THE APPROPRIATE USE OF HUMAN INTELLIGENCE IN COMBATING TERRORISM

Mutlu Koseli B.A.

Thesis Prepared for the Degree of

MASTER OF SCIENCE

UNIVERSITY OF NORTH TEXAS

August 2003

APROVED

John Liederbach, Committee Chair
D. Kall Loper, Committee Member
Chad Trulson, Committee Member
Robert W. Taylor, Chair of the Department of Criminal Justice,
David W. Hartman, Dean of the School of Community Services
C. Neal Tate, Dean of the Robert B. Toulouse School of Graduate Studies

Koseli, Mutlu, The Appropriate Use of Human Intelligence in Combating Terrorism. Master of Science (Criminal Justice), August 2003, 93 pp., references, 111 titles.

When we looked at different issues in terrorism such as definitions, descriptions and motivations, groups and supporters, tactics, strategies, and victims of terrorists and terrorist activities, we see that terrorism is an issue that can be occur at anytime, and in any place, and it seems that terrorism threat will still be exist in the future. It is almost impossible to stop all terrorist activities all over the world, but it is possible to formulate an anti terrorism policy that can keep terrorist activities at a minimum level and prevent planned terror activities by a well developed intelligence network. It seems that to establish a good intelligence collection system an approach in which HUMINT and TECHINT are interdependent with each other is necessary. By using a combination of human and technical intelligence collection methods, intelligence agencies can become more effective and efficient against terrorism.

ACKNOWLEDGMENTS

I would like to thank to my committee for their efforts. First I'm Greatful to Dr. John Liederbach, my thesis chair, whose constant help is dominant and immeasurable in developing the study. Thank to my thesis committee members, Dr. D. Kall Loper, and Chad Trulson for their time and assistance in directing this study. Also thank to Dr. Taylor for his valuable help during my study. Special thanks to Turkish National Police for giving this opportunity to me.

Most importantly I would like to thank to my family my wife Yelda and to my little daughter Sevda for their encouragement, patience and assistance in my education and career.

TABLE OF CONTENTS

Page

CHAPTER 1

INTRODUCTION

The end of the cold war and the faded threat from the former Soviet Union has brought about a new era and a change in focus in the United States intelligence community. At this point, their focus has turned to neutralizing transnational threats such as terrorism, narcotics trafficking, global crime, and information warfare, all of which are now viewed as threats to domestic security. In combating these domestic security threats, the regular and effective collection processing, storage, retrieval and exchange of intelligence among law enforcement agencies is imperative in fighting the war against terrorism (Ellif, 1978). These types of crimes, unlike more traditional street crimes, cannot be detected through victim complaints. Unless the police posses a capacity to identify criminal organizations, there can be little effective investigation for such crimes, because of their conspiratorial and clandestine nature. Traditional criminal investigations conducted solely for the purpose of prosecution are not adequate to support the information needed for proper and effective law enforcement in the fight against terrorism and these other new threats. Intelligence operations have importance in such cases.

Technical Intelligence (TECHINT) and Human Intelligence (HUMINT) are the two main intelligence collection methods that can be used to combat terrorism. The focus of this study is an examination of human intelligence and the collection of clandestine information primarily through the use of spies and informants. For purpose of this study,

human intelligence refers to the gathering of information by human sources, rather than through modern technical apparatus.

Recent advances in technical intelligence have proven their use in gathering information and in many ways TECHNIT has grown to supercede the use of human intelligence efforts. However, important question remain regarding the effectiveness of solely relying on TECHNIT in the face of growing terror threats. Is technical intelligence enough in and of itself to provide law enforcement with the necessary and trustworthy information to combat domestic threats, or are human intelligence types of collection techniques necessary to support this intelligence? Although advances in TECHINT capabilities have reduced the need for HUMINT, the fact remains that HUMINT is the oldest, cheapest and most reliable method for gathering information. There have been numerous occurrences of intelligence failure in cases where only one method of intelligence gathering was used

A recent report by the National Commission on Terrorism emphasized that, "Their first priority is to prevent terrorist attacks. US intelligence and law enforcement communities must use the full scope of their authority to collect intelligence regarding terrorist plans and methods" (National Commission on Terrorism, 2002). Funding for counterterrorism efforts by the CIA, NSA, and FBI must be given higher priority to ensure continuation of important operational activity and to close the technological gap that threatens their ability to collect and exploit terrorist communications. Good intelligene is believed to be the best weapon against terrorism. For this reason, the CIA

has been advised that the aggressive recruitment of human intelligence sources on terrorism should be of the intelligence community's highest priorities.

Purpose and Research Questions

In light of the growing threat of terrorism and the continuing debate about what the proper balance is between human and technical intelligence sources, this thesis seeks to discuss the following research issues: 1) What is terrorism and what threats does terrorism pose? 2) What role does intelligence play in combating terrorism? 3) What factors have contributed to historical failures of Pearl Harbor and September 11 terrorist events in Human intelligence?

In order to address these issues, the present thesis will begin with a definition of the current terrorist threat through an examination of the history of terrorist activities and an overview of different terrorist groups. This discussion will be followed by the identification of methods used to combat terrorism, with a focus on the role of intelligence gathering. Different types of intelligence collection methods are identified in order to compare their effectiveness. This will be followed by an overview of the above-cited cases, including the September 11th attacks and Pearl Harbor, so that the importance and continuing need for human intelligence gathering can be emphasized.

Methodology

Initially, this thesis uses a literature based policy analysis that is designed to gain a better understanding of the role of human intelligence in domestic security matters, especially in combating terrorism. Several tools will be used in this analysis to discuss the use of human intelligence, primarily library based and internet based reviews of

previous literature on the topic. The majority of the literature review was created through an analysis of existing literature and secondary data. Most of the research for this study was library based. Books comprise the primary source from which information was collected, although scholarly journals and government sources were used as well. The internet was also used to obtain the most recent information with keyword searches including "human intelligence", "informants/informers", "espionage", "combating terrorism", and "terrorism/intelligence." In conducting library research, the university of North Texas (UNT) library catalog and electronic research databases were explored to search for books, and journal articles related to this topic. Applicable databases include EBCOHOST, JSTOR, Article First, MasterFile Premier. Related materials were then carefully examined and those that were most relevant were selected for primary examination. At this point, available information was categorized according to research question.

As an augment to this literature based review, the thesis will also discuss two specific cases of intelligence failures in intelligence gathering, including the September 11th attacks and Pearl Harbor. Case study research is especially desirable as a way to investigate complex social phenomena to find out how things are related in some depth (Mc Tavish & Loether, 2002). These cases are intended to evaluate the appropriate use of human intelligence in comparison to other intelligence collection techniques. A case study is used because its design makes it well suited for studying contemporary phenomena that call for in depth examination or the details of some process over time (Pope, Lovell, Brandl, 2001).

Limitations

There are no widely accepted research techniques appropriate for the study of terrorism. Survey evaluation and field research are almost impossible because of the secretive nature of the subjects: "The secrecy of participants, the confidentiality of materials collected by investigative agencies, and filters or screens on the perceptive apparatus of informants and investigators pose serious methodological problems for the social scientists" (Kelly, 1998). In light of these limitations, this thesis provides an analysis of the appropriate use of Human Intelligence collection sources in combating terrorism. This study does not intend to focus on the role of intelligence in general, but the role of human intelligence collection. This study aims to determine the role of human intelligence in comparison with other techniques. Legal aspects of human intelligence are not discussed.

General methodological problems regarding intelligence related issues are prevalent in this study. The secretive nature of intelligence agencies and their information sources made it difficult to gather data. It must be noted that the secretive nature of intelligence collection methods prevents scholarly research from uncovering all relevant official or unofficial records on intelligence sources and their effectiveness. Therefore, the focus of this study is limited to publicly available information on the issue.

CHAPTER 2

THE TERRORIST THREAT

The purpose of this chapter is to examine the extent of the terrorism problem. In order to do so, this chapter is divided into three primary sections. First, I will provide a discussion on defining terrorism and explaining the scope of the issue. Second, a historically-based discussion of early terrorist activities will be provided. Finally, this chapter will conclude with a section detailing several examples of terrorist activities across the globe.

Definition and Overview

"One man's terrorist is another man's freedom fighter" (Velter& Perlstein, 1991; Lodge, 1982; Crenshaw., 2001). This is the dilemma in studying and developing policies to respond to terrorism. The term terrorism has often been applied to individuals, groups, organizations, and nations. The dilemma in defining a group as "terrorist" can be seen in the example provided by the Palestinian liberation organization (PLO). Some countries view this organization as morally unjustifiable because they use violence to achieve their goals, whereas other nations view the PLO as a "legitimate representation of an oppressed people using necessary and justifiable violence not terrorism" (Vetter&Perlstein, 1991). These differences show that there are virtually no unanimous definitions of terrorism either among scholars or those operationally involved in combating terrorist threats including politicians, criminal investigators, diplomats, prosecutors, intelligence officers, public security officers, industrial security experts,

military special forces, and journalists. Each has a different professional view that may or may not be compatible with other equally valid viewpoints (Long, 1990).

A universal definition of terrorism must go beyond behavioral descriptions to include individual motivation, social milieu and political purpose (Wardlaw, 1989). Terrorism is a tactic that insurgents or revolutionaries can employ as well as a strategy that can be employed by a state. Many agree that terrorism involves using violence as a method of strategy to achieve certain goals. This violence can be used by those who oppose existing governments, or it can be used by people who want to maintain exiting power. Historically, terrorist activities have always included violence to achieve goals. Terrorism in and of itself is not a strategy, but rather a strategy of insurrection that can be used by people of different political convictions to gain political goals.

A governmental definition states that: "Terrorism is the threat or use of violence for political purposes by individuals or groups, whether acting for or in opposition to established governmental authority, when such actions are intended to shock, stun, or intimidate a target group wider than the immediate victims. Terrorism has involved groups seeking to overthrow specific regimes, or to undermine international political order as an end in itself (Long, 1990,).

Because of the many motivations for terrorist activity, it is not possible to devise a single definition to account for all possible uses of the term terrorism. However, many definitions share common elements. A significant and consistent concept used in defining terrorism is a political goal. Political goals differentiate terrorist acts from violent criminal acts or those of the emotionally disturbed. Politically motivated terrorism

involves a deeply held sense of grievance over some form of social or economic injustice. Modern terrorist organizations justify their actions not only with stated political aims but also by appeals to some higher "universal truth" that necessitates the need for political change. For a member of Red Army this motivation may involve provoking a cataclysmic world revolution. For Palestinian Liberation Organization members, it is to fulfill their national destiny and regain their homeland (Simonsen, & Spindlove, 2000).

Strategic and tactical objectives are also important in defining terrorism. The immediate objective of the terrorist group is to create terror, not destruction. This is followed by the use of unreasonable fears and the resulting political disaffection such activities generate among the public to intimidate governments into making political concessions in line with political goals. In order to achieve these objectives, terrorist activities must be public (Lodge 1982).

Terrorist organizations employ many different operational tactics in carrying out their activities. In addition to violence, terrorist groups have been known to involve themselves in other criminal activities including murder, assault, hijacking, kidnapping, arson, sabotage, regardless of their alleged political or moral justification. In all of these cases, terrorists' motivations achieve their goals through the use or threat of violence (Livingstone, 1982). Several other operational characteristics of terrorist organizations should be noted. First, the violent and criminal nature of terrorist organizations requires them to work undercover to avoid detection. Terrorists are also typically non-regular in military nature, which distinguishes these groups from others forms of irregular warfare involving the deployment of uniformed services. This is because these groups have no

military goals. Terrorists are typically cheaper to carry out than funding training programs or equipping conventional forces.

Finally an important aspect of effective operations involves the group organizational structure. Group psychology plays an important role in developing the personality of terrorist organizations (Shabad,& Ramo,1995). Like biological organisms terrorist groups are born, mature and die, only differing in their cause of death. The two main sources of death for terrorist organizations include government security forces or deprivation of support from the state, media, or other outlet. Virtually all states have at one time or another, directly or indirectly taken measures that have aided the conduct of terrorist activities.

Terrorist can behave more independently in democratic regimes. The very existence of democratic institutions, including constitutional guarantees of human and civil rights, such as freedom of speech and due process of law, make it immeasurably easier for terrorists to avoid arrest and punishment. This is not the case in the authoritarian regimes. For example, Syria supports many terrorist groups. Former President Asad was totally pragmatic about the use of terrorism and supporting it only when he believes to be an effective tactic (Long, 1990).

Just as legitimate political parties need the broad support of a public constituency, terrorist organizations require public support as well. Such support provides crucial financial, logistical, political and even legal support. The degree of constituent support that terrorist groups can muster depends on public apathy or antipathy toward their cause as well as their general concerning the social order.

Many terrorist activities motivated by political ideologies can further be broken down into the right and the left. Those included in the right are based on a pervasive and binding morality whose paramount value is an ordered society. The paramount value of the left is justice as well as an insistence upon an equal distribution of power, wealth, privilege, and prestige. Members of the right typically desire to maintain the status quo whereas the left desires governmental change (Laqueur, 2002).

According to Vetter & Perlstein (1991) terrorism can occur from above or below. The exercise of power and authority employed by those with sovereign power is considered terrorism from above. In this case, police officers enforce power and legal authority through the permissible use of violence to maintain order. This type of terrorism is used by people in power to maintain that power. Their justification is that they must use terror to defend themselves from terrorists. Examples include leaders of Nazi Germany and Lenin and the Bolsheviks. Although their use of terrorism was alleged to be for the protection of their nation, general welfare, or the will of god, the real reason was for maintenance of power and authority (Amnesty International Spring 1980).

Terrorism occurs from below as the result of a perception and experience of injustice. It originates from a belief that the injustice they perceive is not natural or remediable by force. Terrorism from below can be classified into three groups. These include those who seek prestige and power in the service of a higher cause, those who commit terrorist acts for a personal purpose, and those who commit such acts as a result of mental or emotional problems. The first type includes terrorist groups who use violence to obtain their goals. These groups may operate within their countries or act

internationally (Vetter & Perlstein, 1991). Well known examples of these types of groups include the IRA (Irish Republican Army), PLO (Palestinian Liberation Army), Abu Nidal Movement, ASALA, the ETA (Basques in Spain). Many of these groups also aim to change the social, economic, and political system.

A simpler division of terrorist typologies involves the breakdown of such groups into crusaders, criminals or crazies. By this definition crusaders try to achieve political goals through violent means. Criminal terrorists are those who use illegitimate means to achieve personal goals. Crazies, on the other hand, include people who are emotionally disturbed and driven by reasons that often do not make sense to anyone else (Vetter&Perlstein, 1991).

Most terrorist incidents can be examined through a criminal ideology. However international terrorism is much more than a crime. International terrorism can be described as a terrorist act in a state that is controlled and supported by another state and is considered an act of war (Farrel, 1982). The use of terrorism allows a sovereign state to manipulate international events anonymously instead of using their army to attack the target nation. This is the opposite of conventional fighting tactics in which large masses of men and weapon are used (Jenkins, 1978). Because it is hard to get evidence about state sponsored terrorism, it can be easily hidden or denied by the sponsoring state. Some state-sponsored terrorist attacks have resulted in the proliferation of terrorist attacks worldwide. Although some states' official policy rejects supporting terrorist activities, many have been known to continue to provide financial and operational aid in a clandestine nature. In some cases, states establish puppet terrorist organizations whose

purpose is to act on behalf of the sponsoring state to further the interests of the state and to represent its positions on domestic and religion fronts (Farrel, 1982).

