote{Ibid.}

This case singlehandedly represents the difficulty in penetrating terrorist groups compared to Foreign Intelligence Services. As much as the May 1, 2011, Osama bin Laden raid was the epitome of intelligence success, the December 30, 2009, suicide attack was the epitome of intelligence failure.

As discussed in Chapter four, there are several examples of differences between the infiltration of terrorist groups and Foreign Intelligence Services in the case of al-Balawi. The first is the difference of the organization’s objective. Discussed in Chapter three, the terrorist organization’s objective is to get the most political benefit they can get out of every operation. On the other hand, a Foreign Intelligence Service aims to gain the most valuable intelligence they can get with consideration to the agent’s life. This was glaring in the case of al-Balawi.

The Taliban, in conjunction with al-Qaida and possibly the Haqqani network, orchestrated the suicide attack on the CIA base Camp Chapman, known to the CIA personnel as Khost. It is inconclusive whether at one point or another al-Balawi was actually working for his Jordanian handlers. At which case, al-Balawi provided a connection to the GID and the CIA which the terrorist organization did not want to sever. In December 26, 2009, AS, which stands for As-Sahab media interviewed AD, which stands for Abu Dujaanah, which was al-Balawi’s pseudonym in the jihad blogs;

\begin{quote}
AS: After reaching the Mujahideen in safety and with your booty, did you ever consider cutting your connection with Jordanian intelligence, which had sent you to spy on the Mujahideen?

AD: The fact is, there was no way I was going to sever this connection, because this connection itself had become a bait being offered to Jordanian intelligence, which itself had become a valuable prey. And this is what the Mujahideen here in the Land of Khorasan realized, and that’s why their first action was to form a mini Shura council for this operation. Every single step taken had the goal of luring Jordanian intelligence to this land to arrest or kill them and give them a message written in blood that the Mujahideen will not fail to use the same tactics the intelligence services use. This, then, was the fundamental reason, which is that there was a valuable prey we were anticipating through this
\end{quote}
connection, in addition to the money, money which comes to us from these imbeciles without any effort on our part, the same money the brothers in the Arabian Peninsula got their hands on when they tried to assassinate the idol Muhammad bin Nayef. So this is a new era for the Mujahideen, Allah willing, in which the Mujahideen will use intelligence-based tactics and methods which rival or even exceed those of the security apparatuses of the strongest of states, like Jordan and America, with the permission of Allah, Lord of the worlds. So this was the fundamental reason.102

Al-Balawi’s answer in the interview shows the terrorist group’s mentality in terms of espionage. Instead of trying to use their double agent to gain intelligence on the CIA and the GID, the Taliban made a decision to use their agent for a “martyrdom operation.”

The GID and the CIA did not realize this significant difference between the two groups at the time. CIA had several officers brought in for the debriefing. Many of which would have been tasked to view body language for deception.103 Also a polygraph examiner would have been present as well. The CIA officers failed to realize that their focus should have been on physical security in case their agent had switched loyalties because of the nature of terrorist organizations.

Another difference that can be seen in the al-Balawi case was the difficulty of having to recruit criminals or terrorists as agents. In the case of al-Balawi, he was neither a criminal nor a terrorist. He was, however, a radical extremist. As mentioned previously, he frequently blogged about his extremist views. In his interview, he discusses this:

AS: If you please, brother, could you give us a brief idea about your emigration from Jordan to the land of jihad and your motivations for it?

AD: First of all, when I witnessed the events of Gaza – and very painful events they were – I can’t forget the scene I saw on al-Jazirah channel, in which the daughters of Zion were watching Gaza as it was being bombed by F-16 fighter jets. They were using binoculars and watching the Muslims get killed, and it was as if they were just observing some natural phenomenon, or as if they were watching a theatrical film or something similar. So I wrote an article, the last of my articles, entitled “When Will My Words Drink From My Blood?”…. 

---


103 Ibid.
AS: Could we now start to talk about some of the details of your move from Jordan to the land of jihad and how Allah blessed you to carry out this major operation?

AD: Yes. In truth, it all began with the Jordanian security organs entering my house at 11:30. They came and knocked at the door of my house…. So all praise is due to Allah, Lord of the worlds: the intelligence officer – whose name was Abu Zaid [Ali bin Zaid], and who works with Abu Faisal in the Counter-Terrorism Division – was an idiot, and Allah made His plotting manifest itself by way of this idiot, who asked me to work with the security organs in spying on the Mujahideen in Waziristan and Afghanistan. So this step began with this proposal. They proposed that I go to Waziristan and Afghanistan to spy on Muslims. But the amazing thing which I could hardly believe is that I had been trying to mobilize to jihad in Allah’s path but had been unsuccessful, then this idiotic man comes along and proposes that I go to the fields of jihad. All praise is due to Allah, Lord of the worlds: it was a dream come true!  

This section of the interview shows al-Balawi’s extremist view. He viewed the Jordanian intelligence’s offer to go to Pakistan as his opportunity to go to jihad. Terrorist organizations thoroughly vet their new recruits. They monitor their activities at all times. They can determine if a recruit is a true believer or not. This is why it is necessary to recruit agents like al-Balawi which have extremist views because a recruit that fails to prove their devotion to the cause can be easily rooted out. In contrast, agents trying to penetrate Foreign Intelligence Services do not have to be criminals, terrorists, or possess radical ideology.

The intelligence officers in the case of al-Balawi for both the GID and the CIA were more than likely aware of this significant problem in trying to penetrate a terrorist organization compared to a Foreign Intelligence Service. Al-Balawi was more likely viewed by the GID as a necessary gamble that they had to take. However, the question becomes, did the officers fail to remember the calculated risk that they took in trying to use al-Balawi as an agent? Did they fail to remember that at one point, the agent had sympathies with terrorist organizations? For the case of al-Balawi, this thesis will not answer these questions, however, this thesis will take note of the calculated risk, which may be difficult to circumvent, that intelligence agencies take in terms of this kind of problem. The proper handling of such an agent would be to consider him or her as a double agent even though the agent technically has not switched loyalties.

104 Ibid.
This section of the interview also shows the typical recruitment process of terrorist organizations. In the case of al-Balawi, it was neither the Taliban nor al-Qaida that pursued al-Balawi. Al-Balawi had to seek out the terrorist organization and offer his services even though his pseudonym, Abu Dujana, was popular among jihadist online forums. Also, according to the interview, al-Balawi was becoming frustrated because he was not participating in jihad against the United States. He firmly believed in the extremist ideology but lacked the chance to show it beyond the computer. It was just “due to Allah” that the Jordanians arrested him and provided him the opportunity for jihad.\textsuperscript{105}

Another problem in trying to penetrate terrorist organizations as opposed to Foreign Intelligence Services is the incentive structure. Case officers that can recruit agents who provide valuable intelligence are rewarded in the agency. Al-Balawi in his interview discussed his actions in trying to convince the CIA of his worth:

AS: After taking the decision to maintain the connection and try to use it against them, what are the tactics you used in order to convince them that you were actually spying on the Mujahideen, and how were you able to hide from them that your true intention was to ruin them?

I cut ties for four months, then came back to them with some videos taken with leaders of the Mujahideen, so that they would think that I was leaking videos and betraying the Mujahideen. All praise is due to Allah, the bait fell in the right spot and they went head over heels with excitement. The videos I sent were actually taken with the Mujahideen’s own camera for this very purpose…. And I would throw in some accurate information which we thought the enemy probably already had knowledge of. With time, the Jordanian intelligence apparatus and the idiot Abu Zaid – whom Allah put at my service in this work – became convinced that Abu Dujaanah al-Khorasani was working for them. But in fact, I – with the help of Allah – was working to ruin them.\textsuperscript{106}

In this interview, he shows that he was aware that by providing proof of his access to senior leadership, the GID and the CIA would come to trust him. He stated that he had access to Ayman al-Zawahiri, al-Qaida’s number two at the time. His success came at a very accelerated pace. There were a few officers that voiced concerns that it was happening too

\textsuperscript{105} Ibid.
\textsuperscript{106} Ibid.
quickly.\(^\text{107}\) However due to the reward of capturing or killing al-Qaida’s number two, the concerns were ignored.