Early History of Terrorism

Terror and terrorism have been in existence since it was discovered that people may be influenced by intimidation. The root of terrorism lies in the desire for retaliation against wrongdoers. Later versions of individual retaliation emerged in the form of blood feuds in which a victim's whole family or tribe took revenge on the offender's family or tribe (Simonsen & Spindlove, 2000).

Julius Caesar's assassination is an early example of the use of violence to achieve political goals. Another example of political extremist groups using violence can be seen in the "*assassins*" who emerged in the 11th century in the Middle East. These individuals gained a reputation of being lethal mission murderers who carried out their lethal mission under the influence of hashish (Long, 1990). In the first century A.D. Jewish Nationalists, known as the zealots, conducted a fierce and unrelenting terror campaign against the Roman occupants of the eastern Mediterranean. Zealots enlisted professional killers, called dagger men who struck down rich Jewish collaborators in the cities who opposed violent resistance against the Roman overlords (Livingstone, 1982).

During the first and second centuries, Roman Empire insurgents used technologies such as coercion and intimidation to achieve their goals and gather information. Early forms of terrorism date to the latter part of the eighteenth century when thousands of French were victimized under the political conviction of the French revolution (Vetter & Perlstein, 1991).

Modern Terrorism: Examples Across the Globe

Modern terrorism dates back to the 19th century when the anarchists, disliked and socially oppressed, sought the solution of mankind's problems through the destruction of all governments. This vision led to political assassinations, bombings, and other acts of violence, provoking swift reprisals in almost every country in Europe as well as the US. We now move to a discussion of specific examples of terrorist organizations in the world in order to develop a more through understanding of how and why terrorism occurs (Laqueur, 2002).

Terror in Ireland

Irish terrorism began in the early sixteenth century when England's King James I provided land to Scottish settlers in the area of Ireland. He was hoping to establish a Protestant Church in Ireland as well as convert the Irish to Protestantism, forfeit their lands, and assure Protestant ascendancy to the throne of England. These actions resulted in the first struggle between Protestants and Catholics. Years later, in 1801, the Act of Union resulted in Ireland's becoming part of Great Britain. In 1986, British Prime Minister Gladstone tabled the first Home Rule Bill for Ireland, which the Protestants opposed. The second Home Rule Bill was introduced and resulted in street fighting through Ulster (Simonsen & Spindlove, 2000; Alonso, 2001). Irish journalist Arthur Griffith founded a political organization named Sinn Fein, a Gaelic term which means "We Ourselves" in 1905. The aim of this organization was to aggressively seek self-government (Simonsen, & Spindlove, 2000). This contradicted British desire.

In 1914, the British parliament passed another Home Rule Bill. During World War I, the Republican movement in Ireland, led by Patrick Pearse, saw war as an opportunity to gain total independence from Britain. In 1916, fighting broke out between the republicans and the British. British troops quickly brought them down, executing fifteen republicans. The execution of these protagonists attracted widespread Irish sympathy. In the general elections of 1918, the Republicans, who had gained control of Sinn Fein, won 73 of the 105 Irish seats, but they never took seat in London and chose to meet in Dublin instead. At this meeting the Irish publicly declared their independence from Britain on January 21, 1919. This resulted in a division of Great Britain as well as wide spread fighting through out Northern Ireland from 1920 to 1921.

In order to combat this type of violence, the British government assembled a fighting force called the Black and Tans. This group rampaged and burned several Irish villages north of Dublin. This not only shocked the British public, but also brought about their recall from Ireland. The group was disbanded and withdrawn from Ireland in July 1921. This act divided Ireland into two separate countries, the North and the South. Cities in the North accepted the act and formed the state of Northern Ireland. Republicans in the South rejected the act after which bitter fighting broke out between the Irish Republican Army (IRA) and British troops. In 1921, Britain and the Irish Republicans signed a treaty making the south a dominion of Great Britain to be called the “Irish Free State”. In these negotiations there was disagreement between the various Republicans factions. For example, one group, led by Eamon de Valera wanted total separation from Britain as well as a reunification with Northern Ireland. In 1922, Civil War in Ireland broke out and

continued until the fighting ended in 1923. At the end of this conflict, the IRA was outlawed and its leaders were executed, but the group continued to exist as well as harass and attack British interests (Simonsen, & Spindlove, 2000). During this conflict, the IRA hoped to make Ireland an independent state and believed the killing of British soldiers would influence the British government. In February 1996, the IRA announced a ceasefire and on August 31, 1997 a cessation of military operations.

The 1998 Good Friday agreements was hailed as a blueprint for political compromise and resulted in peace and stability between 1999 and 2001. In 2001, this time of peace abruptly ended with PIRA's (The Provisional Irish Republican Army) refusal to decommission weapons (Dingley, 2002).

IRA members have always believed that physical violence can solve their problems (Monaghan, 2002). Subsequently, splinter terror groups were formed from the original ranks of the IRA such as the Provisional Irish Republican Army (PIRA) and the Irish National Liberation Army (INLA). The Provisional Irish Republican Army (PIRA) was established as one of the most ruthless and well-organized terror groups with much of their success attributable to their organization. This organization consisted of cells of three to four members based on a continental structure to more efficiently carry out terrorist attacks (Silke, 2000). This structure has allowed them to engage in an effective terrorist campaign targeting Northern Ireland in hopes of provoking a response against their Protestant neighbors, members of the British Army Unit, and the predominantly Protestant "Royal Ulster Constabulary" (RUC). The most dramatic organization change was seen in the 1970's when the group evolved from a tight-knit organization to one with

a military structure employing geographically based brigades, battalion and companies. Their most frequent targets range from military establishment to pubs, shopping centers, airports, business districts and cabinet members.

It became clear to republican leaders during the mid 1970s that armed struggle would not be a sufficient tactic in forcing the British out of Ireland allowing for a reunification of the North and South. Nonetheless, violence continued to be used in achieving short-term objectives, whereas propaganda became their main tactic for achieving traditional aspirations. Thus, it is reasonable to question whether the so-called war would have finished earlier had it not been nourished by "armed propaganda" for so long (Alonso, 2001).

Irish terrorist organizations received financial support from many different avenues. They own drinking clubs and pubs, a certain percentage of these profits are transferred to the terrorist group. Armed robbery is a common tactic used by IRA members to obtain funding. For example, in May 1986 IRA members are known to have stolen 18 paintings from the Bert Collection at the Russborough House that were valued at £ 50 million. Drug trafficking is another large source of income for these groups. They also practice loan sharking where they may demand up to thirty percent interest. Counterfeiting has also proven profitable in a wide range of products including clothing, video, audio cassettes, CDs, perfumes, agricultural drugs and currency. Fuel rackets are yet another source of funding (Silke, 2000).

Dominant terrorist groups are directly responsible for the present disorderly structure of Ireland as well as for the creation of alternative forms of justice operating

parallel to the state's criminal justice system. Administered by paramilitaries, this informal criminal justice system includes the use of warnings/threats, beatings, shootings, and execution. These informal justice mechanisms have been used since the time of "the troubles" and have continued to develop. In response to these activities, catholic working class communities have developed informal policing mechanism and set up citizen defense committees (CDC's). Mechanism of informal justice can also be found in working-class Protestant areas where they are administrated by loyalist paramilitaries. Unlike their republican opposites, loyalist paramilitaries do not cite historical precedents for their involvement in such activities (Monaghan, 2002).

The informal justice system used by the IRA is also a response to community pressure for the organization "to do something" about crime in nationalist areas. Thus, activities liable for "punishment" can be divided into two main categories, including "political" and "normal" crimes. "Political" crimes would include working as an informant, misuse of the organization's name, and the return of "Captain Moonlight" or collaborating or fraternizing with the "enemy". Normal crimes include vandalism, car theft, joyriding, muggings, the selling of alcohol to minors, rape, and drug dealing as well as other anti social behavior. Activities considered antisocial by the paramilitaries are diverse in nature and range from youths gathering at street corners, playing music too loudly, verbal abuse of old age pensioners, dumping of rubbish, and fighting with their Volunteers (Monaghan, 2002).

Rampant terrorist activities by the IRA have made life more difficult for the Irish beyond living in fear. Many Irish citizens are stopped, arrested, or detained not because they are terrorists but because they are Irish (Grosscup, 1998).

In struggling against these terrorist activities, British anti terrorist provisions have argued that the special powers given to state authorities are necessary to effectively counter any emergency situation. They maintain that provisions such as those found in the Prevention of Terrorism Act (PTA) are temporary and, thus, only related to special conditions of the present danger of the terrorism. This act was first introduced as temporary legislation permitting a broad scope of activity, primarily the collection of intelligence, information, necessary to effectively combat terrorism (Silke, 2000).

Terror in Spain

The Basque region of Spain spreads from the Pyrenees into Southern France. It is estimated that half a million Basques live on French soil and approximately two and a half million live within the border of Spain. Basque people have lived in the area since before the Gauls and Iberians settled in Spain and France. The Basques have their own dialect, called Euska. The Basque region has not been an independent state, although they have managed to maintain their language and culture over the centuries. The Basque people have been fighting for self-government since the first quarter of the twentieth century (Simonsen, & Spindlove, 2000).

There are several reasons why separatist political violence occurs in the Basque region (Shabad,& Ramo, 1995). The Basque Country, typified as a declining old

industrial region, has not benefited from foreign investors. Spanish industrialization has increased the economic gap between the growing and declining regions (Ferreiro,& Rodrigues, 1997). The industrialization movement created a new class within Basque society that included industrialist and financiers who began to play a dominant role. Their incorporation into the Spanish Oligarchy had a large impact on the conflict in their region (Shabad & Ramo, 1995). Until the mid nineteenth century, the Basque economy was fundamentally based on agriculture, at which time it suddenly became an industrial region resulting in many problems for the people of Basque region (Uranga, 2000). All signs of a distinctive Basque cultural identity are in danger of disappearing as a result of the centralizing policies of the Spanish government.

General Franco's approach to dealing with the Basque nationals was to suppress them at all costs. At the end of the Spanish Civil War, General Franco incorporated the entire Basque region into Span and outlawed their culture and language. These actions led to a rebirth of Basque nationalist fervor in the lat 1950s, which led to the creation of the ETA (Basque, Fatherland and Freedom) in 1959. The ETA was not originally founded as a terrorist organization, but simply as a group dedicated to promote Basque independence. The group became more compelled to use violence in retaliation against Franco's actions against the Basques. Most members were young nationalists who were frustrated with their lack of autonomy. The ETA signifies the emergence of a form promotion of cultural identity, the adherent to the value of individual rights and the development of set of political claims aiming at modifying the political system in a way

that result in greater autonomy for the regional political units (Guarin&Pelletier, 2000 - Houtum, & Lagendijk, 2001).

The Basque Student Solidarity movement was established in the 1940s. This movement promoted the Basque identity and language. After the arrest of several student activists, the splinter group Ekin was founded. Herri Gaztedi (Catholic Country Youth) and the youth section of the Basque Nationalist Party ETA were later established (Houtum, & Lagendijk, 2001).

During the 1950s, the ETA was divided into several different groups. Most hardened and seasoned campaigners for armed action come from the sub-group of the ETA-military. Their structure was similar to the "cell-like structure" adopted by Provisional IRA terrorists on active service duties. ETA operatives finance their terror campaign though robbery and extortion. The group is also influenced from Mao Tse-tung's works and writing (Simonsen, & Spindlove, 2000). The ETA consist of a specialized network of organizations dealing with religious matters, education, the promotion of the Basque language, mass media, ecology, women, drugs, students, children, international solidarity, as well as prisoners and refugees.

A 1985 survey of the Basque public indicated conflicting opinions concerning the armed struggle by the ETA, with the percent of respondents favoring an immediate abandonment of the armed struggle believing it would be a positive step toward improving the situation in Euskadi. The Basque government condemned the ETA for the first time after the assassination of the Chief of the Autonomous Basque Police (Khatami, 1997). On November 10, 1987 all political parties represented in the Cortes signed the

Pacto de Estado against terrorism. This provided the government a consensus for differentiated policies concerning the ETA. The following day in Zaragoza, the ETA responded with a violent act that killed eleven people including several children (Simonsen, & Spindlove, 2000).

Spain differs from all other Western democracies in the strength of their peripheral nationalism but also in the level of violence associated with center-peripheral conflicts. Among western countries, only the terrorism associated with North Ireland surpassed those in Spain. The ETA is the primary Basque separatist group, but other radical separatist organizations exists as well as several right wing counter ETA terrorist groups. These groups combined are responsible for over three hundred deaths in the past thirty years, more than one thousand injuries, sixty kidnappings, innumerable bombings, armed assaults, robberies, and an extended regime of "revolutionary taxation." The ETA, however, was the primary acting terrorist organization between 1968 and 1992. The ETA was the main object of police repression during those twenty-four years, with more than 100 ETA militants killed, more than 20,000 arrested and more than 1,300 imprisoned in Spain and France during 1992 alone (Shabad & Ramo, 1995).

As a response to these terrorist attacks some right wing terrorist groups acted against ETA's actions. Action Nacional Espanila (ANE) was formed in 1970s and it operated against Basques in the region of northern Spain. The group is responsible for reprisal killing of ETA terrorists and sympathizers (Simonsen, & Spindlove, 2000).

Terror in Italy

By 1954, Italy had become the most likely western nation to turn to communism. Although Mussolini had violently suppressed and oppressed Italian Communists after World War I, the formation of democratically elected government provided an opportunity for communists to come to the forefront. A perfect example of this can be seen through an examination of the Italian Red Brigades (Porta, 1992).

Formed in the 1960s, the Red Brigades represented a left wing fundamental movement. In response to Italian industrialization during the 1950s and 1960s, Renato Curcio and Margherita Cagol of the Sociology department at Trent University founded the Red Brigades to combat neglect of the social structure of the country by the government (Simonsen, and Spindlove, 2000). Comprised of a cell structure similar to that of the IRA and ETA, the Red Brigades were difficult to detect or infiltrate. During this time, the Red Brigades seized occupied factories, intimidated, attacked factory workers and management. They bombed industrial and private buildings. They even used kidnapping to further their cause (Weinberg, & Eubank, 1989).

Between 1969 and 1982, 4,362 events of political violence occurred, 6,153 unclaimed bombings against property occurred, and there were 2,712 attacks for which terrorists groups claimed responsibility. 768 people were injured and 351 killed in 657 denominations used by dozens of underground organizations. Thousands of militants were involved in the armed struggle (Evans, 1989).

Although many analysts have tried to understand the reason for such a long and widespread wave of political violence, initially most of them have explained this terror in

terms of some Italian peculiarity in economic, social, political, or cultural systems. However, it can be seen that many of the conditions that fostered terrorism in Italy have also been present in Ireland and Spain (Porta, 1995).