The question then becomes, if this type of success occurred in the penetration of a Foreign Intelligence Service, would the officers be skeptical? Another question can also be asked, was this an isolated incident? If the same set of circumstances can be replicated, would the officers voice concerns over the rapid success? The answers would be moot in this case. The proper question to ask would be, if there was no incentive structure to reward instant success, would it have happened? The answer would more likely be no. The case officers would more likely temper their excitement at the possibility of killing a high value target. Case officers that voice concerns over the accelerated success would more likely be heard.

This problem of incentives is more applicable to the infiltration of terrorist groups because the infiltration of terrorist groups requires more tedious work. Networked terrorist organizations are compartmentalized. New recruits are subjected to a rigorous vetting process and it takes a significant amount of time before the trust of terrorist organization’s senior leadership can be earned.\(^\text{108}\) This problem, although it applies to both the infiltration of terrorist organizations and FIS, applies more to the penetration of terrorist organizations.

In al-Balawi’s case, the use of financial incentives as a means to convince him to spy for Jordan backfired. The recruitment method employed by the GID was specifically asked by his interviewer:

\begin{quote}
\textbf{AS:} Is it possible for you to give us an idea of the methods the villainous intelligence officers used to try to recruit you?

\textbf{AD:} When they arrest a brother and try to convince him to work with them, they will offer him the world and offer him everything, and occasionally, they will use weak arguments, absurd arguments, like telling you that king abdullah is from Ahl-al-Bayt (the House of Prophethood). What does Ahl-al-Bayt have to do [with this]? Abu Lahab was also from Ahl-al-Bayt! Absolutely absurd things! This criminal tried to brainwash me, but in fact, the idiot was digging his own grave. I want to say that the Jordanian security and intelligence apparatuses have a very strong faith in the gods of the lame pelican, America. They believe in their
\end{quote}

\(^\text{107}\) Finn and Warrick, “In Afghanistan Attack.”

\(^\text{108}\) Jones, “Defeating Terrorist Groups.”
gods and believe in the money which comes to them. And glory be to Allah, when your own belief system is corrupt, you think that everyone else will set off from the same corrupt belief system. They tried to entice me with money and offered me amounts reaching into the millions of dollars according to the man being targeted, particularly the leaders of Qaida al-jihad in the Land of Khorasan – may Allah preserve them. So they were offering me millions upon millions,… They think that we worship wealth and lusts just like them. How amazing! How amazing that you propose [such things] to a man whose last article just a short while ago was called “When Will My Words Drink From My Blood?,” a man who burns with desire for martyrdom and who motivates the Ummah to jihad! How can you come to him and have the gall to say to him, “Go and spy on the Mujahideen”?!  

Another important lesson to be learned from the al-Balawi case is to tread carefully when using money as a motivation for an agent in a terrorist organization. As discussed in Chapter 3, money is one of the motivations Foreign Intelligence Services use to convince an agent to spy for them. In fact, Money is considered the ultimate lubricator. Even if the agent does not ask for money, the case officer feels more comfortable if he gives the agent money for his services.  

109 Al-Balawi, “An Interview.”  
110 Hitz, Why Spy?, 34.
CHAPTER 7
RECOMMENDATIONS

The previous chapter discussed why it is more difficult to penetrate terrorist groups compared to Foreign Intelligence Services. However, there is a requirement that terrorist groups have that makes it easier to infiltrate compared to FIS. The previous chapter also discussed that terrorist groups constantly need recruits. Due to the constant requirement for recruitment, this allows intelligence agencies the avenue to penetrate terrorist organizations. This chapter discusses ways in which the problems of penetrating terrorist groups can be alleviated and the weaknesses exploited.

RECRUITMENT POSITION

The first step of the recruitment cycle is to spot potential agents. However, as discussed in the previous chapter, case officers are not always in a position to spot. Non-Government Organizations (NGO) present a medium in which potential recruits may be spotted. NGOs provide aid to communities in the Middle East. Areas that breed terrorists are typically areas that are poor and underdeveloped. Non-Government Organizations provide aid to these areas in terms of supplies, medical services, and education.\(^\text{111}\)

An intelligence officer using the NGO as a non-official cover will be in a favorable position to recruit. The first reason is that the case officer will be in a position to spot for potential recruits. He will be imbedded in the population from which terrorists are recruited. Another reason will be that the case officer will establish relationships with potential agents. And finally, working for an aid organization presents an ideological outlet for potential agents. The case officer can state, if you want me to continue supporting your population, you will support my cause. My aid organization will provide a better life for you and your family rather than the terrorist organization, so support our cause. NGOs also present an

\(^{111}\) Ibid., 169.
avenue for potential walk-ins. It is more likely that an individual from the local population can walk up to an aid organization to provide intelligence compared to an American embassy overseas.

Case officers can also search for potential agents in internet chat rooms and blogs. Internet chat rooms are being used for recruitment by terrorist organizations. The terrorist group al-Shabaab, frequently uses chat rooms as a means of recruitment. There are an estimated 1.5 million Somalis from all over the world that constantly visit internet chat rooms and may be recruited by al-Shabaab commanders. However, not all visitors to these websites become terrorists nor completely agree with the terrorist group’s ideology. Case officers can target these individuals that either do not completely radicalize or do not agree with using terrorism as a means to accomplish their goals.112

AGENT TYPES

Chapter Two discussed the different types of agents that intelligence agencies use to penetrate organizations. The recommendations discussed in this chapter will only use three types: defectors, moles and access agents. These three types are selected because they represent the three levels of access to intelligence by agents. A defector, in the context of terrorist organizations, would be someone that is a member of the terrorist organization or its support networks. It is not necessary for the individual to climb the hierarchy in order to be useful. In contrast, moles would need to improve their position in the organization in order to provide useful intelligence. Moles, in the context of terrorist organizations, would be agents that volunteer to join a terrorist organization in order to gain intelligence. Access agents, on the other hand, are not members of the organization nor are they required to be in order to be useful. Access agents, in the context of terrorist organizations, would be agents that can recruit potential moles or defectors. Their value is in their relationship with potential agents.113


113 IPB USA, U.S. Military Intelligence Handbook, 29.
One of the problems in trying to penetrate a terrorist organization, discussed in the previous chapter, is that the core and operational cells are difficult to penetrate. Terrorist organizations conduct an enormous amount of vetting before an individual can be included in the core or operational group.\textsuperscript{114} It is unlikely that walk-ins and defectors will come out from those groups. For structural networks, however, that is not the case. Case officers should attempt to recruit members of support groups due to the relative ease in penetrating support networks versus other networks of networked terrorist organizations.\textsuperscript{115}

A defector in-place inside a support group of a terrorist organization would be valuable. An agent within a support group can provide intelligence that can prevent an attack. Even if the agent does not have firsthand information about an impending attack, he/she can provide bits and pieces of information that analysts can put together as valuable intelligence. Terrorist groups will always need a support base for financing, logistics and recruiting. As a bonus, the agent can also climb the ladder and be able to infiltrate other groups within the terrorist organization.\textsuperscript{116}

Defectors and walk-ins from terrorist groups are hard to come by. The radicalization process by which an individual transforms from a supporter to an active participator ensures the continued loyalty of its members. Terrorist recruits start their radicalization process by being attracted to the group’s ideology, and once the organization comes into contact with the recruit, they supply the ideology back to the individual ensuring loyalty. Also, by compartmentalizing the organization into separate cells, a sense of brotherhood is developed within the cells. Once the strong relationship is formed, it would be difficult for a member of the organization to betray one’s brother.\textsuperscript{117}

Since it is difficult to recruit from within the organization itself, the most effective way to penetrate terrorist organizations is to recruit from the outside and penetrate through the use of moles. This goes against the prevailing culture for case officers in trying to recruit


\textsuperscript{115} Decision Support Systems, Inc.,"Hunting the Sleepers,” 13.

\textsuperscript{116} Shulsky and Schmitt, \textit{Silent Warfare}, 154.