Terror in Turkey

After the dramatic failure of the Socialist Turkish Labor Party in the election of 1969 many extremist left-wing ideologists seem to regard terrorism as a legitimate method of achieving their objectives. During 1950s, Turkey became a democracy but it did not fulfill public aspirations. This resulted in public disorder and strikes. The new government was unable to prevent anarchy in the country and lost control in 1960 when the armed forces took control. For eighteen months, the country was led by a military commander until civil rule was regained in 1961 (Bal & Laciner, 2001).

As a result of internal immigration to industrialized part of the country during this time, there was growing socialist movement headed by the Turkish socialist of the 1960s. The extension of educational opportunity and the growth of mass communication systems resulted in a noticeable rise in economic and social expectations among the populace. This made it more difficult for largely traditional political leaders to maintain control over the new more politicized working groups.

Global political trends inevitably nourished Turkish leftist ideologies. Turkish political life was vulnerable to radical ideological movements, but many were not ready for this change. During this time Turkish university students began to have an active and radical force in political life (Bal & Laciner, 2001). Several emerging organizations were

willing to use force or violence to achieve their goals. Two of these groups, the revolutionary left (Dev-Sol) and the PKK will now be discussed.

Dev-Sol is a left wing Marxist group that has its origins in the Turkish Peoples Liberation Army from which it split in the late 1970s. The objective of this organization is to foster an uprising or popular national revolution amongst the Turkish working classes. They are vehemently anti-American and NATO. The group is financed primarily through criminal activities carried out in Turkey including armed robberies and extortion from businesses. The group has killed numerous police and military officers, has engaged in robbery, kidnapping, bombings as well as several attacks on United States military personnel. In 1992, the group launched a rocket attack against the United States Consulate in Istanbul. Members of this group are known to have trained with other terrorist organizations. Although efforts by Turkish Security Forces have slowed the activities of this group, they remain a threat to both Turkey and the United States.

The Kurdish Workers Party (PKK) is a militant, separatist organization that aims to create an independent Kurdistan in the Turkish state of Anatolia (Button, 1995). The group began as a student movement at Ankara University, and was founded by Abdullah Ocalan. Their specific objective is to liberate the Kurds. Under his leadership, members of the party and fellow Kurds perform brutal terrorist acts. It is believed that Ocalan killed more that 10,000 Kurds during the 1980s. The PKK has been an active terrorist organization since 1974 involving itself in insurgent activities with aid from Iran, Syria, Iraq, and also extensive support from the Europeans (Button, 1995). They primarily

operate out of southeastern Turkey and desire the creation of a Kurdish state fashioned along Marxist ideologies.

Turkish authorities have argued that there is no Kurdish problem in Turkey, that the citizens of Kurdish ethnic heritage enjoy full rights as Turkish citizens and that their problem is with the terrorist rather than the Kurdish people. Beginning in the mid-1970s, Turkish Kurds have actively demanded more cultural, linguistic, and political rights. In August 1984, Ocalan launched a fifteen-year insurgency that has resulted in more than 31,000 deaths, the destruction of as many as 3,000 villages, and the removal of some 3,000,000 people from their homes (Gunter, 2000). Within Turkey, the separatist terrorism problem impedes the implementation of democratic and human rights reforms and harms the economy when the government is forced to finance counter measures. Turkey has long aspired to join the European Union (EU), however, the democracies of Western Europe have been alienated as a result of their terrorism problem and leaves them open for pressure when it comes to negotiating foreign policy (Gunter, 2000).

During the early 1990s, Ocalan began to intensify his terrorist activities, however he quickly became over extended. The Turkish military spared no expense in containing Ocalan, and they were able to slowly marginalize the military threat of the PKK. Ocalan made yet another bad decision in August 1995, when he attacked Massoud Barzani's Iraqui Kurdistan Democratic Party in Northern Iraq because of their support for Turkish government. The final blow to Ocalan's power came when Turkey threatened to go to war with Syria unless Damascus expelled Ocalan from his long-time sanctuary in that country. (Gunter, 2000) Ocalan fled to Russia and later Italy in November 1998. He

thought he might be able to turn his military defeat into a political victory by having the European Union try him and thus also try Turkey. But in the end because of pressures, Italy and others to rejected Ocalan, and labeled him a terrorist undeserving of political asylum or negotiation.

Abdullah Ocalan (Apo) was captured on February 16, 1999 in Nairobi, Kenya. Upon his detention, PKK activities have entered a new phase. Despite his earlier reputation as a Stalin-like murderous terrorist, Ocalan had done more to re-establish a sense of Kurdish self-esteem and nationalism in Turkey (and possibly elsewhere) than any other Kurdish leader in recent years. (Gunter, 2000).

Against a backdrop of Turkish national pride, Ocalan's capture initially led to a wide spasm of Kurdish violence throughout Turkey and Europe. Osman Ocalan, Ocalan's younger brother and a senior PKK commander in his own right, called upon Kurds throughout the world to extract a heavy price from the Turkish state and let no representative of the Turkish state have peace at home. The PKK'S sixth congress authorized its military arm, the “Peoples Liberation Army of Kurdistan” (ARGK) to wage a fight in the true spirit of an Apo through attacks against all kinds of elements of government. In Berlin, Germany, Israeli guards killed three Kurds and wounded another 16 when they tried to storm the Israeli consulate. Another group calling itself the “Revenge Hawks of Apo” killed 13 people when it set fire to a crowded department store in Istanbul. Further protests occurred in London, Paris, Marseilles, Brussels, Copenhagen, The Hague, Strasbourg, Stockholm, Cologne, Bonn, Hamburg, Frankfurt, Stuttgart,

Hanover, Dusseldorf, Bern, Geneva, Milan, Vienna, Leipzig, Moscow and Yerevan (Lyon & Ucarer, 2001).

Terror in Mexico

The present Mexican conflict began in 1994 when the Zapatista Army of National Liberation (EZLN) launched a rebellion in Chiapas, Mexico. This movement is best described not as a guerrilla struggle for state power, but rather as a social movement resisting the dominant mode of globalization being imposed from above (Stahler-Sholk, 2001). The origins of this conflict date back almost a century.

Since the 1910 revolution, the Revolutionary Party has been in power and the country has undergone significant economic growth resulting in rapid social and economic advances for idle and upper class members of Mexican society. A major issue facing the Mexican government is the land dispute surrounding the Chiapas region in southern Mexico (Gilbreth, & Otero, 2001). Although Mexicans have recently experienced unprecedented levels of economic growth, this has been accompanied by a failure to properly distribute wealth and a lack of social reform. As a result, Mexico remains a country of "haves and have nots." In addition to Chiapas, other regions have experienced guerrilla warfare or, as the Mexican government portrays them, terrorist movements, such as conflict seen in Oxaca and Hidalgo as well as Vercruz and Puebla (Stahler-Sholk, 2001).

Immortalized from the days of the revolution, Emili Zapata, killed in 1919, is lauded by the peasantry of southern Mexico as their true hero. Using Zapata as a symbol

of revolutionary righteousness, the Zapatista movement is currently waging an armed struggle for land rights in the Chiapas region (Castillo, 2001). They first appeared on the world scene in 1994 by waging an armed uprising against the Mexican government to protest the unfair distribution of the land in the region. Although this group uses terrorist tactics to achieve notoriety and political strength, they more accurately fit the description of a guerrilla movement. The referred to land dispute was the result of the enactment of the North Amercan Free Trade Agreement (NAFTA) between Mexico, the United States, and Canada. Upon the adoption of NAFTA, the Mexican government ended the land distribution program. This angered many Chiapas men who had previously worked these farms for a living and in return where granted land for their families from he Mexican government. After NAFTA, many armed and angered Chiapas came down from the hills and attacked populated cities. The Mexican government responded to this local and popular uprising wit the commission of their military. At this point, the Chiapas region was patrolled and controlled by the Mexican Army. The continuing problems facing Mexico are a result of a stumbling economy. The erosion of the ruling Institutional Revolutionary party's power has also contributed to the continuing unrest (Stahler-Sholk, 2001).

In 1995, 30,000 Mexican soldiers intent on the destruction of the Zapatista National Liberation Army (ELZN) guerillas invaded the Chiapas region. Their attempt was a failure, as the ELZN disappeared into the hills of Chiapas. Peace and Justice, another right wing group, pledges its support to the Institutional Revolutionary Party and operates as a death squad in the Chiapas trying to end ELZN activities (Castillo, 2001).

Civil society has responded to the Zapatista uprising in many forms, including protesting for the government to stop the war, organizing human rights security lines to encircle the dialogue site when peace talks were in session, bringing supplies to jungle communities surrounded by federal army units, establishing "peace camps" and observing human rights conditions in communities threatened by the military presence, organizing health, education, and alternative production projects, forming nongovernmental organizations (NGOs) to monitor respect for human rights, building civilian-based Zapatista support groups, and participating in forums and encounters convoked by the EZLN to discuss democracy and indigenous rights. A great deal of mobilization has taken place outside traditional political channels, motivated by the EZLN's call for democracy (Gilbreth & Otero, 2001).

Soon after the uprising, the Mexican government appeared to advocate peace by establishing a cease-fire and agreeing to negotiate with the EZLN. The government appointed a peace commissioner, and just three months after the uprising EZLN representatives and government officials were meeting face-to-face in San Cristóbal. The first round of negotiations broke down in June 1994 as national elections approached, but the process was reestablished in spring 1995 in response to a military action by Ernesto Zedillo's government aimed at arresting the EZLN leadership. The 1995-1996 negotiations in San Andrés Larráinzar established a framework for discussion and a process for achieving signed accords.

The restart of negotiations took place as part of an agreement that required the government to limit the number of troops in the eastern lowlands as a measure of security

for civilian communities threatened by their presence. Despite the agreement, soldiers continued to pour into regions with known support for EZLN as the peace talks continued through 1996. The policy of pursuing peace on one hand and using repression on the other was interpreted by human rights organizations as a form of low- intensity warfare, with parallels to counterinsurgency strategies used during the wars in Vietnam and Central America. From the moment that the Zapatistas' first communiqué was faxed to the national press, the indigenous rebels took their place in history as cultural icons in Mexico.

Recent Changes in Terrorist Activities and Threats

Over the last three decades, terrorist organizations have become more dangerous with availability of new and destructive weapons. Recent years have also witnessed a change in the identity of the terrorists, their motives, and their financiers. Many countries that once excused terrorism now condemn it, and many terrorist organizations have simply disappeared. For example, the Soviet bloc, which once provided support to terrorist groups, no longer exists.

Fighting terrorism is a war without limits. Modern terrorism thrives in urban, industrial, nontraditional environments. Societies most vulnerable to terrorism today are those that are open, and posses a high degree of personal mobility as well as extensive personal freedoms accompanied by government safeguards against arbitrary action by the state against opponents (Livingstone, 1982). The technological infrastructure of modern society represents potentially extremely important and vulnerable targets for weapons that are increasingly sophisticated and available. Modern industrial societies have

vulnerabilities that terrorists or criminals could successfully exploit. In many instances, a small band of determined, knowledgeable individuals could carry out actions that, if successful, could have far reaching consequences. Modern society's vulnerabilities include water supply systems, transportation systems, energy systems, communication systems, computerized management and information systems (Velter& Perlstein, 1991).

An examination of the many forms of terrorist activity will provide a better understanding of the modern terrorist threat. Political assassinations of high-ranking officials have been used by these organizations. Some groups are already involved in drug trafficking to finance their activities. The 1970s and 1980s witnessed a surge in air piracy incidents. Terrorist organizations increasingly use the internet as an effective means of communications and as an avenue for cyber attacks (National Commission on Terrorism, 2002). Many organizations make use of conventional weapons while others have shown interest in acquiring chemical, biological, or nuclear capabilities which would allow for the potential to conflict mass casualties. Transnational terrorist organizations pose a unique threat in that their activities are difficult to predict, track, and penetrate. They receive financial and logistical support from a number of different sources including front organization such as legitimate businesses and nongovernmental organizations.

Although terrorist organizations of the 1970s and 1980s had clear political objectives, it has become apparent that their desires and activities have become more lethal. Whereas earlier attacks were calibrated to produce just enough bloodshed to get attention for their cause, more recent attacks have resulted in less public support because

a growing percentage of terrorist attacks are designed to kill as many people as possible. During 1990s, a terrorist incident was almost 20 percent more likely to result in death or injury than an incident occurring two decades ago (National Commission on Terrorism, 2002). Unlike other threats to the peaceful and orderly conduct of domestic and international relations, terrorism directly affects the personal lives of millions of people, not only through victimization, but also through fear (Long, 1990). There is virtually no place in the world that is safe from terrorism. In the one form or another, terrorism is the disease of the last several decades. This disease is diminishing the freedom of all people (Liston, 1977, Laueur, 2002).

Having examined the definitions, descriptions and motivations of terrorist groups and their supporters as well as their tactics, strategies, and victims, it remains necessary to address the fundamental question of "what is the proper way to combat terrorism?" One of the most important issues in combating terrorism is to know what terrorists are planning beforehand, which can be provided by good intelligence. This will be the focus of the remainder of this paper.

CHAPTER 3

INTELLIGENCE AGAINST TERRORISM

Effective intelligence gathering systems are necessary to law enforcement in the fight against terrorism. The greatest weakness of modern liberal nations in their defense against terrorism is their reluctance or inability to see subversion as a problem until it is too late (Velter& Perlstein, 1991, Long, 1990). It is commonplace to assert that the ability of an open society to deal with terrorism depends on its intelligence capacity. With the developing threat of terrorism in the world, counter-terrorism assistance programs as well as close intelligence and law enforcement relationships have been instigated with many nations in order to prevent terrorist incidents or resolve them in a manner that will deny the terrorists political and financial benefits from their actions (Kahn, 2001).

A well-developed intelligence capability may provide authorities with information concerning upcoming terrorist operations, permitting them to take steps to avert the incident or at least to minimize the damage, as well as aid in the apprehension of suspected terrorists and their prosecution. Activities that can be undertaken by intelligence organizations include the surveillance of suspected terrorists, the infiltration of terrorist movements, the development of informant networks, the design and implementation of contingency systems to respond to terrorist threats, the collection storage and analysis of information as well as direct counter terrorist warfare (Livingstone, 1982). A policy can only be successful when law enforcement knows who the enemy is and where and when he is most likely to strike next. Since terrorist operations are covert, efforts to obtain this information must also be largely covert.

There is almost no debate as to the need to place a high priority on intelligence collection against terrorist threats (Jenkins, 1982). Because lives are at stake, the timely acquisition of tactical intelligence on planned or suspected terrorist attacks is vital if adequate counter measures are to be effective.

Intelligence is comprises of a wide range of activities. There are various methods of collecting information, and there are different techniques for analyzing the information that has been collected. Some of these may be similar to the methods the social sciences use, while others, such as decoding of encrypted messages, are peculiar to the intelligence world. Some of the activities may also be similar to law enforcement work, such as investigating and trailing suspected foreign intelligence agents to learn about their activities. Using encryption to protect communication is another intelligence activity. There are also some ways to deceive adversaries such as "double agent" operations and transmitting of fake messages (Herman, 1996).