\textsuperscript{117} Jones, “Defeating Terrorist Groups,” 10.
agents that already have access to intelligence. The new approach requires tedious work that may or may not result in the collection of valuable intelligence. As previously discussed, terrorist groups constantly require recruits, and recruitment for terrorist organizations start from the bottom up. Agents working for the U.S. can then volunteer their services to terrorist organizations for the purpose of infiltrating them. The likelihood of moles penetrating the inner circles of terrorist organizations is possible if not probable. So instead of attempting to target current members for defection, case officers should focus on recruiting individuals that are willing to act as moles.

**POTENTIAL AGENTS**

Since the focus on penetrating terrorist groups will be on recruiting moles, it is important to consider which type of individuals would be suitable moles—people that went through the training or religious indoctrination but decided not to join the organization as terrorists. Based on the recruiting process for terrorist organizations, we have learned that it begins with a group of friends that share the same ideology. The group of friends have social ties with each other either by being relatives or by attending the same mosque. After making a decision to join the jihad, the group goes through indoctrination and training in order to become terrorists. At each step of this process, there is a possibility that a member of this group decides to separate. Case officers should target these individuals that changed their minds at the last minute.\(^{118}\)

These potential agents should be convinced to act as moles for the U.S. They would be in an advantageous position because they already have the social ties necessary in order to gain entrance into the organization. They would have someone from within the organization to vouch for them which will make the vetting process easier. Convincing these individuals would be relatively easier because they changed their minds in the first place. The case officer should identify the reason why they changed their mind and use that as motivation to recruit them as agents for the U.S.

Prior associates of individuals joining a terrorist organization should be targeted for recruitment as well. The associates do not necessarily have to be from the same group. They

\(^{118}\) Ibid., 10.
can be relatives, colleagues, or members of the same mosque.119 In 2007, Russell Defreitas and his associates had a plot to blow up the jet fuel pipeline in John F. Kennedy Airport. Defreitas tried to recruit Steven Francis who was a member of the same Brooklyn mosque. Defreitas was not aware that Francis was an informant for the FBI. He revealed his plan to Francis and brought him to conduct surveillance on his target. Francis then informed his FBI handlers of the impending plot and the terrorist attack was averted.120

Acquaintances of individuals prior to their radicalization can possibly provide valuable intelligence, but their main value would be to act as moles. Due to pre-existing social ties and similar backgrounds with current members of terrorist organizations, they would have an easier time going through the vetting process. Case officers should try to convince associates of known terrorists to join the terrorist organization and act as a mole for the U.S.121

In Chapter 5, it was pointed out that one of the problems in trying to penetrate a terrorist group is due to the radicalization process. First, intelligence agencies must identify radical groups. Then, there is also the problem of requiring probable cause before surveillance can be conducted particularly on groups within the U.S. Then, once the group makes a decision to resort to violence, it is virtually impossible to penetrate.122

A recommended solution to this problem is to recruit sleepers from these groups. Case officers should target members of groups with radical causes who would not be willing to use violence to further the cause. According to Godson, instead of quitting the group, when the time comes, officers should try to convince them to join the terrorist group;

This tactic is useful in infiltrating terrorist organizations, which is planting or recruiting someone inside a terrorist support group. It can be relatively easy to penetrate a nascent movement or organization,… as the United States found when it penetrated Students for a Democratic Society and various Communist and African-American groups in the 1960s and 1970s. As organizations mature,

119 Ibid., 10.
121 Godson, Dirty Tricks or Trump Cards, 210.
However, penetration becomes more difficult. The terrorist organization will not easily accept unknowns into its inner circle. It may demand loyalty tests, such as committing a murder, to which a plant will usually not submit.\textsuperscript{123}

Unlike typical moles, sleepers do not constantly report activities to their officers. By waiting until the right moment to report, sleepers would not circumvent fourth amendment rights. By recruiting agents from radical groups before they resort to terrorism, intelligence agencies would have an informant from the beginning.