Given these wide-ranging parameters, this chapter will outline two broad categories of intelligence collection, including human intelligence (Humint) and technical intelligence (Techint). Prior to this discussion, a brief overview of the elements of intelligence collection will be provided, because these elements are largely common to both Humint and Techint collection methods.

The Elements of Intelligence

The term "elements of intelligence" refers to dividing intelligence according to the types of activity involved. These are *collection, analysis, covert action,* and *counterintelligence* (Shulsky & Schmitt, 2002).

Collection refers to the gathering of raw data through espionage, technical means, open sources, or in any other manner. After collecting information, some *analyses* of information are necessary in order to decide whether it is useful. *Covert* action is different then the other elements of intelligence. Covert actions seek to influence political events directly. In terms of intensity, covert action can range from persuasion or propaganda to paramilitary action (Maurer, Tunstall,& Keagle, 1985). Counter intelligence seeks to protect a society against any harm that might be inflicted by hostile intelligence services. Counter intelligence involves denying certain information to adversaries. Given these other elements of intelligence gathering, this thesis will focus on data collection methods, including those using human and technical intelligence (Holden, 1999).

Human Intelligence Sources

Human intelligence (HUMINT) refers specifically to the "collection of information for intelligence purposes from humans, and related documents" (Foxen, 1999). Human intelligence collection is also sometimes referred to as espionage. These terms typically involves the identifying and recruiting of a foreign official who, by virtue of a position of trust in his government, has access to important information and who is willing to pass this information on to officers of one's intelligence service. In most cases, the person providing the information may not be a government official but a private individual, who has the opportunity to observe something of interest (Shulsky, &Schmitt, 2002).

Another detailed definition made by Michael W. Pick describes HUMINT as follows: “Human Intelligence (HUMINT) is derived from the analysis of foreign positive information collected by a trained HUMINT Collector from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human contacts and informants as a tool, and a variety of collection methods to gather information that satisfies the critical information requirements and cues other collection resources. HUMINT is a foreign intelligence activity focused on the penetration of an adversary's decision-making architecture to obtain information regarding capabilities, vulnerabilities, dispositions, plans, and intentions. HUMINT entities employ human sources or contacts (controlled and not controlled), exploit documents, and execute reconnaissance and surveillance activities to satisfy requirements regarding the adversary” (Pick, Rentner,& Dukat, 1999).

Humint is one of the collection sources that is the oldest, cheapest and still important collection method. The role of Humint is described as getting information from people diplomats cannot meet. There are many kinds of human information sources such as casual travelers, refugees, business contacts, wartime prisoners, wartime occupied populations, occasional secret informants, political opponents, exiles, alternative governments, defectors and agents/informants in place. This last group consist of people who are consciously spying within their own countries, and informers who provide information from within terrorist or other clandestine organizations.

Human intelligence has some limitations compared to technical sources. The identification and recruitment of potential agents takes a long time. Also, communication

and control are always problematic issues. It is very hard for the controller to make sure that the agent doesn't lie or fabricate evidence. Although it has problematic issues it still has special advantages that will be identified and discussed subsequently (Herman, 1996).

The Role and Types of Humint Intelligence Officers

Intelligence officers work secretly in order to be able to garner information from different sources. They must have a plausible reason for being in the country. This may include a clearly visible source of financial support, which can be used as a pretext for meeting people with access to information (Shulsky, Schmitt, 2002). Sometimes an intelligence officer is disguised as a diplomat or some other kind of governmental official. This is called as official cover. Nonofficial cover refers to any other types of disguise that could explain why the officer is in the host country, such as businessman, journalist, tourist, etc…However, official cover has several drawbacks. Most important among these is that the host countries' counter intelligence service may be able to determine fairly precisely which "diplomats" are intelligence officers and which are not. Also, nonofficial cover has too much difficulty. One method is to persuade a private organization to allow an intelligence officer to pose as a member of its staff (Shulsky & Schmitt, 2002).

Collection Techniques

According to Fitchbach (1997) there are two subdivision of human intelligence. The first one is the use of open human intelligence sources, such as gathering information from citizens traveling abroad or official contacts with foreign governments and correspondents with their security and intelligence service. Another open gathering intelligence method from human sources is collection activity through civilian and military personnel assigned to diplomatic and consular posts. The second subdivision is clandestine intelligence collection by human sources (Fitshbach, 1997). HUMINT collection includes "operations conducted using HUMINT collection techniques regardless of the ultimate use of that information." HUMINT activities include a great variety of operations, analysis, and liaison duties (Foxen, 1999). Some of these different collection sources are defined and described below:

CI Force protection source operations (CFSO). This is a tactically oriented overt collection program that uses human sources (informants) to identify potential and actual threats from adversaries. Sources can provide early warning of imminent danger and provide information that helps in the decision-making process.

Liaison activities. Liaison activities involve the gaining of rapport with and elicitation of information from the host country and allied military and civilian agencies. Agents conduct liaison activities with a host nation's military and law enforcement personnel. Liaison can answer collection requirements, coordinate activities, and foster cooperation.

Document exploitation (DOCEX): Is the systematic extraction of information from documents to aid in HUMINT collection operations and to obtain information in response to collection requirements.

Surveillance. Involves the observation of a facility, activity, or individuals to answer collection requirements, support the commander's decision-making processes, or support a CI program.

Screening operations. These are operations to identify sources that may be able to answer collection requirements, serve as CFSO sources, or be a part of a base or area security program. This operation is both a tactical HUMINT and CI operation. Screening operations include: Mobile and static checkpoints (e.g., refugee or displaced persons). Part of a cordon and search operation. Locally employed personnel security. Enemy prisoner of war and detainee.

Interrogation and detainee operations. This is the systematic questioning of large numbers of enemy prisoners of war or detainees in response to collection requirements. This usually occurs at an agency-operated collection facility.

Friendly force debriefing operations. This is the systematic debriefing of forces to answer collection requirements.

Refugee debriefing operations: These are the systematic debriefing of refugees and displaced persons to answer collection requirements.

Single-source HUMINT analysis: This is the analysis of information obtained from HUMINT operations listed above (Foxen, 1999).

Debriefing. This is the systematic effort to obtain information to answer specific collection requirements by direct and indirect questioning techniques of a person not in the custody of the forces conducting the questioning.

Interrogation. This is the effort to acquire information to answer specific collection requirements by direct and indirect questioning techniques of a person in the custody of the forces conducting the questioning. Some examples of interrogation sources are enemy prisoners of war and detainees.

Elicitation. This is the direct interaction with a human source to gain information where the source is not aware of the specific purpose for the conversation. Elicitation is the baseline method for initiating source operations.

Screening. Screening encompasses the techniques used to identify an individual for further exploitation or investigation. Discriminators used in screening can range from general appearance and attitude to specific questions to assess areas of knowledge and degree of cooperation. You must remember that screening is not an intelligence collection technique (in itself). It is a timesaving measure that identifies those individuals most likely to answer an intelligence or CI requirement (Foxen, 1999).

Like intelligence officers, intelligence sources also can be classified. Some groups of people volunteer to assist the intelligence agency, whereas recruited sources are generally considered more reliable, since the intelligence officer has had a chance to study their character and motivation before attempting to recruit them. Sources to be recruited are chosen according to their ability to access to the desired information. On the

other hand, volunteer people can be used by host countries intelligence service to pass false or misleading information.

In addition to classifying sources, we can also distinguish among the reason for why they provide information. Sources may be motivated by ideological, ethnic, and religious loyalties that are stronger than their ties to the countries of which they are citizens. They may be disillusioned by the actions or ideologies of their own countries. They may be greedy. They may be somewhat unbalanced people who wish to bring some excitement into their lives. They may desire to avenge what they see as ill treatment by their government. They may be subject to black mail. The relative importance of these motives depends on the characteristics of the societies involved and on the tactics of the opposing intelligence services (Shulhsy & Schmitt, 2002).

Technical Intelligence Collection Methods

The new information era has focused increasing attention on the power of new information and communication technologies (ICTs) to transform human affairs. Technology is now a definite power in military conflict and state security matters. Information in the form of intelligence has always played a role in war and defense. This kind of warfare (called information warfare) is defined by the deployment and use of information-rich weapons that are not just smart but brilliant (Black& Brunt, 2001). Besides admitting the importance of new ICTs, some theorists have doubted their potential to both shape human activity, emphasizing instead the action of human needs on technology, and to create a fundamentally new society, an information society substantially different from the industrial society of the past two centuries

(Webster,1995). Parallel to these developments, a new term "technical intelligence" has emerged to explain the technological adaptation of intelligence collection.

Technical Intelligence Collection (TECHINT) refers to a group of techniques using advanced technology, rather than human agents, to collect information (Outzen, 1997). These include: Photographic or Imaginary Intelligence (PHOTOINT); Signal Intelligence (SIGNINT); Communication Intelligence (COMINT); Electronic Intelligence (ELINT); Telemetry Intelligence (TELINT); Measurement and Signature Intelligence (MASINT); and Intelligence Collection from Computers and Internet (HACKINT).

Collection platforms can range from the mundane to the exotic. For a modern, technologically advanced intelligence community, the decision about which platforms to use and in what combinations is principally a product of two assessments: Which platforms can best collect the desired intelligence? Second, what are the relative costs and risks involved in using particular platforms? The section below outlines some of the more dominant technical intelligence collection tools.

Photographic or Imaginary Intelligence (Photoint or Imint)

In general, imagery intelligence (PHOTOINT or IMINT) involves photography for intelligence purposes. More specifically, PHOTOINT allows the controller access to intelligence from sources that are not directly accessible (Shulsky, Schmitt, 2002). Early PHOTOINT techniques began to appear around the turn of the twentieth century with the invention of the camera and aviation (Burrows, 1988).

The importance of IMINT is obvious in that a picture is worth a thousand words. As Brigadier General William Mitchell, the American apostle of airpower in the interwar period, wrote, "One flight over the lines gave me a much cleaver impression of how the armies were laid out than any amount of traveling around on the ground" (Weigley, 1977). Through the use of new digital technology collection method, more types of imagery are possible and dissemination time is shorter.

At the beginning of the First World War in August 1914, the British forces conducted aerial surveillance of the German troops (Weigley, 1977). Then in World War II (WW II), cameras were placed on reconnaissance planes (Shulsky, Schmitt, 2002). Years later, unmanned aircrafts were developed for photographic surveillance over adversaries' terrain (Wilson, 1996). Today, governments are investing heavily on satellite reconnaissance. The main advantage of photographic reconnaissance from space is the quality and power of the optical equipments. Today's technology allows for space images to be recreated on earth in virtually "real time," with negligible delay (Hough, 1992). The combination of imagery with geo-location accuracy and digital terrain elevation data (DTED) allows for the display of all-source data in the context of terrain so that enemy capabilities for observation cover and concealment, as well as and firing and maneuvering can be seen (Smith, 1996). This technique also has some drawbacks. Photo quality may be affected by the position of the satellite to the sun and because the light must pass through the entire atmosphere, images may become blurred (Shulsky, & Schmitt, 2002).

Signal Intelligence

Signal Intelligence (SIGINT) is the generic term given to the process of deriving intelligence from intercepted electromagnetic waves or signals. There are several types of signals that are frequently intercepted (Shulsky & Schmitt, 2002). These are: 1) communication intelligence (COMINT), 2) Telemetry intelligence (TELINT), and 3) Electronic intelligence (ELINT).

Communication intelligence. The oldest signal intelligence is COMINT. It is practically synonymous with the use of radio for military and diplomatic communications. It is basically using technological advantages to intercept any means of communication. Another technique, known as "traffic analysis", can derive useful information from fluctuations in the volume and other external characteristics of radio communications, even when the content of the messages cannot be understood. For example, if an army headquarters and its subordinate command post exchange an unusually large number of messages, an analyst might conclude that an important operation is about to take place. Similarly, the location of a ship, plane or command post can be determined by defining the geographic origin of transmitted radio signals (Peterson, 2000).

It is expected that a nation's most sensitive radio messages will be encrypted to protect their confidentiality, so this kind of precautions against interceptions of communication may make SIGINT ineffective (Peterson, 2000).

While most COMINT involves the interception of radio messages, messages transmitted by wire also can be intercepted. This technique is more difficult in that it

requires physical access to the wires making its application less general, although in some cases it may prove vital (Hatch & Benson, 2000).

Technological advances in telecommunications pose new problems for the collection of communication intelligence. Whereas traditional radio interceptions were dependent on the ability to place a receiving antenna of sufficient sensitivity in the right location, the tapping of standard telephone line requires physical access to such line making the interception of advanced communication methods more difficult. For example, fiber optic cables, which have been adopted commercially because they provide much greater ability to transfer more information per unit, are also much more difficult tap than the wires they have replace (Peterson, & Basinger, 1996).

In the future, individuals will use pocket-sized, wireless, personal communication systems to transmit voice and data to any location around the globe. Encrypted systems using spread-spectrum multiplexing techniques and advanced, complex digital modulations will gradually become the norm (Peterson, 2000).

Telemetry intelligence (TELINT). Telemetry intelligence, or TELINT similar in concept to COMINT except that the communications on which one is eavesdropping are between a test vehicle (such as a missile) and a ground station and they consist not of words but of readings from various sensors on board the equipment. The value of such variables as the acceleration a vehicle is undergoing, the temperature at various points within the vehicle, the rate of flow of fuels, and so forth, taken together, give engineers on the ground a picture of what is happening in the test vehicle. This helps the engineers

trouble shoot any problems that may have occurred during the test and perfect the vehicle's performance.

At the same time, such information is obviously valuable to potential adversaries. If they can intercept and interpret those data streams, they will gain insight into new weapons systems still in the testing stage. Thus, just as in the case of COMINT, the country conducting the test may seek to deny others access to telemetry information by broadcasting it back to ground stations in encrypted form. Alternatively, the telemetry data may be recorded and kept on board a test vehicle to be recovered and extracted at a later time. This process, called encapsulation, secures the data against interception, however it may be a risky procedure, since in the case of a catastrophic failure of the test vehicle, precisely when the telemetry data would most useful, the 'capsule' containing it may be destroyed or hard to locate (Shulsky & Schmitt, 2002).

Electronic intelligence (ELINT). Monitoring and analyzing electromagnetic emanations, other than communication, from foreign military equipment, involves electronic intelligence (ELINT) (Shulsky & Schmitt, 2002). Generally countries use ELINT to keep track of key elements of another country's armed forces. The EORSAT (Elint Ocean Reconnaissance Satellite) system used by the former Soviet Union, and now Russia, is an example of this kind of monitoring. For years, these space collectors have been used to locate and track U.S. warships by intercepting the routine electronic (such as radar) signals emitted by the ship as they travel on the high seas (Peebles, 1987).

ELINT collection involves more than detecting of the presence of an emitter. For example, one can determine various operating characteristics of radar, such as its beam

width (how much space it can scan at one time) and its maximum operational range just by intercepting radar signal.

Measurement and Signature Intelligence (MASINT)

This is a "new" source of intelligence which was employed to support the oldest form of intelligence -the process of trying to identify an object or event (Moore, 2003). MASINT capabilities include the development of technologies to detect and characterize nuclear detonations. These include seismometers, which measure the shock waves associated with underground nuclear tests; devices to detect the radioactivity associated with nuclear materials or the fallout of above-ground nuclear tests; and sensors for the remote detection of the flashes of light produced by above-ground nuclear tests (US Congress, Office of Technology Assesment, 1988). MASINT techniques include, acoustic, magnetic, seismic, nuclear, biological, and chemical, radar, multi-spectral, hyper- spectral, and ultra-spectral, electro-optic (EO), radio energy, olfactory, and other signatures (Outzen, 1997).

Also, radar-based MASINT intelligence at the tactical level developed. Hyper spectral MASINT (HSM) technology is also being investigated for future applications that will allow armies to examine and identify battlefield entities using new sets of discriminating sensor suits. Some intelligence officials have labeled MASINT “the intelligence of the future’’ with significant applications ranging from strategic to battlefield intelligence (Moore, 2003). The use of new MASINT techniques allows intelligence agencies to accomplish many task quickly and efficiently. These include the

ability to automatically detect, identify, and report an adversary's activities as well as the ability to measure the potential for weapons of mass destruction (WMD) to be used in a particular area. They will allow agencies to detect and locate, provide real time signature data on reprogrammable munitions and sensors, tag and track enemy equipment of all types no matter the environmental conditions, monitor no-fire and demilitarized zones it counter enemy stealth technology (Richelson, 2003).

In addition to these strategic applications, MASINT may also be used as a means of enhancing the performance of smart weapons on the battlefield. The usefulness of MASINT's scope and diversity can be seen in the identification of its various components including, radar, geophysical, infrared and optical, nuclear radiation, radio frequency, materials, multi- and hyper spectral imagery (Sibbet, 1990).

Intelligence Collection from Computers and from the Internet (HACKINT)

The espionage trade is one of the areas in which the internet has proven quite useful (Wettering, 2001). According to the new United States Defensive Investigative Service (DIS), the computers and internet are one of the fastest growing areas of intelligence gathering by foreign governments and potential enemies of the U.S. and its allies. The Internet simplified numerous methods and techniques of espionage, collectively referred as tradecraft by American professionals (Wettering, 2001). Unless individuals or organizations take extraordinary security measures, the Internet offers little privacy. "Cookies'' are electronic intrusions that allow Web site owners to monitor online movements by placing a tag on the visitor's computer tracking his subsequent

Internet use and are already commonly used, similarly various "snitch wares'' software programs that track all sorts of consumer and other on-line behavior are increasingly being used (The American Bar Association, 2000).

Hacker software, which continues to outpace defensive measures, is freely available on the Internet. Intelligence services have learned that mining and analyzing, can reveal useful secrets (Rosen, 2000). According to The National Counterintelligence Center's (NACIC) report (1996): the use of Internet messages by foreign spies is the fastest-growing method of economic spying.

There are several ways for intelligence service to obtain information from computers. These techniques include stealing computers, placing "trapdoors," and hacking into a computer system. The first technique, stealing computers, is not specifically internet related but important to discuss. Laptop computers are obvious targets for theft so that information can be obtained from the hard drive. For example, laptop computer containing thousands of pages of top-secret information vanished from the U.S. State Department in early April 2000, while the British services, MI-5 and MI-6, and Israel's Mossad have also reported missing laptop computers containing secrets. These incidents have the potential to be detrimental to international security.

Placing trapdoors is the next technique that allows for covert entry into a computer system and can be accomplished through three different methods. The first is to place a trapdoor on a computer before it's delivered to the customer. Another is to place a trapdoor on software before it is loaded onto a target compute. Finally, it is possible to hack into a computer and place a trapdoor. Trapdoors are frequently used by government

agencies. For example, several years ago the Iraqi government reported receiving 50 computers that had trapdoors installed on the systems before delivery (Ignatius, 2000).

The third technique is another method of secretly entering another's computers. In general, hacking refers to stealing inadequately protected secrets from government, private companies or an individual person's computers. The Pentagon reported that hackers successfully infiltrated Pentagon computers more than 160,000 times in 1996 with and only one hack out of 150 hacks being detected (*Richmond Times Dispatch*, 1996). In late 1999, the FBI informed Congress that they believed a Russian intelligence effort designed to hack into US government computers has secretly existed (Wettering, 2001). The Pentagon reports over 350,000 attempted computer break-ins (hacks) occur each year, and the FBI estimated losses to U.S. business in 1997 alone at $300 billion (Wettering, 2001).

CHAPTER 4

CASES OF HUMINT FAILURE: PEARL HARBOR AND THE SEPTEMBER 11 ATTACKS

In this chapter I will discuss two specific cases, specifically the Japanese attack on the US naval base at Pearl Harbor, Hawaii in 1942 and the September 2001 terrorist attacks in New York City and Washington, DC. These cases are intended to give the reader a better understanding of the effectiveness of intelligence collection methods. The chapter will emphasize the importance of HUMINT, and the problems that can result from an over-reliance on TECHINT collection methods. These two specific cases were selected because they are generally recognized as cases where there was a failure to recognize the importance of HUMINT, and there was too much attention paid to TECHINT collection methods. These cases can be said to be the worst intelligence failures in United States history. If US intelligence gathering and analysis methods do not vastly improve, more horrific attacks will likely happen in the future.

The Case of Pearl Harbor

Intelligence failures often occur when circumstances change extremely rapidly, events take on a chaotic nature, or when there is an unexpected and unlikely introduction of new actors. These intelligence failures can occur on three district levels, including the collection of information, the analysis of information, and the use of information by politicians or decision makers. The Japanese surprise attack on Pearl Harbor on the 7th of December 1941 demonstrates many of these typical aspects of intelligence failures. Since the attack, a great deal of research and investigation has attempted to illuminate the

causes of failure, and indeed some of the real causes may never be known in full. Some commentators suggest that most intelligence failures are the result of the latter two levels of the intelligence process. In the case of Pearl Harbor it is different. It is rather an example of "failure in the collection" of intelligence and the interpretation and use of intelligence data (Brennen, & Duffy, 2003).

By the middle of the 19th century and the early 20th century, Japan had transformed itself into to a modern industrial and military power from a closed feudal society. During the 1930s, military influences led Japan to embark on a series of conquests. The aim of these conquests was to seize European colonies in Asia by the start of World War II. The main reason for these expansionist policies was to get the resources of oil, coal, rubber, and tin (Wohlstetter, 1962). At this time, Japan's relationship with the United States was also deteriorating. This deterioration started when Japan took Peking, China in 1937. The existing problems made the US move the Pacific Fleet to Hawaii in the spring of 1940. After 1940, the US restricted shipments of oil and other war material to Japan. This move was followed by a more complicated embargo by the U.S and other nations against Japan (Mayer, 2002).

Despite subsequent negotiations with Japan, on November 25, 1941 United States authorities sent a group of additional military forces to Hawaii that included a fleet of 32 warships. In this fleet there were six aircraft carriers and 432 planes. The fleet sailed for Hawaii on a course north of the usual shipping lanes. On Sunday, December 7, 1941, at 6 a.m. Japan launched the initial strike force of 183 aircraft. Also there were Japanese submarines charged at the Pearl Harbor entrance. The first wave of aircraft started at

07:55 and lasted half an hour. Following this there was a second attack that began at 08:45. This second wave of attack lasted almost an hour (Navy Region Hawaii, 2003). Oahu's military airfields were attacked to prevent interdiction of the striking forces. The damage on the United States side was a catastrophic. Several hundred damaged and destroyed U.S. aircraft; aircraft carriers and 16 battleships and 10 other ships were sunk or beached and were damaged. More than 2,000 Sailors lost their lives in the attack, along with several hundred other service members and civilians.

Factors That Contributed to Intelligence Failures at Pearl Harbor

The American intelligence failures at Pearl Harbor were largely related to a lack of human intelligence. Specific problems included isolationist policies, military neglect, lack of professional intelligence programs, Japanese intelligence successes, and a general lack of attention paid to human intelligence needs. These failures made the successful attack on Pearl Harbor almost inevitable.

Isolationist Policies, Military Downsizing, and Neglect. It has been suggested that the United States has had a weak intelligence tradition, primarily because there had been virtually no serious external threats to U.S. security during the first 140 years of its history. Until the advent of World War I, the United States kept defense preparations to a minimum (Lowenthal, 1984). Because of this posture, there was lack of demand for intelligence in order to protect national security. The notion was that the US does not need a well-developed intelligence community. While the US fell behind, nations in other

part of the world (especially Europe) encouraged the development of codes and code breaking in order to deal with continuing conflicts (Piacine, 1997).

On the other hand, there was a strong isolationist sentiment within the American government during the years following World War I. The Hoover administration closed MI-8 (Military Intelligence Section 8-codes and cyphers search established by the War Department's Military Intelligence Section) in 1929, and all personnel and files were transferred to the Army Signal Corps. This limited the State Department's capabilities to formally collect, evaluate, and coordinate intelligence from a variety of sources, and it forced US diplomats to rely solely on its embassies for information to support foreign policy. Isolationist-driven downsizing also impacted the capabilities of military intelligence during this period, thus contributing to the failure of Pearl Harbor (Wohlstetter, 1962).

Lack of intelligence professional development programs. There was lack of professional development programs by intelligence agencies to provide continuity and skill development to intelligence officers. The selection of new candidates for the job was not based strictly on professional capabilities, but rather they selected individuals on the basis of their availability because the job was not attractive for most of the people at that time. In 1930s military promotions were notoriously slow, and few professional officers elected to remain in these assignments longer than absolutely necessary. During the interwar years selection and training was better but still not enough. This training resembled an apprenticeship, and consisted primarily of academic and language study in select foreign countries. At that time training was limited to small numbers of personnel,

and decision makers did nothing to improve the situation. On the other hand, there was no emphasis on using intelligence for operational purposes. All of these shortcomings in professional development created a situation where there was only a very limited number of intelligence experts. During 1940-1941, the system also had some problem in quickly expanding their ranks with foreign language experts, area specialists, all-source analysts, and cryptanalyst and HUMINT specialist to meet the increased requirements for operational intelligence (Piacine, 1997).

Japanese Planning, Security and Deception Activities. During the intelligence collection process related to the attack on Pearl Harbor, the United States focused on technical intelligence collection methods, especially the code breaking of Japanese communication signals. But United States officials were ignoring some disadvantages of technical intelligence collection methods. These weaknesses include the fact that technical intelligence can be made to be deceptive by the enemy. Also, it is difficult to adapt to an adversary's new technology. The Japanese employed strict security measures within Japanese society and throughout the military, and they used deception in order to misguide the US technical intelligence capabilities (Henderson, 2002).

In 1940, the US government managed to break Japanese diplomatic codes and ciphers, known then as the "purple" code. These code-breaking activities were referred to as "magic" by US intelligence officials, because it enabled a select and limited number of government and military officials to read Tokyo's instruction to its diplomats (Kincaid, 2003 & Gaddis, 2001). Despite these code-breaking successes, Japan successfully kept the attack on Pearl Harbor an operational secret from US intelligence sources. The

Japanese were careful about the enemy's capability of getting information while they were planning the attack, and they never transmitted the information concerning the attack along usual channels.

In terms of Japanese military intelligence, all knowledge of the plans for the attacks were kept on a strict need to know basis, including only a tight circle of officials in Tokyo. Plans for the attack were distributed by hand to the ships of the task force so that the Japanese could conceal plans to attack Pearl Harbor. While the Japanese attitude against United States' intelligence capabilities was to make it ineffective, any cryptanalysis and technical means of intelligence collection was useless in foretelling the attack on Pearl Harbor (Thomas, 2003).

In addition to these protection efforts, the Japanese were also changing their communication technologies and encryption methods against US intelligence, factors that also contributed to intelligence failures. By September 1941the US couldn't read Japan's system, because the cryptanalists had failed. The Japanese had changed a major part of the system in December 1940, and the US couldn't break the new codes. According to Commander Etta-Belle Kitchen, the US was clearly unable by this time to learn what the Japanese were up to (Azzole, 1995). These points show that for technical intelligence methods to be effective, they must be supported by HUMIT collection methods.

Neglect of Human Intelligence Needs. There was almost no contribution of HUMINT to the US intelligence community in the case of Pearl Harbor. The main reason for this concerned a general attitude of neglect towards clandestine intelligence operations and espionage in the United States prior to the attack on Pearl Harbor. The

Human Intelligence sources of the United States only included diplomatic, military attaché, observer, and counterintelligence reporting systems, but did not include Non official Cover Officers (NOC's) or informants that could have been used to supply more intelligence information. The absence of NOC's and intelligence informants limited the US's ability to collect relevant information that could have indicated Japanese intentions concerning Pearl Harbor prior to the attack (Rubsridger, & Nave, 1991).

During the period of time prior to the attack, US decision makers did not trust existing intelligence sources. This lack of trust is best illustrated by the case of Joseph C. Grew, US Ambassador to Japan at the time. Ambassador Grew sent a telegram to the State Department that told of a rumor then circulating in Tokyo that Japanese forces would make a surprise attack on the fleet at Pearl Harbor (Kincaid, 2003 & Gaddis, 2001). This information was not from a clandestine source who was close to the attack planners, so the information was dismissed by the division of Naval intelligence. The information couldn't be confirmed by a second trustable intelligence source. There were no known data regarding the present disposition and employment of Japanese naval and army forces. No moves against Pearl Harbor appeared to be imminent or planned for in the foreseeable future.

During the early 1940's, the Federal Bureau of Investigation (FBI) was primarily in charge of investigating matters related to espionage, sabotage, and violations of the neutrality regulations. For these tasks the FBI was mainly working in the continental United States, its possessions (including Hawaii and the Philippines), and in foreign countries of the Western Hemisphere. FBI agent tasks included surveillance and reporting

of activities by personnel assigned to the Honolulu Consulate and the Japanese Embassy staff. They mostly used observation and wiretaps on official and unofficial telephone lines (Piacine, 1997). These wiretaps were used in the absence of any significant HUMINT collection methods. As a result, the organization was not in a position to provide intelligence that could directly foretell the Japanese attack.

In addition to these failures by the FBI, the US State Department was also not able to collect enough intelligence prior to the attack because of a neglect of HUMINT data. MI-8 was in charge of code breaking and supplying information for State Department intelligence gathering efforts. In 1929, the State Department transferred MI-8 to the Army. The main reason for this change was that according to the Secretary of State at the time Henry L. Stinson, decoding of foreign diplomatic communication was unethical. President Hoover was also in agreement with Stinson on these matters, and MI-8 was transferred to a military orientation under the Army Signal Corps (National Security Agency Association, 2003). After that, the State Department's main source of information collection and reporting became the U.S. ambassadors and their embassy staffs. The embassy's primary focus, however, was on political and economic reporting. Because of these priorities, the US embassy in Tokyo was incapable of getting information on Japanese military intentions. While embassy staff worked as official cover officers, they worked under very difficult conditions when trying to obtain information concerning Japanese governmental and military activities, and failed to provide effective information prior to the attack.