The strategies outlined above are based on ties that potential agents currently have with terrorist organizations. However, it is extremely difficult to spot and recruit agents that have current ties to terrorist organizations. Intelligence agencies would have to resort to the cold approach in trying to penetrate terrorist organizations. Case officers would have to try to recruit agents to volunteer to join terrorist organizations. The list of candidates significantly increases; however, based on the current recruitment process it is also proportionally more difficult.

In order to alleviate some of the difficulties of an agent trying to join a terrorist organization without prior ties, the agent should present a valuable skill that the organization desperately needs. Al-Qaida is currently in need of doctors to support their operations in Afghanistan, Pakistan and Iraq. Bomb making skills would also be valuable to them. Al-Qaida or any other terrorist organization would be hard pressed to turn away volunteers that can offer valuable skills.\textsuperscript{124}

Another advantage of presenting a mole that possesses valuable skills is that the mole would less likely be asked to conduct suicide attacks. It would be in the terrorist organization’s best interest to keep valuable members of their organizations alive. There is also the possibility that moles with specific skills can get through membership without conducting terrorist attacks. Doctors, for example, are programmed to save lives. If a doctor refuses to kill someone, it may be viewed as understandable.

\textsuperscript{123} Godson, \textit{Dirty Tricks or Trump Cards}, 212.

\textsuperscript{124} Whitlock, \textit{Spy}. 
ACCESS AGENTS

As discussed in Chapter 5, case officers are not always in a position to spot agents. The cultural and language barrier might be too difficult to overcome. Case officers stand out in the potential agent’s environment which would severely reduce the possibility of clandestinely recruiting them. Also, the terrorist organizational networked structure is compartmentalized which limits access to potential defectors. Case officers would have a difficult time spotting members of a terrorist organization. Another problem in trying to recruit an agent for the U.S. is the perception of Americans and Westerners in the Middle East and other areas. It would be hard to convince an agent to work for the U.S. based on ideology. It would also be hard to convince an agent to receive payment from the United States.\textsuperscript{125}

One way to get around all these problems is to recruit access agents. Access agents typically do not provide intelligence to officers; they provide access to agents that do. American case officers have difficulty trying to blend into a potential recruit’s environment. They neither have the language skills nor the cultural skills to solicit information from the targeted population. A solution to this problem is to use access agents. Access agents provide information or contact to espionage agents. If a potential recruit is deeply embedded in a Middle Eastern population and a case officer would try to recruit him or her, a case officer could try to recruit a relative, a business owner or an associate that has the ability to come and go within the population, as an access agent. That recruit would then provide access to the potential agent.\textsuperscript{126}

This solution would be effective for many reasons. The first reason, as discussed previously, is to circumvent the language and cultural barriers that Middle Eastern populations present. There is reluctance in hiring case officers that have deep ties to the Middle Eastern population. The language skills of current case officers are inadequate to properly address the intelligence requirements. Access agents would be a quick solution to these problems. Access agents would be in a position to spot, develop and recruit agents that

\textsuperscript{125} Hitz, \textit{Why Spy?}, 23.

\textsuperscript{126} Godson, \textit{Dirty Tricks or Trump Cards}, 218.
can provide intelligence on terrorist organizations. Another reason is to alleviate the Middle Eastern negative view of the United States. Americans are viewed in a negative light in the Middle East, so it would be difficult to ask an agent to directly work for the U.S. By means of access agents, the agent within the terrorist organization is not necessarily working for the West. It is also possible that the final recipient of the intelligence could be hidden from the agent as well.

**AGENT MOTIVATIONS**

Chapter Three discussed the recruitment process for Foreign Intelligence Services. Intelligence officers typically use vulnerabilities or motivations to manipulate a potential recruit. Every recruit would have to be assessed on a case-by-case basis. Each potential recruit would have different possible motivations to conduct espionage for the United States. Case officers should try to use all seven that were listed in Chapter Four, depending on each situation. However, this thesis will discuss certain motivations that would be significant in recruiting agents against terrorist organizations.

The first motivation that should be explored is the use of money. Chapter Three discussed that money as a motivation does not exactly mean financial transactions for intelligence. The case officer is the one selling to the potential agent. Cultural aspects should be carefully considered when recruiting against an Islamic terrorist organization. Case officers should be aware that the offer of money for information might not sit well with potential recruits. It may turn them away, "This is a much more difficult target than the Soviets were. These people are true believers. They're living according to their beliefs, not in the lap of luxury."\(^{127}\)

While it is more difficult to recruit agents from an Islamic population using money, there are constants in society that will always remain: human need and greed. Greed would be more likely in the low-ranking members of the terrorist organization. The chances of using money to recruit agents would be higher in the support networks as well. It would be

---

specifically effective against people that provide support for terrorist organizations in exchange for money such as arms suppliers and individuals that arrange logistics.\textsuperscript{128}

Case officers should keep in mind that there are other ways to compensate potential recruits. Middle East countries typically have sub-standard medical facilities compared to Western countries. A potential recruit or a relative that requires medical services that only a developed country can provide would welcome help in exchange for providing intelligence.\textsuperscript{129}

Another motivation that should be explored against Islamic terrorist organizations is coercion. Chapter Three discussed that Western intelligence agencies generally do not use coercion to recruit agents. Sex can be used as a weapon in order to recruit agents from an Islamic population, but Western intelligence officers do not know enough to properly use it. One way to use sex as a weapon is to threaten to dishonor a member of their family. Some examples may include heterosexual activities outside of marriage, more specifically loss of virginity, homosexual acts and cross dressing. The slur may or may not have some credibility behind it. If it becomes public, the family may be forced by the community to perform an honor killing. In order to prevent this from happening, the potential recruit may be compelled to provide intelligence for the U.S.\textsuperscript{130}

Intelligence agencies are always vulnerable to disgruntled employees. Some of the high profile espionage cases against the CIA and the FBI have been from dissatisfied employees. Terrorist organizations are no different from intelligence agencies in this regard. They could be vulnerable to members that are disgruntled as well. The 9/11 commission have learned that Mohammed Atta, the leader of the hijackers had difficulty controlling other members of the group. Some members of the group requested to travel abroad with the possibility of not returning. A close analysis of that group and their relationships would have assisted intelligence agencies in rounding up the group.\textsuperscript{131}

\textsuperscript{128} Ibid.

\textsuperscript{129} Hitz, \textit{Why Spy?}, 38.

\textsuperscript{130} Ibid., 54.

There is also a possibility that not everyone agrees with the operational decisions in al-Qaida. Unfortunately, we do not know who makes the operational decisions at this time. Osama Bin Laden was popular with al-Qaida and its branches. Ayman Zawahiri was the operational brains of al-Qaida during Bin Laden’s tenure and does not have the same level of popularity as Bin Laden. Since Zawahiri took over as the overall leader, after Bin Laden’s death, there is a possibility that he will be more of a micro manager which could result in dissatisfaction within the members. This possibility can be exploited by case officers by trying to recruit members that want to exact revenge on their leadership.

**COLLABORATION WITH ALLIES**

A short term solution to some of the problems in penetrating terrorist organizations is to collaborate with friendly intelligence organizations in the Middle East. The CIA is currently working with other intelligence agencies and has done so in the past. Two countries that work with the CIA are Jordan and Pakistan. Pakistan’s intelligence agency, Inter-Services Intelligence (ISI), worked with the CIA during the Soviet invasion of Afghanistan.

An advantage in using this approach is that case officers can now have access to recruits which they could not have on their own. There are not enough case officers with the necessary language skills and the cultural knowledge to put them in a position to recruit agents. Case officers also stand out based on their physical appearance. Middle Eastern intelligence services have the language skills and the cultural knowledge to be in a position to recruit agents.132

Acting on behalf of the United States, the surrogate intelligence agency can offer rewards to potential agents. They can either claim the compensation is coming directly from them or reveal it is coming from the U.S. By having a proxy, the CIA can get around the negative perception of Americans in the Middle East. Islamic agents would not feel that they are betraying their principles to the U.S. for money.