Failures by the FBI and the State Department were followed by US military intelligence failures. Enough funding was not provided for the establishment of Human Intelligence (HUMINT) networks in the Far East. Because of security concerns, Army Intelligence could not work efficiently and could not support the field officers with dynamic information that could have included warnings about Pearl Harbor.

Aerial reconnaissance for intelligence purposes prior to the attack on Pearl Harbor was largely impractical. The use of aerial photography was restricted to wartime operations. Because there were concerns about violation of the territorial integrity of sovereign states, these kinds of missions were impossible without presidential approval (Piacine, 1997). This also negatively affected the use of one of the most precious intelligence resources IMINT. In fact, it is unlikely to use only aerial reconnaissance to get al the information to prevent the disaster at Pearl Harbor. Only deployment of the forces and unusual intense movements of forces would have been detected to get clues of the attack.

It primarily appears that intelligence failures related to Pearl Harbor were the result of dysfunctional technical intelligence collection methods, primarily as a result of Japanese counter-intelligence efforts. These problems could have been minimized through more effective use of HUMINT intelligence collection methods. It seems that the United States intelligence community placed too much trust in its code breaking ability. The Japanese were able to effectively neutralize these efforts by avoiding the transmission of attack plans and changing encryption techniques. Under such conditions, technical information needs to be supported by HUMINT sources in order to prevent

failures resulting in the loss of billions of dollars, thousand of military and civilian personnel, and lost trust on the part of the US's own citizens.

The Case of the September 11th Attacks

In this part of the study we are going to examine the terrorist group al Qaeda and its terrorist attacks against the US on September 11th 2001. This attack represents another case of a failure to effectively use HUMINT by the US intelligence community. This section will highlight the failure of the US intelligence community to penetrate al Qaeda, and highlight this failure as one of the most important shortcomings within the U.S. intelligence community (House and Senate Intelligence Committees, 2002).

History of Al Qaida (The Base) and September 11

Al-Qaida (The Base) was established in1988 by Osama bin Ladin. Based in Afghanistan, bin Ladin used an extensive international network to maintain a connection between Muslim extremists in many countries (Federation of American Scientists, 2003). The organization's aim is to replace the Muslim state governments with the rule of *Sharia* (Islamic law). Al Qaida assumed that existing Islamic state governments were corrupt (Alexander, & Swetnam, 2002).

In February 1998, bin Ladin announced the formation of an umbrella organization called "The Islamic World Front for the struggle against the Jews and the Crusaders" *(Al-Jabhah al-Islamiyyah al-`Alamiyyah li-Qital al-Yahud wal-Salibiyyin)* Among the members of this organization are the Egyptian al-Gama'a al-Islamiyya and the Egyptian al-Jihad. Both of these groups were active in terrorism over the past decade. On May 28,

1998, Osama bin Ladin announced the formation of an International Islamic Front for *Jihad* against America and Israel (South Asia Terrorism Portal, 2001). The justification of the formation by Bin Ladin was that Muslims everywhere in the world were suffering at the hands of the U.S. and Israel (Katzman, 2002). According to Bin Ladin, the new Islamic Front would eventually vanquish the American enemy (Federation of American Scientists, 2003).

Some of its more successful operations against the US include: (1) A truck bomb in the parking garage of the World Trade Center on February 23, 1993 that killed six people and injured hundreds, requiring more than $20 million to repair the damage, (2) A truck bomb that killed 19 U.S. servicemen in the Air Force's Khobar Towers housing complex in Dhahran, Saudi Arabia, an attack that injured more than 500, (3) Another attack against the US on 7 August, 1998 involving a truck bombing of the U.S. embassies in Nairobi, Kenya and Dar es Salaam, Tanzania, leaving 234 dead, including 12 Americans, and injuring more than 5,000, and (4) an attack in October 2000 that involved suicide bombers in a boat that blasted a hole in the USS Cole as the ship took on fuel in Aden, Yemen, killing 17 sailors and wounding 39. The US knew before the September 11 incident that Al Qaida posed a big threat for US. These mentioned terrorist attacks should have been seen as a signal of bigger attacks by the US intelligence community.

On September 11, 2001 19 al-Qaida suicide attackers hijacked and crashed four US commercial jets, two into the World Trade Center in New York City, one into the Pentagon near Washington, DC, and a fourth into a field in Shanksville, Pennsylvania, leaving about 3,000 individuals dead or missing-(Center for Defense Information, 2002).

Intelligence Failures That Led to the September 11 Terrorist Incidents

Even before the previous attacks of Al Qaida, the US intelligence community couldn't learn of the activities of the group before hand. Beginning in 1995, 6.7 billion dollars was added to government agencies for counter terrorism. By 2001, federal spending was 19.5 billion. Most of the money was spent on new computer systems, analysts, and hardware. These were all investments aimed at improving technical intelligence resources, but they didn't prevent the September 11 attacks (Gertz, 2002). The technical capabilities of The United States were so great that the National Security Agency (NSA) had networks of listening post around the world capable of intercepting two million electronic messages per hour. These intelligence sources included all forms of electronic communications, from cellular phones to military communications (Aid, 2001).

The terrorists of September 11 entered the US under the radar screen of US intelligence monitoring capabilities. The men were adept at not being detected. They used legal documents, and sometimes adopted false identities. Once in the country, the terrorists obtained post office boxes, covert e-mail accounts, driver licenses, and bankcards. They avoided contact with strangers and communicated with each other by using prepaid cards at payphones or e-mail sent from public libraries (Gertz, 2002). They couldn't be detected. Even traditional law enforcement techniques would have been of more use in developing intelligence on these terrorists than sophisticated technical methods. The traditional "cop on the beat," equipped with plenty of local contacts, would have been more effective. He would have learned legitimate suspicions about these men

by local resistance sources, and could have alerted the US intelligence agencies (Stephen, 2001).

America's intelligence failures led to September 11. Of course, there are many factors that led to this failure, including bureaucratic turf wars, cultural ignorance, outdated technology, and process-oriented biases within the intelligence community (Shelby, 2002). Agencies including the CIA, FBI, NSA, DIA (Defense Intelligence Agency), NRO (National Reconnaissance Office), and INR (Intelligence and Research), despite having many talented and dedicated people, all failed to some degree in preventing and responding to the terrorist attacks of September 11 2001 (Goodman, 1998). One of the main reasons appears to be that too much emphasis was placed on technical intelligence collection methods, and the US intelligence community ignored the method that is most effective in targeting clandestine terrorist group structures—human intelligence. As some analysts believe, this over-reliance on technology-based surveillance may have led to such a catastrophic lack of awareness. According to Knight (2001) there has been a lack of investment in human intelligence work by the US intelligence community. The US intelligence organizations assumed that Osama bin Laden was planning an imminent attack against American interests somewhere in the world, but not in the United States (Gerolymatos, 2002). Unfortunately, they did not have a clue that America itself had actually become the target.

HUMINT is a valuable intelligence source for the CIA. Despite huge technical collection capabilities within the NSA and NRO (the latter serving as U.S. spy satellite builders and operators), the United States failed to recruit human intelligence assets

inside al Qaeda (Sanderson, 2003). Reliance on such assets would have been essential, considering that bin Laden had learned the capabilities of US technical intelligence. For example, his satellite phone was being used to triangulate his position and eavesdrop on his conversations. While Bin Laden had knowledge of this, he created some precautions against US intelligence, such as not to using technical devises without encryption. While there is a possibility that technical intelligence may not be effective, the other reliable intelligence collection method, HUMINT, needs to be implemented against such a group. In addition, U.S. intelligence policies and certain overly restrictive laws make it extremely difficult to recruit human sources from within such a fanatical, dedicated group. In the end, America was left largely unaware of the approaching plans of the terrorists (Sanderson, 2003).

Even prior to the beginning of the attacks in October 2001, the CIA had virtually no local allies on the ground (Gertz, 2002). Abdul Haq, who is a member of the pivotal Pashtun tribe in southern Afghanistan, was the only person on the side of the United States (Center for Defense Information, 2001). Haq served as an important information source to the Western-friendly Northern Alliance force that was engaging Taliban and al Qaeda forces. In late October he left Pakistan with a small contingent, but later he was ambushed and killed. Despite his calls for help, the CIA hadn't provided enough support for him. By losing him, America did not have human intelligence support inside the group (House and Senate Intelligence Committees, 2002). The CIA's failure to engage human sources is the starting point of the intelligence failure of September 11. Even after

the attack the CIA never established solid contacts with the various Pashtun tribes in the south (Pincus, 2001).

The danger posed by Osama bin Laden and al Qaeda was known to U.S. intelligence agencies for years. This fact can be seen from the above-mentioned attacks linking bin Laden and al Qaeda operatives to the crimes (Sanderson, 2003). U.S. intelligence agencies did not have reliable sources close to bin Laden that could have provided intelligence about plans for attacking America (Shelby, 2002). According to Gerz (2002), the US has no reliable sources close to bin Laden, nor any reliable way of intercepting his communications despite spending $ 30 billion annually. US intelligence agencies were totally helpless in tracking down El Qaida (Gertz, 2002). All US intelligence agencies had high capabilities in terms of technological intelligence collection, but these agencies significantly lacked human intelligence from people in a position to know the plans and activities of al Qaida (Henderson, 2002).

Effect of the group's structure and training against technical intelligence techniques. The communications methods employed by such terrorist organizations are designed to defy technological surveillance. Besides using encryption, the group also uses non-technological communication methods in the distribution of the most important information, especially human couriers (Knight, 2001). The group appears to be a network of smaller groups rather than a single organization with a unified command structure. Al Qaida's structure is decentralized, diffuse, and flexible. The group trains their personnel and warns them against possible technical intelligence tactics of US intelligence agencies, such as not to contact each other by phones or regular e-mails.

Small cells of terrorists usually communicate only with members within each cell of the organization rather than those from outside each individual cell. So while there is communication within each cell, it is impossible to detect their relation with other group members. It means that it is impossible to have information about the entire organization (Cameron,1999).

Legislation preventing effective use of HUMINT. While Deutch was the president of CIA, a New Jersey democrat alleged that the CIA was directly involved in the murder of an American and a leftist guerilla in Guatemala. This action occurred through a Guatemalan army colonel that was used by the CIA. As a result of these accusations, Deutch fired two CIA officers and disciplined several others for being candid about the case. This incident also led to the firing of about one thousand covert CIA operatives. It also led to restrictions (since term as "Deutch rules") in the recruitment of agents abroad that have since made it extremely difficult for the US intelligence community to effectively use HUMINT as a weapon against terrorists. The fired agents included Middle Eastern sources. These sources could have been effective as tools preventing the September 11 attacks (Henderson, 2002). These new rules also prevented CIA case officers from recruiting spies, because the rules blocked CIA officers from recruiting agents with criminal or questionable pasts unless these recruitments were approved by CIA headquarters. In these cases, approval was unlikely because of potential political embarrassment to the agency (McLaughlin, 2001).

The effect of the church committee. By the mid 1970s, senator Frank Church (Idaho), and democratic congressman Otis Pike (New York) headed a congressional

hearing that accused the US intelligence community of illegally investigating domestic groups and individuals (Wannal, 2002). As a result of the controversy, by the 1970s the FBI had almost completely shut down its entire domestic security apparatus for fear of being accused of civil rights violations. The FBI was left to deal with specific criminal acts without engaging in collection, analysis, or utilization of intelligence about politically motivated organizations. Subsequent to these actions, the FBI began conducting very limited intelligence gathering operations under strict guidelines set by the US Attorney General. According to Oliver B. Revell former associate deputy director of the FBI, groups believe violence cannot be investigated unless there is evidence that they have committed a violence crime. By that time, intelligence gathering (whether by electronic surveillance or recruiting informers) is probably too late (Gertz, 2002).

Detrimental effects of the carter administration. HUMINT intelligence resources have particularly suffered since the Carter administration (McLaughlin, 2001). Under President Jimmy Carter, human intelligence (espionage) was severly curtailed and dozens of the CIA's most experienced operations officers were fired. Similar actions were taken in the Department of Defense during these years. The decision makers at the time clearly chose technical intelligence collection methods over human intelligence in order to satisfy their primary intelligence collection needs. These decisions would come back to haunt the US in 2001.

A second wave of pressure from congressional and human rights advocates during President Clinton's administration further restricted the effectiveness of covert operations because of human right concerns. A host of other congressionally mandated restrictions

came in, including those preventing the CIA from using cover agents as journalists, clergy or aid workers (Associates of Former Intelligence Officers, 2001). After the events of September 11, American intelligence agencies are intensifying efforts to infiltrate and destroy global terror networks, but this mission involves new difficulties, dangers, and ethical riddles (McLaughlin, 2001).

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

With the collapse of the Soviet Union, the focus provided by the battle against world communism and the balance of nuclear terror disappeared. The biggest effect of the collapse is emerging instability around the world. The single massive threat of the Soviet Union has been replaced by many smaller, but individually highly destructive, threats that are harder to monitor (Pappas, & Simon, 2002). These transnational threats include terrorism, narcotic trafficking, and global crime and information warfare (Fischbach 1997).

Compared to the Cold War era, the threat posed by small, close-knit terrorist groups is more difficult for US intelligence agencies to counter (McLaughlin, 2001). Failure to undermine and destroy these terrorist groups has allowed terrorism to strike fear into the US public, and has destabilized US society. Unlike the Cold War environment, the world of terrorism is always unpredictable. It is a common feature of terrorists that they strike without warning. But states that are the target of terrorist activities have attempted to predict their actions by a sophisticated intelligence effort (Pappas, & Simon, 2002, Taylor, 1987). It seems that agencies have failed to produce enough intelligence regarding terrorism. The United States employs thirteen agencies and thirty billion dollars per year to gather information on individuals, organizations and countries that could or would pose a threat to American security, however they have failed to predict terrorist attacks against two major American cities that caused thousands of deaths and billions of dollars in damages (Pincus, & Priest, 2002).

US intelligence has relied mostly on advanced technology, but use of HUMINT sources still keeps its importance. Virtually all the technical capabilities developed over the last several decades are now publicly known. Satellite imagery is now commonly understood. Because of commercial use of these systems, companies have increasingly challenged the government's traditional dominance of imagery. Signals and communications intercept capabilities have been degraded by the digital and fiber optic revolution and the marked increase in commercially available and effective encryption. The public availability of secure communications means that security is now affordable and accessible to terrorists, organized criminals, and others (Pappas, & Simon, 2002).

Besides these issues, the technology used by the intelligence community has become antiquated. It cost too much money to adapt new technologies to develop new technical intelligence systems. New solutions remain undiscovered and new funding will take time to have an effect. For most of the Cold War, technological advances were almost always initiated by the US government and driven by huge budgets directed at a victory over communism.

In such conditions the United States has spent billions of dollars every year to continue its leading position in electronic intelligence, however, in September 2001 such efforts proved impotent. Basically, electronic intelligence enables the CIA, the NSA, FBI and the other overt or semi-covert organizations to break just about every code and to eavesdrop on friends and enemies alike. It means that they can listen to almost every telephone conversation in the world, read electronic mail, use satellite imagining in order to track the military movements of hostile states. High-speed computers also track any

unusual activity on the Internet by accessing billions of pieces of information, whether business transactions, medical data or credit card purchases (Aid, 2001).

The traditional agent-based operations have been detrimentally affected by these technological advancements. It is now more difficult for case officers to collect information about criminal persons. Terrorists or other criminal groups disguise special documents and communications by using sophisticated technological devises themselves (Pappas, & Simon, 2002). As a result of this, the US's ability to maintain advantages in intelligence collection systems have diminished, and the rest of the world has gained greater access to technology through advanced commercial tools. In terms of the use of technology by terrorists and other criminal groups, there are two results that have surprised the intelligence community, including the use of known technology in unexpected ways and innovative application of combinations of new technologies (Pappas, & Simon, 2002).

Indeed, technological advantages have not only created a false sense of security but also may have enabled bin Laden to manipulate the very sophisticated electronic intelligence techniques to his advantage. Terrorists such as bin Laden have kept up with the technological revolution and have used very sophisticated communications tools. According to some reports, bin Laden has on occasion employed complex digital masking technology (steganography) to transmit photos over the Internet where hidden messages appear within the pictures (Gerolymatos, 2002). Remarkably, it is now possible for anyone with just basic computer skills to easily download from the Internet highly sophisticated encryption software made available free of charge (Wettering, 2001).

Terrorists already have a good idea of how American intelligence is trying to track them. That is why many discard their mobile phones every week or so to confound anyone trying to trace them. Or they log on at Internet cafes using e-mail accounts they change with similar frequency (Berkowitz, 2003). Under these circumstances, bin Laden and other terrorists are able to mask their activities, and the United States intelligence community may not detect them because there is too much electronic intelligence for the US agencies to process, analyze and interpret (Gerolymatos, 2002).

Although technological collection methods lead us to reach most valuable information, admiration for the technology can easily lead to an overestimation of what TECHINT can accomplish and an underestimation of human intelligence capabilities. In the United States, this view was particularly prevalent during the 1970s. Since that time however, Humint's importance has received renewed recognition by a drastic intelligence failures such as the September 11th attacks (Shulsky & Schimitt, 2002)

Recommendations

Just as more legitimate political parties need the broad support of a public constituency, terrorist organizations require public support groups. Such groups provide crucial financial, logistical, political and even legal support. The degree of constituent support that terrorist groups can muster depends on public apathy or antipathy to their cause as well as their attitudes towards the social order generally. To do this it needs a broad human network, and democratic regimes are best for the establishment of this network. The very existence of democratic institutions, including constitutional guarantees of human and civil rights, such as freedom of speech and due process of law,

make it immeasurably easier for terrorists to avoid arrest and punishment than it is in states with authoritarian regime. Penetrating in these groups by HUMINT collection method seems more suitable.

As these two cases of intelligence failure indicate, the current structure of human and technical collection procedures and the US intelligence community's analytic capabilities are in need of repair or replacement. Because the main focus of this study has been to highlight and identify the appropriate use of HUMINT in combating terrorism, the final portion of this thesis will evaluate and recommend possible solutions to the HUMINT crisis. This thesis has attempted to show that the cases of Pearl Harbor and September 11 represent specific examples of US intelligence failures. By highlighting and identifying the problems that caused these intelligence failures, it is hoped that future policy makers will alter these shortcomings in the use of HUMINT.

As Pappas, & Simon (2002) indicate: "First the United States must organize networks of agents to infiltrate the major and more dangerous terrorist groups." The conventional argument is that it is too difficult to plant operatives in terrorist organizations, and it takes years before the agents are in a position to provide useful information. Although the establishment of effective human intelligence structure takes time, the dividends are high and less costly. A well-placed agent can give warning of impending attacks and is better placed to provide information on the short and long term intentions of terrorists or competing states (Gerolymatos, 2002). In order to destroy terrorist networks, more emphasis must be placed on HUMINT sources.

Increased Emphasis on Human Intelligence

Against terrorist groups, the intelligence strategy must be based on a continuing effort to penetrate terrorist groups, whether by human or technical means. Military and civilian law enforcement and diplomats must stay on the offense continually against terrorism around the world (House and Senate Intelligence Committees, 2002). The September 11 attacks renewed questions about the adequacy of U.S. human intelligence capability. Use of spies is an essential aspect of combating terrorism, and the intelligence community has ignored human intelligence against Osama bin Laden's al Qaeda organization (Deutch, & Smith, 2002).

According to the Report of National Commission on Terrorism, the CIA must recruit informants with unique access to terrorism plans. That sometimes requires recruiting those who have committed terrorist acts or related crimes, just as domestic law enforcement agencies routinely recruit criminal informants in order to pursue major criminal figures (National Commission on Terrorism, 2000). Spies and double agents are not nice or reputable people. To satisfy the job of espionage agents, they must be liars, cheats, thieves, and may even engage in criminal activity while working under cover. Spies may be unsavory characters but eminently useful (Gerolymatos, 2002). It seems necessary that Washington bureaucracy should change its attitude towards the role of human intelligence.

TECHINT and HUMINT Interdependency

It seems that policy makers don't pay too much attention to clarify the data gathering through more technical means of collection. As Fitchbach (1997) said the capability of technical intelligence is increasing everyday. This causes a reduction of reliance on human intelligence sources, however, human sources cannot be viewed as inconsequential. HUMINT and TECHINT are interdependent with each other. It must be understood that these two methods are most appropriately used in combination with one another so that failings can be compensated for. For example, human intelligence can be used to fill gaps existing in technical intelligence collection systems. Human sources, or HUMINT, can provide access to valuable signal intelligence, which incorporates primarily voice and data communications intelligence, thus strengthening human intelligence resources. But human intelligence collection methods cannot be separated from other intelligence activities (Deutch, & Smith, 2002).

Technologic advocates have overestimated the abilities of TECHINT and have failed to recognize its weaknesses. On the other hand, advocates of HUNINT have ignored the technical capabilities of terrorist and organized crime groups. The decision makers have to remember the independency between Humint and Techint. In other words, human intelligence sources should be supported with new technologies and both sources should be interdependent. The main reason to show emphasis on Humint is it can be used to have information that can't be obtained by any other intelligence collection method of intelligence (Davies, 1999).

Technological information gathering methods and their capabilities have become so broad that these technologies must be controlled so that they are able to distinguish important information from unimportant information. By doing this, technical intelligence can be used on real targets and the methods become more effective. Human intelligence collection can provide essential first indication that something of interest is occurring or will occur at a given location. This makes it possible to utilize technical intelligence tools to target this area. In short, by using a combination of human and technical intelligence collection methods, intelligence agencies can become more effective and efficient (McCutcheon, 2001). In addition, human intelligence source can also provide the clues necessary to interpret the raw data gathered by a technical collection system. Even with a good quality pictures, an intelligence officer cannot determine its function, however, a human source who is familiar to the situation can provide valuable additional information.

Increasing Resources to Establish Improved HUMINT Networks

In some cases, the US needs to implement expensive policies in international and national intelligence gathering strategies, however, the use of greater HUMINT resources can reduce these costs. The U.S. Intelligence community must have the requisite number of agents, and investments in time, people, and funds for the development of HUMINT capabilities must be made in order to combat the terrorist threat (Fitscbach, 1997).

Reward Programs for Information Concerning National Security

The criminal acts of September 11, 2001 resulted in changes to existing U.S. law, including rewards offered to confidential informants who provide information on terrorist activities. Prior to September 11, there were several different venues under which an informant could be eligible for a reward, depending on which agency received the information. Although the events of September 11 did not increase these types of rewards, they modified the incentives to informants, including those who are non-citizens (Kash, 2002) These changes and incentives are necessary in order to encourage people who have access to information about terrorist groups.

Establishing a Separate Clandestine Service for Human Intelligence

In the wake of Sept. 11, Congress wants to change the existing intelligence culture. Besides an increase in funding and scrapping the "Deutch rules," the House intelligence committee wants to create a separate clandestine service for human intelligence akin to Britain's MI-6 (McLaughlin, 2001). The separate human intelligence service, "would combine all HUMINT resources under a similar tasking and operating structure," roles now handled primarily by the CIA's directorate of operations with some coordinated Pentagon covert human collection activities (Pincus, 2001).

The Elimination of Drawbacks

While the terrorist threat against the US grows, intelligence agencies struggling with national security matters need to feel more comfortable with less restriction. While

they are focusing on using HUMINT sources, the elimination of restrictions is an additional way to improve their performance. The reason for this is the information that the policy makers need about terrorist activities and other global crimes can only obtained through associating with those groups. Often, the information policy makers need information about terrorist groups, drug lords, and global crime syndicates. Much of the time, this information can only be obtained through those with associations to these groups, who almost by definition are people of inferior moral character (Madinger, 2002).

The biggest problem of HUMINT for the case officer is working with people in crime groups who may be of questionable character. This situation can cause problems in different levels of operations. In the interest of reducing these risks, in 1995 the CIA developed guidelines to be more selective in their recruits. According to these guidelines, the recruitment of agents whose background includes assassinations, torture and other serious criminal activities needs to be approved by CIA headquarters. Humint needs more attention because agencies can gain more specific information by Humint. Also restrictions my negatively influence the agencies' efforts (House Permanent Select Comity on Intelligence, 2002).

Previously, we have explored the issue of terrorism in terms of definitions, descriptions, motivations, tactics, strategies, and victims of terrorists and terrorist activities. Through these descriptions it becomes clear that terrorism is a problem that can occur at anytime, and in any place. It seems certain that terrorism will continue to be an issue in the future. It is almost impossible to stop all terrorist activities all over the

world, however, it is possible to formulate an anti terrorism policy that can keep terrorist activities at a minimum level and prevent planned terror activities by a well developed intelligence network. It seems that to establish a good intelligence collection system, the approach needs to include both HUMINT and TECHINT, as these methods are interdependent with one another. By using a combination of human and technical intelligence collection methods, intelligence agencies can become more effective and efficient against terrorism.

References :

Aid, M. M., (2001). The National Security Agency and The Cold War. *Intelligence & National Security, 16,(1),* 27-40. Retrieved January 20, 2003 from Ebscohost database.

Alexander, Y. & Swetnam, M. S., (2002). *Usama bin Laden's al-Qaida,* New York: Transnational Publisher.

Alonso, R. (2001, February). The Modernization in Irish Republican Thinking Toward the Utility of Violence, *Studies in Conflict & Terrorism,* 24 *(3),* 131–144, Retrieved January 20, 2003, from Ebscohost database.

Alynna J. Lyon & Ucarer, E. M., (2001, *November 6*). Mobilizing ethnic conflict: Kurdish separatism in Germany and the PKK*, Ethnic and Racial Studies 24* (6) 925–948. Retrived February 24, 2003 from Ebscohost database.

Amnesty International, (1980, Spring). *Matchbox.* Retrieved May 2, 2003, from Ebscohost database.

Associates of Former Intelligence Officers, (2001, September,17). *Weekly Intelligence Notes* , *37 (01)*. Retrieved from World Wide Web: http://www.afio.com/sections/wins/2001/2001-37.html

Azzole, P., (1995, November, 26). A Successful Failure; Communications Intelligence and Pearl Harbor. *The US Naval Cryptologic Veterans Association,* Retrived June 27 from World Wide Web: http://www.cl.cam.ac.uk/Research/Security/Historical/azzole4.html

Bal, I., & Laciner, S., (2001). Challence of Revolutionary Terrorism to Turkish Democracy, 1960-80. *Terrorism and Political Violence, 13 (4)*. Retrived February 24, 2003, from Ebscohost database.

Berkowitz, B., (2003, February 16). The Nation: Terrorists' Talk. Why All That Chatter Doesn't Tell Us Much. ***RAND.*** Retrieved May 10 2003 from World Wide Web: http://www.rand.org/hot/op-eds/021603NYT.html

Black, A., & Brust, R., (2001, Summer). Information Management in Mi5 before The Age of Computer. *Intelligence and National security 16 (2)*. 158-165.

Brennen, B., & Duffy, M (2003). "If A Problem Cannot Be Solved, Enlarge It": An ideological critique of the "Other" in Pearl Harbor and September 11 New York Times coverage" *Journalism Studies*, *4, (1)*, 3–14. Retrieved May 30, 2003 from Ebscohost datase.

Burrows, W. E., (1987). Deep Black: Space. *Espionage and National Security.* New York: Random House.

Button, S.H., (1995). Turkey Struggles with Kurdish Separatism. *Military Review*, *75* (1). Retrieved, February 20, 2003 from Ebscohost database.

Cameron, G., (1999). Multi-track Microproliferation: Lessons from Aum Shinrikyo and Al Qaida. *Studies in Conflict & Terrorism, 22*, 277–309. Retrieved December 04, 2002, from Ebscohost database.

Castillo, R. A. H, (2001, March). Between Civil Disobedience and Silent Rejection Differing Responses by Mam Peasants to the Zapatista Rebellion. *Latin American Perspectives*, *28* (117). Retrieved February, 10, 2003 from Ebscohost database.

Center for Defense Information, (2001, November 28). *Report from the Norther Alliance.* Retrieved March 11, 2003 from World Wide Web: http://www.cdi.org/terrorism/northern.cfm

Center for Defense Information, (2001, September 14). *The International Islamic terrorist Network.* Retrieved March 11, 2003 from World Wide Web: http://www.cdi.org/terrorism/terrorist-groups.cfm#al-qa'ida

Crenshaw M., (2001). *Terrorism in Context.* Pensilvania: The Pennsylvania State University Press.

Davies, F. H.J., (1999). Information Warfare and The Future Of The Spy, Information. *Communication&Society, 2 (.2* , 155-133. Retrieved August, 10, 2002 from Ebscohost database.

Deutch, J., Smith, J. H., (2002, January). Smarter Intelligence. *Foreign Policy*, *128;* 64-70. Retrieved May, 3, 2003 from World Wide Web: http://www.foreignpolicy.com/issue_janfeb_2002/deutch.html

Dingley J., (2002). Peace in Our Time? The Stresses And Strains on the Northern Ireland Peace Process. *Studies In Conflict & Terrorism, 25,* 357–382. Retrieved May, 10, 2002 from Ebscohost database.

Ellif J. T. (1978). *The reform of FBI Intelligence Operations,* Princeton NJ: University Press.

Evans, R. H. (1989, July). Terrorism and Subversion of the State: Italian Legal Responses. *Terrorism & Political Violence, 1,(3),* 324, 353. Retrieved January, 10, 2003 from, Ebscohost database.

Farrel, W.R. (1982). *U.S. Government Response to Terrorism.* Colorado: Westview Pres.

Federation of American Scientists (2003, June 1). A*l-Qa'ida (The Base) Qa'idat al-Jihad/ Usama bin Laden Network*. Retrieved May 18, 2003 from the World Wide Web: http://www.fas.org/irp/world/para/docs/980223-fatwa.htm.

Ferreiro, J. Rodrigues, C., (1997, October). The Role Of Foreign Direct Investment In An Old Industrial Region: The Case Of The Basque Country And Japanese FDI, *European Planning Studies*, *5 (5)*, 637 658. Retrieved May, 12, 2002 from Ebscohost database.