There are some disadvantages with working with Middle Eastern intelligence services. First, “friendly” intelligence services might have their own separate agenda and

---

their actions might not necessarily line up with U.S. policy. This situation occurred during the mujahedeen in Afghanistan. The ISI directed their support so that certain Pashtun tribes would gain power in Afghanistan after the Soviet Union was defeated. The Taliban took over the government as a result of the ISI’s direction. Another disadvantage is that there is no way to verify if the surrogate intelligence agency is passing all the information to the CIA. The “friendly” agency could be filtering the information in order to accomplish their own agenda. This occurred during the mujahedeen as well.\textsuperscript{133}

Instead of inserting a single mole, inserting a group of moles might be more effective. Terrorist organizations are based on friendship and social ties. In order for a single mole to successfully infiltrate a terrorist organization, he or she would either need someone within the organization to vouch for him/her or need to catch the attention of the organization. Both tasks are very difficult to accomplish. However, if a cell of sleeper moles were presented. The probability of recruitment would increase. It would require only one of the sleepers to have a social tie with the terrorist organization or require only one of them to catch the terrorist group’s attention. Once a sleeper is inserted into the organization, he or she can then vouch for the rest of the group. “You don’t recruit an individual; you recruit families, clans, and tribes.”\textsuperscript{134}

**CONCLUSION**

The previous chapters showed that infiltrating terrorist organizations are different compared to infiltrating Foreign Intelligence Services. First we must keep in mind that their respective objectives are different. Terrorist organizations aim to gain the most political benefit while FIS aim to gain the most intelligence as possible. Therefore, when protecting against double agents, the agency should consider their physical security as much as the security of their sources and methods.

Secondly the recruitment process of terrorist organizations is different compared to FIS. Terrorist organizations recruit from the bottom up while the FIS prefers to initiate the recruitment process. It is also significant to note that the organizational structure of terrorist

\textsuperscript{133} Ibid., 15.

\textsuperscript{134} Baer, *See No Evil*, 70.
organizations is compartmentalized. Recruits also undergo an extensive vetting process. Because of these characteristics of the recruitment process, the best way to infiltrate terrorist organizations is through the use of moles.

This thesis also recognizes that infiltrating terrorist organizations is more difficult compared to infiltrating Foreign Intelligence Services. The first reason is that terrorist organizations may require agents to commit terrorist activities. United States intelligence agencies cannot knowingly allow an agent to commit a terrorist act which will result in loss of lives. The terrorist organization may also require the agent to perform martyrdom operations. The second reason it is more difficult is because it might be necessary to recruit criminals, terrorists or radical extremists as agents. The recruitment process of terrorist organizations requires a heavy amount of social affiliation. More often, only terrorists and radical extremists have the social ties necessary to join a terrorist organization. Another reason why it is more difficult is due to the perception of America in the Middle East. The United States is viewed negatively, so an intelligence officer would find it difficult to find someone in the local population willing to work for the U.S. Even if an individual is willing to work for the U.S., he or she might not do so because someone in the community may find out.

Another main reason why it is more difficult to penetrate terrorist organizations is because of the Western culture’s aversion to risk. Protecting sources is the intelligence agency’s number one priority. This priority was acceptable in the espionage activities during the cold war. However, with terrorism, intelligence agencies find themselves in a dilemma of protecting lives from an impending terrorist attack versus protecting their source. All these problems that are associated in penetrating terrorist organizations were evident in the al-Balawi case. Some of the things we have learned from that case were that we had to rely on other intelligence agencies for recruitment. Also, it is sometimes necessary to recruit individuals that are already radicalized into extremist ideology. And the use of money as a means to convince a potential agent, especially one that has extremist views, has a good chance of backfiring. And finally, deception activities by terrorist organizations are not aimed to collect intelligence, but rather to gain political recognition.

Based on the lessons learned from the al-Balawi case and the comparison of infiltrating terrorist organizations to Foreign Intelligence Services, intelligence agencies will
continue to use allied intelligence services. The intelligence officers for the United States do not have the necessary language and cultural skills needed to be in a position to recruit. Case officers must use money sparingly as a means to convince an agent to work for the U.S. If recruiting an individual that has been radicalized and already believes in extremist ideology, that agent must be treated as a double agent. Every precaution must be taken when dealing with the agent.
REFERENCES