Fischbach J. (1997). *With A Little Bit Of Heart And Soul Analyzing The Role Of Humint In The Post Cold War Era.* Retrieved from World Wide Web: http://www.fas.org/irp/eprint/snyder/humint.htm

Foxen, P. J. (1999, January). Defining CI and HUMINT Requirements. *Military Intelligence Professional Bulletin*, *25, (1)*, 47. Retrieved January, 10, 2003 from the database MasterFILE Premier.

Gaddis, D. (2001). The Story Behind The Telegram. *Naval History, 15* (6) Retrieved June 28, 2003 from Academic Search Premier database.

Gerolymatos, A., (2002). *The Failure of Intelligence.* Retrieved February 10 2003 from the World Wide Web: http://www.omogenia.com/~diogenis/thefailureofintelligence.html

Gertz, B., (2002). Breakdown: How Amerikan Intelligence Led to September 11. Washington, DC.: Regnery Publishing, Inc.

Gilbreth, C. & Otero, G., (2001, July, 29). Democratization in Mexico/The Zapatista Uprising and Civil Society. *Latin American Perspectives*, *28 (119)*. Retrieved February, 21, 2003 from Ebscohost database.

Guarin, D., Pelletier, R., (2000). Cultural Nationalism and Political Tolerance in Advanced Industrial Societies: The Basque Country and Catalonia. *Nationalism& Etnic Politics*, *6 (3).* Retrieved February, 02, 2003 from Ebscohost database.

Goodman, M. A., (1998, May 5). US Intelligence Failure Shows Need for Reform, *Christian Science Monitor*, *90 (120).* Retrieved January 5, 2003 form Ebscohost database.

Grosscup, B., (1998). *The Newst Explosion of Terrorism*. New Jersey: New Horizin Press.

Gunter, M. M., (2000, October). The Continuing Kurdish Problem In Turkey After O¨Calan's Capture . *Third World Quarterly*, *21 (.5)*. Retrieved February 24, 2003 from, Academic Search Premier database.

Henderson, P. G., (December, 2002). Intelligence Failures of 9/11*, World & I, 17 (12).* Retrieved April 13, 2003 from database Topic Search.

Holden, L. R (1999, July September). Counterintelligence: A Decade of Change , *Military Intelligence Professional Bulletin*, *25 (3)*. Retrieved on October 2002 from the Database MasterFILE Premier.

House and Senate *Intelligence* Committees (2002, October, 17). *Joint Hearing On Pre-9/11 Intelligence Failures.* Retrieved April 13, 2003 from database Topic Search.

House permanent Select Comity on Intelligence (2002, July). *Counter terrorism Intelligence Capabilities and performance Prior to 9-11*. Retrieved 13 April 2003, from database Topic Search.

Hatch. D. A., & Benson, R., L., (2000). *The Korean War: The Sigint Background.* Retrieved August 24, 2002, from World Wide Web: www.nsa.gov/korea/papers/signint_background_korean_war.htm.

Herman M, (1996). *Intelligence Power in Peace and War.* UK:Cambridge University Press.

Hough, H., (1992). *Satellite Surveillance.* Texas: Thomas Investigative Publications, Inc.

Houtum, H. and Lagendijk, A., (2001). Contextualising Regional Identity and Imagination in the Construction of Polycentric Urban Regions: The Cases of the Ruhr Area and the Basque Country. *Urban Studies, 38 (4),* 747–767. Retrieved February 24, 2003 from, Academic Search Premier database.

Ignatius, D., (2000 February16). Software At State, Courtesy of Ex Soviets,'' *The Washington Post,* pp. b1-b7.

Jenkins, B. M., (1982). *Terrorism and Beyond An International Conference on Terrorism and Low Level Conflict*, CA: Rand.

Jenkins, B. (1978). "*International Terrorism: A Balance Sheet*." In J.D. Elliot & L.K.Gibson, (eds.) *Contemporary Terrorism; Selected Readings,* (pp. 235 245). Gaitherburg, MD: International Assosiation of Chief of Police

Katzman, K., (2002). *CRS Report for Congress: Terrorism: Near Eastern Groups and State Sponsors.* Retrieved February 01, 2003 from World Wide Web: http://www.fas.org/irp/crs/RL31119.pdf

Kelly, Robert. (1998). Field Research among deviants; A consideration of some methodological recommendation, in Tontodonato P., F., Hagan. [eds.], *The Language of research in Criminal Justice (pp.98).* Boston: Ally and Bacon.

Kahn, D., (2001). An Historical Theory of Intelligence. *Intelligence and National Security 16 (3)*, 79 92. Retrieved February, 02, 2002 from Database Masterfile Premier.

Kash, D. A., (2002, April). Hunting Terrorists Using Confidential Informant Reward Programs. *FBI Law Enforcement Bulletin, 71..(4),* 26 32. Retrieved March 12, 2003, from Academic Search Premier database.

Khatami, S. (1997, October). Between Class And Nation: Ideology And Radical Basque Ethnonationalism. *Studies In Conflict & Terrorism*, *20, (4)*. Retrieved January, 10, 2003 from, Academic Search Premier database.

Kincaid, C., (2003, June, 5), Bush Must Rectify Pearl Harbor Smear. *Aimreport-Accuracy in Media.*. Retrieved from June 19, 2003 from the World Wide Web: http://www.aim.org/publications/aim_report/2003/11.html

Knight, W., (2001, September, 13). Intelligence technology may not stop terrorists, *New Scientist.* Retrieved December 11 2003 from World Wide Web: http://www.newscientist.com/news/news.jsp?id=ns99991297

Laqueur, W., (2002). *A History of Terrorism.* New York: Transaction Publishers.

Liston, R. A., (1977). *Terrorism.* New York: Thomas Nelson Inc.

Livingstone, N. C., (1982). *The War against Terrorism.* D.C.: Lexington Books.

Lodge J. (1982), Terrorism and Europe: Some General Considerations, in, In Lodge, J. [ed.] *The threat of Terrorism (pp.150).* Colorado: Westview Press.

Long, D. E., (1990). *The Anatomy of Terrorism.* N Y: The Free Press.

Lowenthal, M. M., (1984). *U.S. Intelligence: Evolution and Anatomy*. New York, NY: Praeger Publishers.

Madinger, J. (2000). *Confidential Informant: Law Enforcement's Most Valuable Tool*. Florida: CRC Press.

Maurer, A.C., Tunstall, M.D., & Keagle, J.M., (1985). *Intelligence Policy and Process."* Colorado: Wetview Press.

Mayer, G., (2002) December 7th , 1941. *Australian Screen Education,(28),*6-14 Retrieved May 10 2003, from Academic Search Premier.

McCutcheon, C; T., Pat, T. (2001, October, 10). Fixing U.S. Intelligence: A Cultural Revolution. *CQ Weekly*, *59* (38), 2304. Retrieved, January 13, 2003 from Academic Search Premier.

McLaughlin, A. (2001, May). A matter of ethics for cloak-and-dagger set. The Christian Science Monitor 93 (219), 2. Retrieved May 01 2003 from World Wide Web: itor.com/2001/1005/p2s1-usju.html

Mc Tavish & Loether, (2002). *Social Research, An Evolving Process*. Massachusetts: Allyn&Bacon

Monaghan, R., (2002). The Return Of "Captain Moonlight" 1 Informal Justice In Northern Ireland. *Studies in Conflict & Terrorism, 25,* 41–56, Retrieved January, 10, 2003 from, Academic Search Premier database.

Moore, W. K., (2003, January). MASINT: New Eyes in the Battlespace. *Military Intelligence Professional Bulletin*, *29* (1). Retrieved April, 24, *2003* from database MasterFILE Premier.

Navy Region Hawaii, (2003). *Pearl Harbor: A Grateful Nation Remember*. Retrieved May 10, 2003 from the World Wide Web: http://www.hawaii.navy.mil/Dec7/background.htm

National Commission on Terrorism, (2002). *Report on countering the changing threat of International Terrorism.* Retrieved April, 24, *2003* from MasterFILE Premier database.

National Counterintelligence Center (1996). *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage.* Retrieved February, 10, 2003 from, Academic Search Premier database.

Outzen, R.H.M. (1997, July*) Technical Intelligence: Added Realism at the NT. Military Intelligence Professional Bulletin*, *23 (3),* 20-23. Retrieved January, 10, 2003 from, Academic Search Premier database.

Pappas, A. A., & Simon, J. M., (2002) The Intelligence Community: 2001-2015, *Studies in Intelligence* v.46, i.1,. Retrieved February 20, 2003from the World Wide Web: http://www.odci.gov/csi/studies/vol46no1/index.html

Peebles, C. (1987). *Guardians: Strategic reconnaissance Satellites.* California: Novata.

Pentagon Computers Easy Targets, (23 May 1996). *Richmond Times Dispatch*. p. A12

Peterson, K. C., (2000 ,July). Prophet: Tactical Sigint For The 21st Century, *Military Intelligence, Professional Bulletin, 26, 3,* 40-43. Retrieved April, 11, 2003 from MasterFILE Premier database.

Peterson, K. C., Basinger, P. G., (1996, July). Joint Stars: The Warfighter's Window to the Battlefield. *Military Intelligence Professional Bulletin*, *22 (3)*. Retrieved January, 10, 2003 from, MasterFILE Premier database.

Piacine, R. F. (1997). Pearl Harbor: Failure of Intelligence? *Air War College- Air University.* Retrieved June 29, 2003 from the World Wide Web: http://papers.maxwell.af.mil/projects/ay1997/awc/97-152.pdf

Pick, M.W., Rentner, K. S., & Dukat, R. J., (1999, January). CI and HUMINT in Multinational Operations: The Lessons of Vigilant Blade 97. *Military Intelligence Professional Bulletin*, *25 (1). 16-21.* Retrieved January 10, 2003, from the database MasterFILE Premier.

Pincus, W. & Priest, D., (2002, May, 15). Congress Moves to Lift Intelligence Spending. *The Washington Post*, Page A01.

Pincus, W., (2001; October 2). House Panel Suggests Revamping Intelligence, Washington Post, Page A11.

Pope, C. E., Lovell, R., Brandl, S. G. (2001). *Readings in Criminal Justice*. Milwaukee: Wadsworth.

Porta, D., (1995). Left Wing Terrorism In Italy, in Crenshaw, M., [eds.] *Terrorism in Contex.* Pennsylvania: The Pennsylvania State University Press.

Rosen, J., (2000, April, 30). The Eroded Self: Why Internet Privacy Matters. *The New York Times Sunday Magazine*. Retrieved from World Wide Web: http://www.nytimes.com/library/magazine/home/20000430mag-internetprivacy.html

Richelson, J. T. (2003). MASINT: The New Kid in Town. *International Journal of Intelligence and CounterIntelligence*, *14*, 149 192, Retrieved April 7, 2003 from Ebscohost database.

Rubsridger, J., & Nave, E., (1991). Betrayal at Pearl Harbor. New York, NY: Summit Books.

Sanderson, T., (2003, Jan). Chaos and Neglect , *World & I, 18,(I)*,1. Retrieved April 13, 2003, from database Topic Search.

Shabad, G and Ramo, F. J. L., (1995). Political Violence in a Democratic State: Basque Terrorism in Spain. In M. Crenshaw (eds), *Terrorism in Context* (pp. 51-89). Pensilvania: The Pennsylvania State University Press.

Shelby, R. C., (2002, December, 10). *September 11 and the Imperative of Reform in the U.S. Intelligence Community*. Retrieved from the World Wide Web: http://www.darpa.mil/iao/Excerpt.pdf

Shulsky, A. N.,& Schmitt, G.J., (2002). *Silent Warfare Understanding the World of Intelligence.* Virginia: Brasley Inc.

Sibbet, D. B. (1990). MASINT: Intelligence for the 1990s. *American Intelligence Journal, 11 (3)*, 23 26. Retrieved January, 10, 2003 from, MasterFILE Premier database.

Silke, A., (2000). Drink, Drugs, And Rock'n'roll: Financing Loyalist Terrorism In Northern Ireland. S*tudies in Conflict & Terrorism, 23,* 107–127. Retrieved January, 09, 2003 from, MasterFILE Premier database.

Simonsen, C. E., & Spindlove, J. R.(2000). *Terrorism Today, The Past, The Players, The Future.* NJ: Prentice Hall.

Smith, D. W., (1996, April, June). Force XXI: An Army Imint Concept. *Military Intelligence Professional Bulletin, 22, (2)*. Retrieved November, 09, 2002 from, MasterFILE Premier database.

South Asia terrorism Portal, (2001), *International Islamic Front.* Retrieved February 30, 2003 the World Wide Web: http://www.satp.org/satporgtp/usa/IIF.htm,

Stahler-Sholk, R., (2001). Globalization and Social Movement Resistance: The Zapatista Rebellion in Chiapas, Mexico. *New Political Science, 23 (4)*. Retrieved December, 11, 2002 from, MasterFILE Premier database.

Stephen, G. (2001, May). Proactive Policing, The key to the successful crime prevention and control, *USA Today Magazine, 129 (2672),* 32, 35. Retrieved June 1 2002 from the data base Academic Search Premier.

Taylor, W.R (1987) Terrorism and Intelligence. *Defense Analysis, 3 (2),* 165-175.

The American Bar Association, (2000). ``Facts About Privacy and Cyberspace,'' Retrieved February, 18, 2003 from the World Wide Web: http://www.abanet.org/media/factbooks/cyberspace.pdf

Thomas, W (2003). Are Intelligence Failures Inevitable? Counter Intelligence- Counter Espionage Counter Terrorism. Retrieved June 20, 2003 from the World Wide Web: http://www.ci-ce- ct.com/article/showquestion.asp?faq=5&fldAuto=298

Uranga, M. G., (2000, August). Panorama of the Basque Country and Its Competence for Self Government. *European Planning Studies, 8 (4)*. Retrieved December, 11, 2002 from, Academic Search Premier Database.

US Congress, Office of Technology Assesment (1988). *Seismic Verification of Nucear Testing Treaties.* Washington, DC.: U.S.:Government Printing Office.

Velter , H. J. Perlstein, G. R. (1991). *Perspective on Terrorism*, California: Wardsworth, Inc,

Wannall, W. R., (2002). Undermining Counterintelligence Capability *International Journal of Intelligence and Counterintelligence,* 15 (3),

Wardlaw, G. (1989). *Political Terrorism*. New York: Cambridge University Press,

Webster, F., (1995). *Theories of The Information Society***.** London: Routledge.

Weinberg, L.; Eubank, W. (1989, April). Leaders and Followers in Italian Terrorist Groups. *Terrorism & Political Violence*, 1(2), 156 177. Retrieved April, 11, 2003 from Ebscohost database.

Wettering, F. L (2001). The Internet and the Spy Business. *International Journal of Intelligence and CounterIntelligence*, *14*, 342 365. Retrieved on April, 11, 2003 from Ebscohost database.

Weigley, R. F. (1977). The *American Way of War* , Bloomington: Indiana University Press.

Wilson, R.W. (1996, July September). Eyes in The Sky, *Military Intelligence Professional Bulletin, 22 (3)*. Retrieved on April, 11, 2003 from Ebscohost database.

Wohlstetter, R.(1962)**.** *Pearl Harbor: Warning and Decision*. California: Stanford University Press.